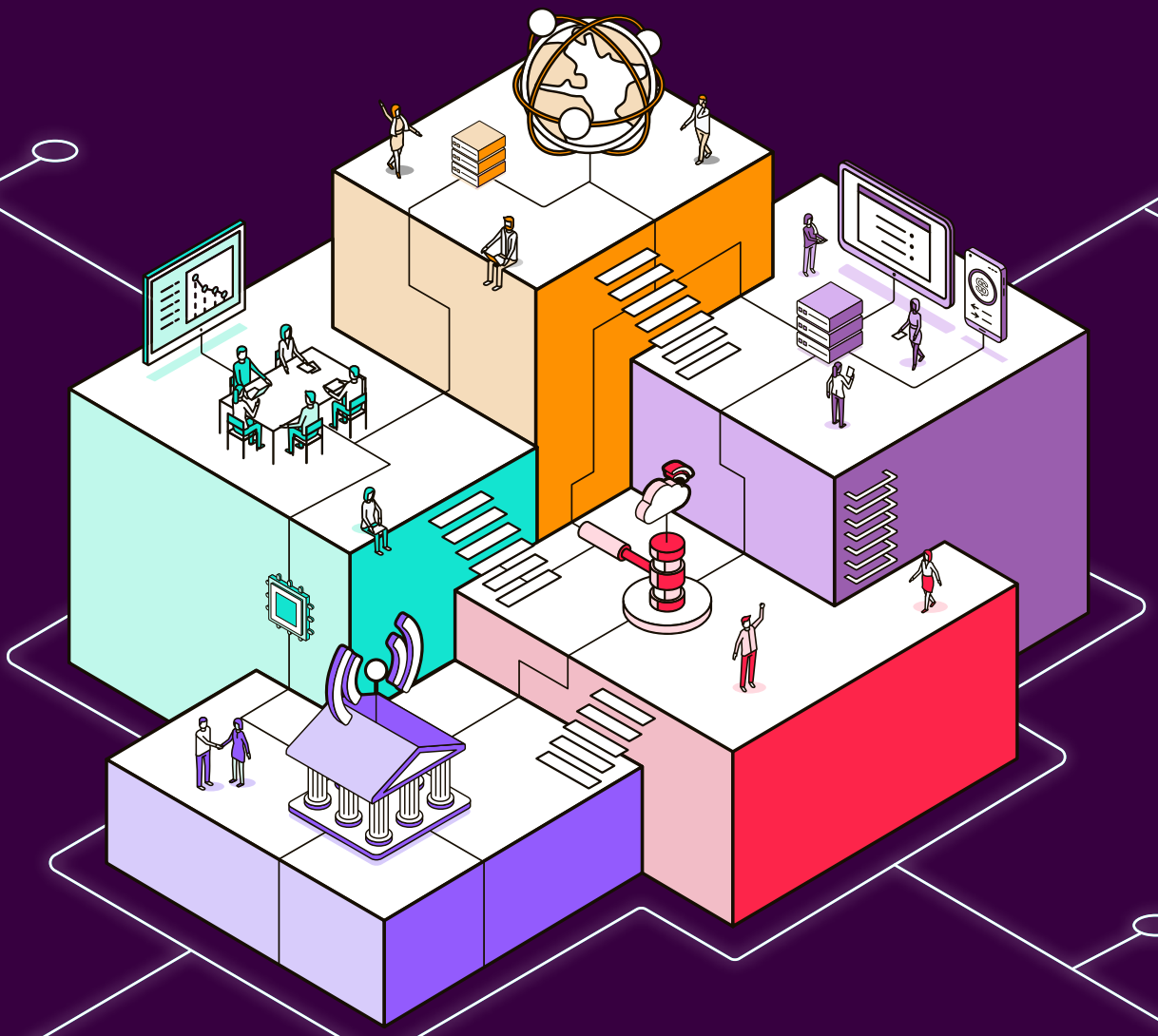


Government digital transformation guide

IDB

Government digital transformation guide

IDB

Authors
Aitor Cubo, José Luis Hernández Carrión, Miguel Porrúa, Benjamin Roseth.

Acknowledgements
Adela Barrio, Alejandro Pareja, Angela Reyes, Antonio García Zaballos, Ariel Nowersztern, Arturo Muente, Darío Kagelmacher, Eduardo Martelli, Elsa Estevez, Estefanía Calderón, Eva María Ortíz Tovar, Evelyn Molina, Florencia Aguirre, Florencia Serale, Francisco Joaquín Martín, Horacio Nemeth, Jesús María Barba Lobatón, José Antonio Mejía, José Clastornik, Julián Inza Aldaz, Julieth Santamaria, Lee Harvey Urquijo, Mar de las Heras Muñoz, Marcelo da Silva, María Inés Vásquez, Mario Cruz Vega, Mildred Rivera, Nuria Simo, Pedro Farías, Rafael Corlazzoni, Sandra Pérez de las Heras, Santiago Paz, Seong Youn Kim, Sheila Grandío and Tomás Sánchez Ochovo.

JEL Codes: H11, H83, O33

Keywords: digital transformation, digital government, governance, regulatory framework, digital talent, digital tools, digital services

Copyright © 2022 Inter-American Development Bank. This work is licensed under a Creative Commons IGO 3.0 Attribution-NonCommercial-NoDerivatives (CC-IGO BY-NC-ND 3.0 IGO) license (https://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode) and may be reproduced with attribution to the IDB and for any non-commercial purpose. No derivative work is allowed.

Any dispute related to the use of the works of the IDB that cannot be settled amicably shall be submitted to arbitration pursuant to the UNCITRAL rules. The use of the IDB's name for any purpose other than for attribution, and the use of the IDB's logo shall be subject to a separate written license agreement between the IDB and the user and is not authorized as part of this CC-IGO license.

Note that the link provided above includes additional terms and conditions of the license.

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.

Inter-American Development Bank
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

The Institutions for Development Sector was responsible for the production of this publication.
Production Editor: Sarah Schineller (A&S Information Partners, LLC)
Editorial review, design and layout: .Puntoaparte Editores www.puntoaparte.com.co
Vectors: Shutterstock.com/Hilch

Content

Prologue

The need for the digital transformation of government is evident in many ways. Citizens want to interact with the government online to access the information and services they need, anytime, without traveling to an office. Public institutions that operate solely on paper are not only more inefficient in their processes, but also less effective in their purpose. A digital government not only exploits the potential of a digital society and economy, but also enables and empowers them.

Achieving digital transformation requires a whole-of-government and citizen-centric approach. It is necessary to: create an institutional framework and governance that guides, drives, and coordinates the effort; develop a regulatory framework that provides the legal basis to new digital processes; design the infrastructure and tools that lay the technological foundations of transformation; promote digital talent; and to create new digital processes and services to transform how the public administration interacts with citizens.

To support the complex process that is the digital transformation of government, the IDB, through the Innovation for Citizen Services division of the Institutions for Development Sector, has developed the Government Digital Transformation Guide. It serves as an "encyclopedia of digital government", as it classifies and summarizes cutting-edge knowledge that, in most cases, is not elsewhere consolidated. All the knowledge in this document was gathered from leaders in the field, who wrote each section to generate the greatest added value for the reader. Like an encyclopedia, it is not necessary to read it from cover to cover - although we recommend doing so.

This Guide allows the reader to go directly to the content that interests him or her. Each section contains examples, links, and self-assessment questions to complement the theoretical description. In short, this guide is designed to be a practical tool that readers can use to drive the digital transformation of government.

I would like to emphasize some principles that underpin the document:

- **Transversality:** Digital government is a resource that can benefit all sectors. Therefore, anything that has applications in multiple contexts (such as sending electronic notifications to citizens) or involves multiple stakeholders (such as interoperability) should be created by a central entity, and only once—to be replicated and expanded across government.

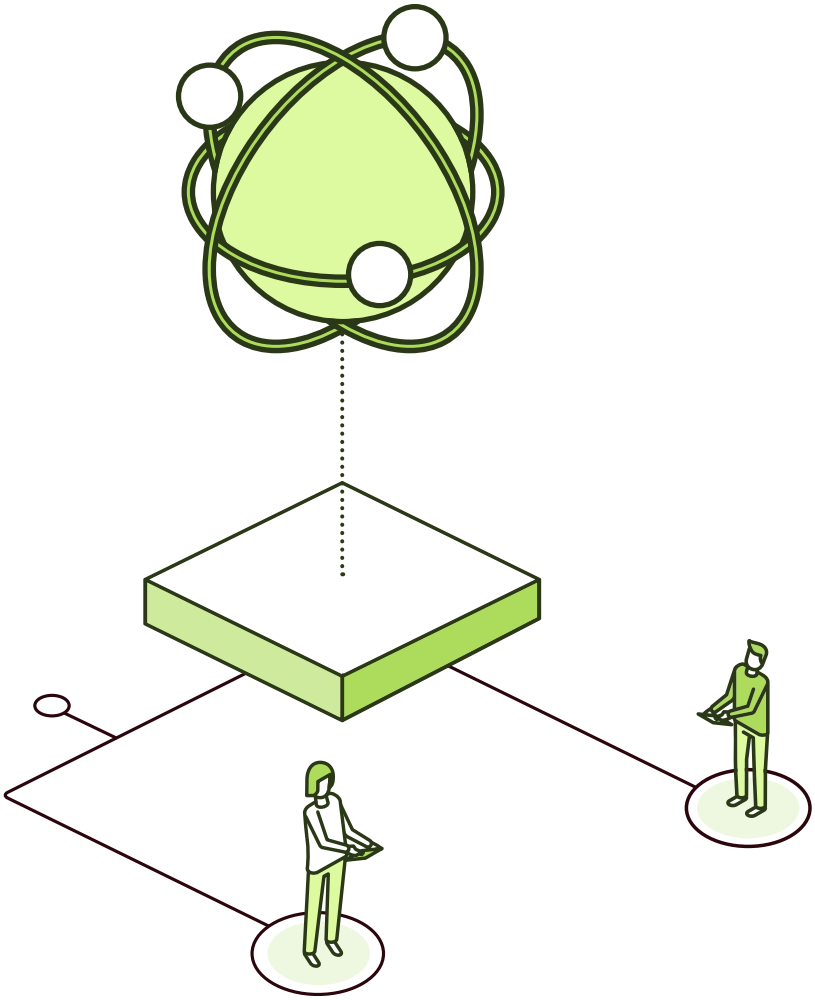
- **Comprehensiveness:** Technology is important, no doubt. But to make the most of it and design it correctly, it is necessary to consider the appropriate regulatory framework, institutional framework, governance, and talent.

- **Technological neutrality:** Technology is most effective when the solution is designed according to the need, and not the other way around. Therefore, the guide adopts a technology-agnostic perspective with respect to specific technologies, emphasizing guiding principles and desired functionalities.

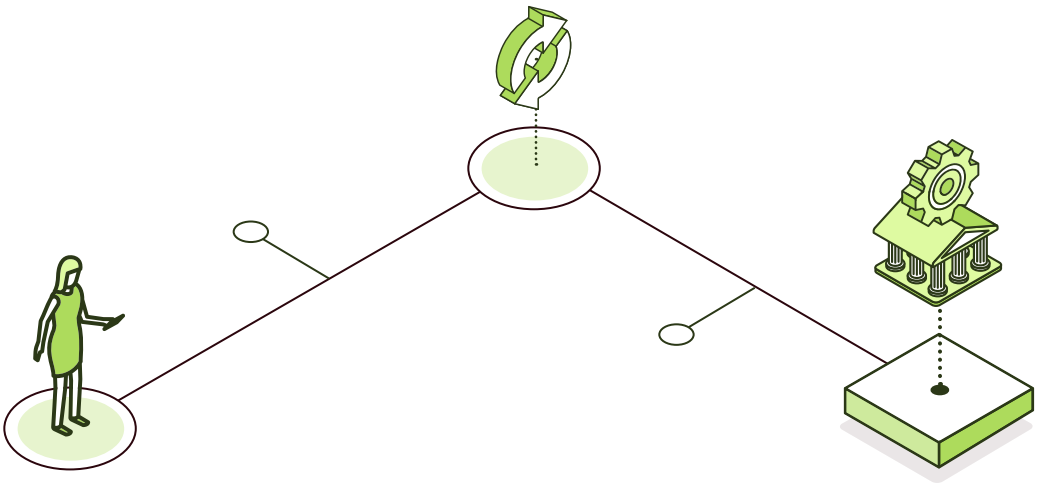
- **Practicality:** Although it is attractive to plan to have all the pieces in place before getting started, we rarely have the ideal conditions for digital transformation. The guide advises on the minimum requirements for a given tool to be feasible, without letting the ideal become the enemy of the possible.

At the IDB we believe in the benefits of open knowledge, especially in the digital field where there is so much to be done. Our goal with this Guide is to empower all policymakers, advisors, consultants, companies, academics, and students to drive the digital transformation of their governments. I invite you to explore it and to join in the journey.

Susana Cordeiro Guerra
Manager
Institutions for Development Department
Inter-American Development Bank



Executive summary



The development of digital technology offers great potential to address the most relentless challenges facing the Latin American and Caribbean (LAC) region, such as lack of trust, low productivity, and persistent inequality. Until March 2020, this phrase could often be read in documents related to the future development of the region as one of the relevant tools to accelerate progress. But with the onset of the COVID-19 pandemic, the expression "digital transformation" has become ubiquitous and is almost always associated with two concepts: inclusiveness (i.e., for the benefit of all), and urgency (i.e., for the present).

COVID-19 has turned digital transformation from a wish or an aspiration to a basic tool in public policy. The concepts, references, and recommendations shared in this document do not vary in the context of COVID-19, or any other adverse event that limits the capacity for personal interaction of human beings, but they do make the availability of the content of this publication more urgent and surely more valuable for those who have to accelerate the digitization of their countries.

For some people and companies in the region, technology has already changed paradigms: how to communicate, how to buy, how to access public services. However, this progress has been partial for various reasons:

- Paper continues to reign supreme.
- Many people and companies are still unable—or unwilling—to use the internet, let alone access services through it.
- Many institutions continue to function as they did last century.
- Many governments provide digital services through a series of ad hoc efforts, with varying quality and limited use.

To address large-scale challenges, it is necessary to adopt a comprehensive and strategic approach that includes all sectors of society and all levels of government and aims at a cross-cutting paradigm shift.

However, this is not to ignore the great progress that has been made in the digital area in the region. As proof of the interest shown by governments, more than 70 percent of LAC countries have a digital government strategy[1]. In addition, there are more cell phones than people in the region, and 64 percent of the population is connected to the internet[2]. Some countries have already digitized most of the procedures provided by the central government, in some cases including the use of digital identity and online payments, and already consolidate their entire web presence in a single domain.

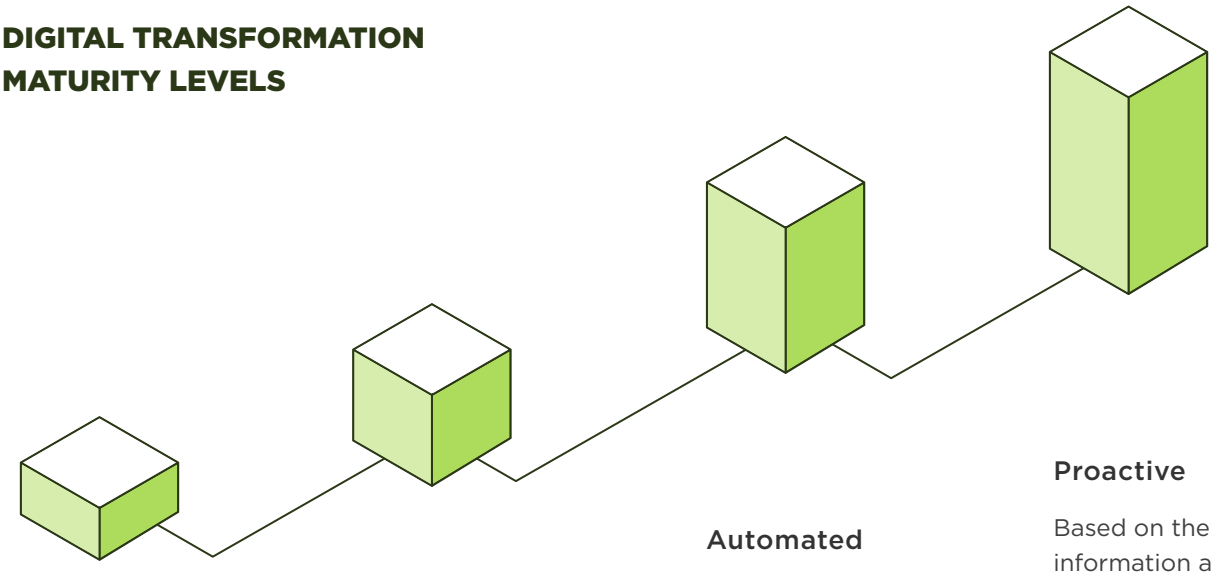
However, it is time to move from isolated efforts to a comprehensive approach and to translate plans into practice. This comprehensive approach—national-level digital transformation—depends largely on the actions of the central government, as no other actor can establish a regulatory framework, create standards, provide common services, and convene all segments of society and all levels of government. Citizens demand it, and the economy needs it: a transversal leveraging of technology and the internet to bring more efficiency, certainty, and transparency to interactions and transactions, both public and private. At the same time, governments in the region also need it to respond to the pressures of fiscal austerity and the hightened expectations they face from citizens.

Government digital transformation is the change in corporate culture, organizational models, methods, and processes that takes advantage of information and communication technologies (ICT) to enable public institutions to meet the needs of citizens and businesses in an efficient, transparent, and secure manner. It goes without saying, then, that digital transformation is more than creating applications and web pages.

DIGITAL TRANSFORMATION HAS FOUR LEVELS OF MATURITY RANGING FROM E-GOVERNMENT (ESSENTIALLY, A DIGITAL REPLICA OF PAPER-BASED PROCESSES) TO PROACTIVE ADMINISTRATION (WHICH TAKES ADVANTAGE OF ALL THE INTELLIGENCE, INTERCONNECTION, AND AUTOMATION THAT ICTS OFFER).

1. https://publications.iadb.org/publications/spanish/document/Panorama-de-las-Administraciones-P%C3%BAblicas-Am%C3%A9rica-Latina-y-el-Caribe-2017.pdf
2. https://publications.iadb.org/publications/spanish/document/Panorama-de-las-Administraciones-P%C3%BAbli-Am%C3%A9rica-Latina-y-el-Caribe-2017.pdf

DIGITAL TRANSFORMATION MATURITY LEVELS



Electronic

Elimination of paper transactions and the need to visit offices in person. Electronic procedures mirror paper-based ones.

Interoperable

Regulated exchange of data between public institutions, which makes the citizen provide his information only once to any institution (or never provide it, if it comes from a public registry).

Automated

The administrative procedure—including the making of some decisions—is done automatically, eliminating manual intervention by civil servants, with algorithms and criteria that can be traced and explained by human beings.

Proactive

Based on the information already provided by the citizen, the state takes actions proactively and in an automated way so that the citizen does not have to initiate them. This can particularly occur around life events (for citizens) and business episodes (for companies).

A key element of digital transformation is horizontal services, also known as "shared tools" or "platform services." These are the tools that serve all of government, including citizens and businesses, only needing to be created once. While it sounds natural that there should be a single digital ID that serves all public and private purposes, and a single interoperability platform that serves the entire country, there are other elements that have typically been replicated institution after institution: payment systems, data centers, and notifications, among others. Leveraging economies of scale is key to achieving the goals of digital transformation.

Building reusable tools helps achieve the following:

- **Efficiency gains**
  The cost of repeated development of the same tools is eliminated.

- **Speed**
  No time is lost in development.

- **Compatibility**
  If everyone uses the same tool, they will be compatible by default.

- **Improved user experience**
  You learn to use a system once, and it is the same regardless of the institution you are interacting with.

THE ROAD TO DIGITAL TRANSFORMATION

It is extremely important that the path to digital transformation be holistic and comprehensive. This is achieved through four key elements:

1. A strong drive from the center that encompasses the whole of government, including the different branches of national government and subnational governments. The central government is ideally positioned to ensure that duplication is avoided and economies of scale are maximized. When digitization efforts are uncoordinated, opportunities are missed. For example:

   - A digital ID is good, but it is better if it is unique and universal.
   - An online service is good, but it is better if it is accessed through a single point of access, where the other services are also located.
   - An electronic court file is good, but it is better if it interoperates with the state's other information systems and administrative records.
   - A digital system of municipal administrative management can be good, but it is better if it is provided free of charge to any municipality that wants it and offers similar functionalities to the municipality next door, even if it is a fraction of the size

2. Broad—and active—participation of all segments of society. It is a pity when a service is put online and nobody uses it, or when it is used but does not really solve the most pressing needs. That is why private companies, civil society, academia, and ordinary citizens need to be involved in the design of digital transformation. This is a two-way communication exercise: listening about the needs and also communicating about the changes to come and the shared responsibilities.

3. Inclusion of all levels of government. While the central government is important in coordinating and driving initiatives, it is the subnational governments that generally face citizens. Particularly in Latin America, many municipal governments are in an extremely difficult situation, with great responsibility for spending execution and service delivery on the one hand, and limited administrative capacity on the other. In that sense, digital transformation has immense potential for municipal governments, as it allows those governments to:

- Improve the provision of services to citizens and businesses;
- Ease administrative burdens;
- Reduce spending on technology.

However, to date, the vast majority of digital government efforts have been made only at the central level. For the digital transformation to be truly national, subnational governments must play a leading role

4. Inclusion by design, so that digital transformation truly becomes a tool for social equity and does not become an aggravating factor of inequality. The great danger of digital transformation is that it will increase the gaps in society, whether based on income, gender, age, ethnicity, location, or other factors. As the most unequal region in the world, Latin America cannot afford an exclusionary digital transformation. Digital offers a great opportunity to democratize access to information, participation, communications, and services, as long as the closing of gaps is an objective from the beginning.

HOW TO STRUCTURE DIGITAL TRANSFORMATION

In order to have a holistic vision of digital transformation and ensure its success, **it is important to take into account five axes[3]:**

Governance and institutional framework

Legal and regulatory framework

Digital talent and change management

Infrastructure and technological tools

New digital processes and digital services

3. It is essential to point out that the different issues addressed throughout the document—such as digital identity, interoperability, and cybersecurity, among others—often appear in multiple axes. They are mainly addressed in the regulatory framework axis and in the infrastructure and tools axis, due to the weight they have in both of them, but it cannot be forgotten that any of these will be supported by the actions carried out in the other axes, such as the actions of the strategy or operational management, which will serve as a substrate for the generation of the new digital processes of the administration.

GOVERNANCE AND INSTITUTIONAL FRAMEWORK

Given the need to promote holistic vision, to coordinate a multiplicity of actors inside and outside government, to create and operate a wide range of horizontal services, to promote and operationalize regulatory changes, and to provide technical assistance to many public institutions, four main elements of governance and institutional framework are essential:

- A **digital transformation strategy** that ensures that
  - The objectives to be achieved are defined;
  - The actions to achieve the objectives are planned;
  - Procurement, communication, cybersecurity, and monitoring plans are aligned to ensure success.
- A **strong lead institution** in charge. This institution, whose remit is general—not tied to any sector—must have the mandate, the powers, the human talent, and the budget to respond to the great challenge of driving digital transformation.
- **Governance mechanisms,** which are absolutely necessary to respond to the needs of all those involved in a major digital transformation and to ensure that the interests of all are considered.
- **Operational management,** because as the explosion of digital services is generated, it is necessary to have perfectly defined and standardized architecture, operation, demand, and portfolio management mechanisms. Operational management cannot be done by brute force to ensure success, so it must be proceduralized.

LEGAL AND REGULATORY FRAMEWORK

The regulatory corpus in many countries is several decades old or more and, in many cases, is not adjusted to the new reality that the digital transformation brings. The incorporation of new regulations serves to provide legal certainty to digital tools and ways of working. Appropriate regulations are what makes it possible to:

- Verify identity digitally;

- Sign a document or save transaction records electronically and automatically;
- Regulate new vulnerabilities that arise in the digital environment, such as those associated with data protection and cybersecurity.

It should be borne in mind that, especially in the public sector, legal certainty is essential for carrying out administrative actions. Therefore, it is necessary that all tools, procedures, and systems have a clear legal basis. In addition, it is important to consider that the regulatory framework should not be confused with the legal framework, since the latter would be encompassed by the former. Thus, the regulatory framework encompasses both the legal framework and the organizational regulations, in addition to semantic and technical standards. In fact, depending on the detail of each aspect to be regulated, the level at which it is regulated (law, decree, technical standard, etc.) must be decided in each case.

DIGITAL TALENT AND CHANGE MANAGEMENT

In the twenty-first century, it is not possible to lead the digital transformation of a country or a large sector without the appropriate resources. At this point, a common mistake that is often made is not having such means and embarking on the process anyway. However, digital transformation cannot be bought on a shoestring. Of course, a large part of it is acquiring goods, whether hardware or software, or hiring people, but a large component of success lies in the internal transformation of the administration itself, of the public employees that make it up. That is why it is necessary to

- Have the right positions to lead this change in functioning.
- Train public employees according to their needs.
- Manage change in an orderly manner and based on criteria and instructions given in the offices, with preset rules.

INFRASTRUCTURE AND TECHNOLOGICAL TOOLS

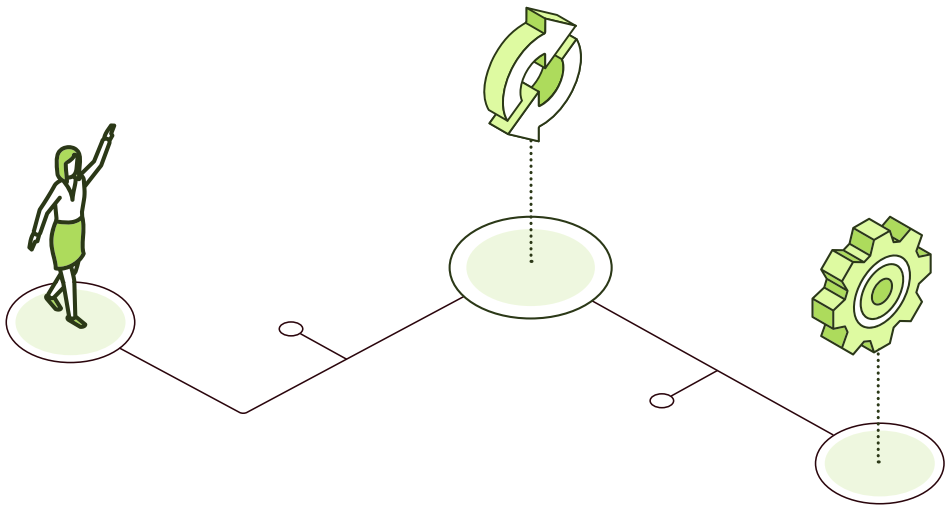
The heart of digital transformation is formed by the different technological tools used. While there are a myriad of sectoral applications of technology that drive digital transformation (e.g., virtual classrooms in education or telemedicine in healthcare), this Guide mainly emphasizes those core, shared, and enabling systems. It briefly reviews the infrastructure requirements to enable digital transformation to become a reality.

NEW DIGITAL PROCESSES AND DIGITAL SERVICES

This is the goal in itself. Digital transformation is carried out not by simply having technology, but by using it efficiently and intelligently to move from a slow, in-person, paper-based administration to a technology-based one, accessible from the internet, twenty-four hours a day, seven days a week, and without lines. To this end, it is necessary to review administrative processes and procedures to adapt to the new reality, making use of available technology and the new regulatory frameworks. Above all, we must avoid "automating chaos."

There are opportunities for digital transformation in every area of public sector activity. In health, education, transportation, security, environment, taxation, etc., a digital transformation can bring improvements such as greater efficiency, effectiveness, and transparency, which bring benefits for both service users—citizens and businesses—and for the institutions themselves. However, it is important to distinguish two types of changes that can be promoted at the sectoral level:

- Those that are unique to the sector. For example:
  - In the health sector: digital remote surgery, telemedicine, digital health records, and much more.
  - In education: virtual classrooms, digital readers, adaptive learning, etc.



EACH SECTOR MAY ALSO HAVE ITS OWN STRATEGY TO PROMOTE DIGITAL TRANSFORMATION.

- Those that are shared by multiple sectors and/or levels of government. For example:
  - A national interoperability scheme to facilitate the exchange of information
  - A digital ID
  - A digital signature
  - Cloud services

The focus of this document is on the common elements, which can be used in a variety of sectoral contexts. In that sense, examples of applications in different sectors will be found in the anecdotes presented after the descriptions of each element. However, it is important to note that the intention is to promote a centralized development of the different systems and tools described. This is key for a variety of reasons:

- It generates economies of scale by creating a tool once and reusing it.
- It ensures compatibility of systems between institutions.
- It allows small institutions (including municipal governments) to benefit without having much capacity of their own.
- It provides a unified experience for both citizens and businesses (e.g., by having a single digital ID instead of one per sector) and officials (e.g., by having a single interoperability scheme instead of many bilateral arrangements).

As the rest of this document will make clear, there are a large number of common elements. Therefore, it is essential to complement the technological with a regulatory framework and an institutional framework capable of managing the digital transformation in a consolidated way, so that it acts for the benefit of all public institutions, citizens, and businesses.

As will be discussed in some sections of the document, mainly in the strategy sections, the axes of a country's digital transformation can be the main motivation for driving the transformation and some countries will emphasize one aspect over another due to their particular context. If a country has an easier

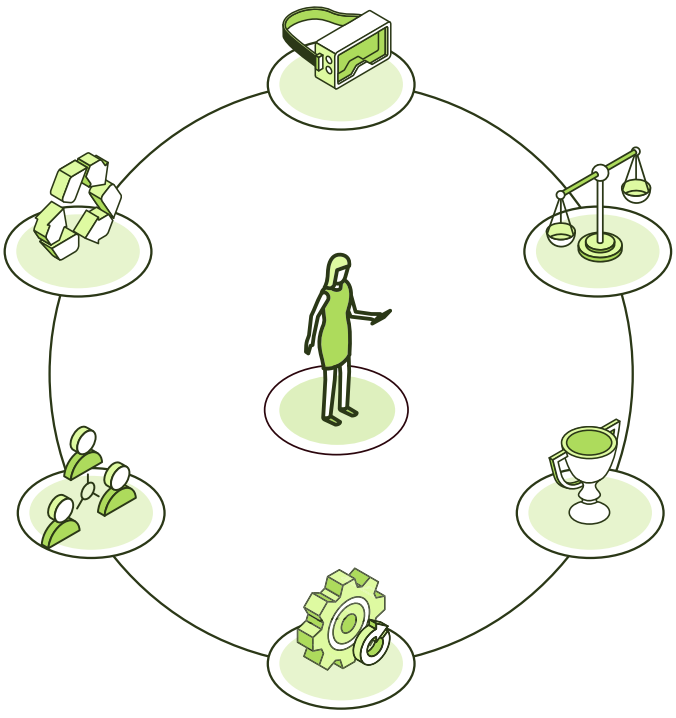
regulatory development path (for example, because the government has a legislative majority), it should take advantage of that path, without neglecting the rest. If a country can develop technological tools that favor transformation, it should not be paralyzed because the other pillars do not advance at the same pace.

In the long run, however, progress needs to be balanced. For example, a technological solution for digital signatures is of little value if there is no regulatory framework to give it legal validity. Likewise, it is of little use if there is no lead institution to support its implementation throughout the state.

Similarly, in each element there is also a sequence: it makes no sense, for example, to talk about an electronic file exchange system if the electronic file as such is not first standardized at the country level. Requirements of this type are common to many elements of digital transformation.

Finally, it is important to note that this guide is not intended to be an exhaustive study of each of the topics covered, but rather to offer a general and holistic view of all the levers of change that need to be worked on when addressing the digital transformation of a country.

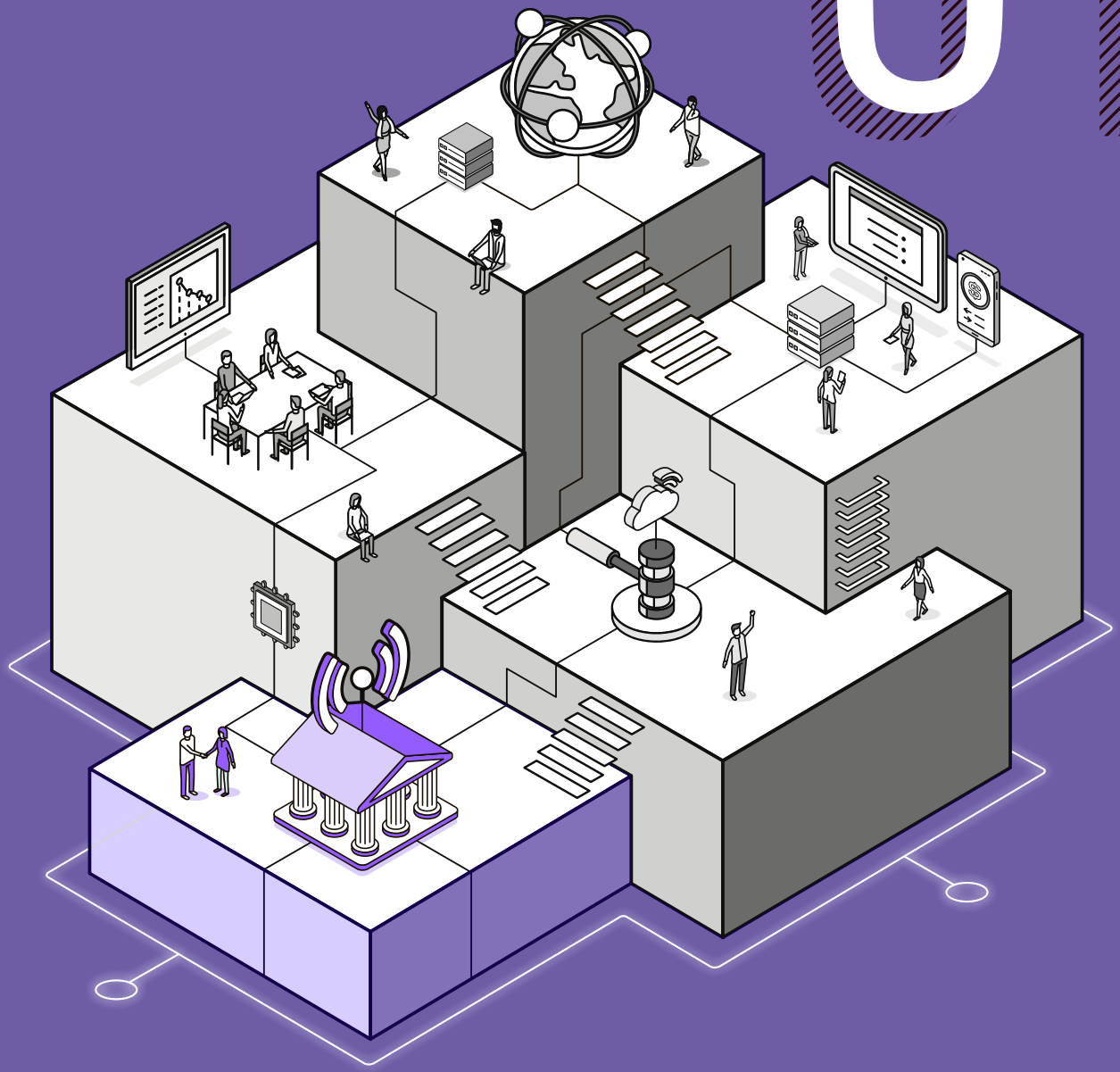
ABOVE ALL, IT SEEKS TO HIGHLIGHT THE KEY MESSAGES FOR THE SUCCESS OF A DIGITAL TRANSFORMATION:



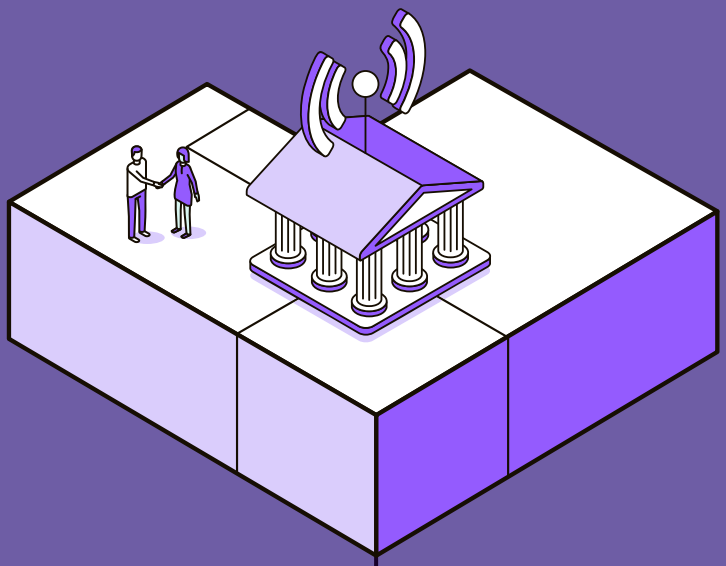
1. Holistic vision, through a 360-degree strategy
2. Extensive supporting regulatory framework
3. Acquiring the essential human talent for the transformation
4. Managing change
5. Identifying common components, opportunities for reusability and cross-cutting standardization
6. Reformulating administrative processes to make them digital and citizen-focused

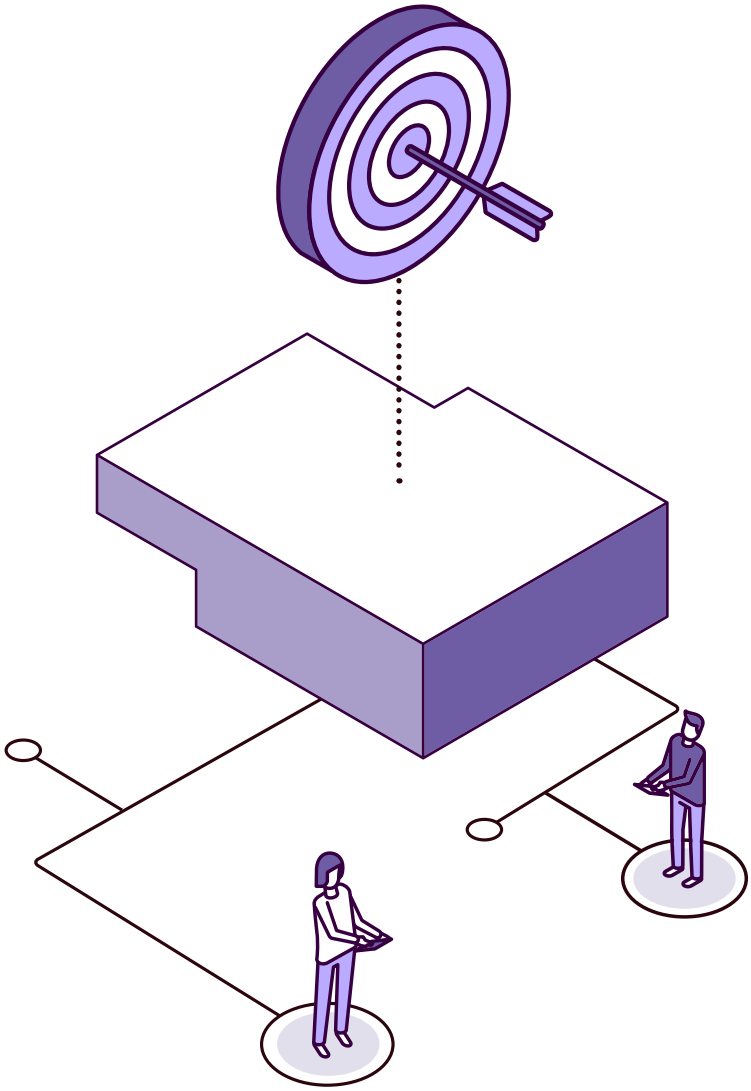
CHAPTER

01



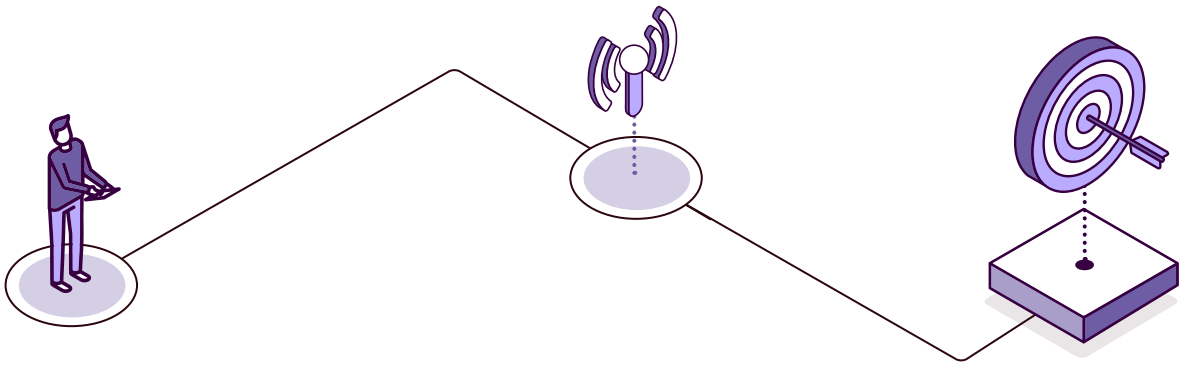
Governance and institutional framework





1.0

Introduction



Government digital transformation involves not only great opportunities but also challenges that must be faced from the outset.

This process must

- generate the necessary synergies within the government to take advantage of the intellectual capital existing in different institutions.
- take advantage of the efforts and resources available.
- design a common strategy for digital transformation based on ICTs and focused on the provision of public services with the citizen at the center[4].
- involve decision-making bodies at the highest level.
- appropriately regulate the governance structure and institutional framework for digital transformation.

---

4. This makes it necessary to work on all the elements that make up the digital transformation strategy together because on many occasions it is tempting to establish a digital agenda, which is composed exclusively of strategic objectives, and expect it to behave like a real strategy, that leads to results. However, this is not possible because, in order to achieve results, it is necessary to establish a digital agenda, which includes the objectives to be achieved and how to measure them, and in turn a road map (i.e., how to achieve those objectives; what projects, programs, and actions to carry out; and in what order and dependencies to achieve them). Moreover, this strategy must provide the necessary enablers for the digital agenda and the road map, as the main elements of the strategy, to be developed successfully. These enablers, at a minimum, are composed of a technology strategy, a procurement plan, a communications plan, a cybersecurity plan, a risk management plan, and a monitoring plan, and all of them, together, constitute the digital transformation strategy.

- involve not only the IT units but also the administrative units that provide the government's general and sectorial knowledge that are key to transformation;
- include all stakeholders and professionals from the public and private sectors, so that they are aligned and feel part of the digital transformation.

Governance requires an organizational structure, at the highest level, to drive and coordinate the necessary actions and drive the overall digital transformation of the various facets of information and communications technology policy across government. This body should operate with a high level of independence (organizational and functional) vis-à-vis the actors involved in the ICT field in the government of the state in question. In this way, independence and coresponsibility in the government's digital transformation strategy is sought. Likewise, an appropriate legal framework must be regulated to establish its composition, its functions and responsibilities, its relationship model (institutionalism), its form of cooperation, and the results of its operation.

The governance model should include

- a national governance body, also called a digital transformation lead institution, to lead the oversight of the government's overall digital transformation strategy;
- sectoral governance bodies responsible for ensuring that their digital transformation plans are aligned with the national governance strategy, but tailored to the needs of the sector in question;
- interdisciplinary working groups, made up of government experts, that will make technical decisions on infrastructures and technological tools.

This organizational structure of collegiate bodies should be supported by

- the existence of figures such as president, vice president, and secretary for each governance body, or similar profiles representing the top management;
- internal operating rules, also regulated and establishing the relationship model, meetings, deliverables, and other documentation to be prepared;
- an operating model based on meetings such as plenary sessions, strategic commissions, sectoral commissions, and meetings of technical groups of experts, among others.

This relationship model would constitute the institutional framework for digital transformation. It is therefore a series of relationships both within the government, and external parties including the private sector, industry associations, and other key players.

The governance model, therefore, has to be designed taking into account

- both the interests that are to the entire public administration, as well as their specificities of each particular sector;

- the inter-institutional relationships within government, as well as the necessary connections with technological partners, professional associations, and the private sector in general, both for the cross-government and sector-specific dimensions.

The success of digital transformation of government depends on the participation of all stakeholders, enabling a system of multidirectional communication and coordination. This also applies to the citizen, whose role places him or her at the center of the design of public policy and service delivery. Today's increasingly digital society expects public institutions to make efficient use of resources and to rely on technologies to provide public services in an efficient, effective, and reliable manner and under a paradigm of economic rationality and sustainability in; in short, citizens expects, efficient, collaborative, and expert governance to lead this strategy, with a clear focus on results.

Governance and institutional frameworks must take into consideration all the domains that support the public sector:

- **Business architecture plan,** including strategy, organization (governance and its relationship model), public sector capabilities, development of the regulatory framework, and key processes that achieve the desired capabilities (i.e., the different sectoral businesses that constitute it and their associated processes, both cross-cutting and sectoral).

- **Information architecture plan**, describing the organization of data, information, and, nowadays, knowledge, thanks to AI. This includes the description of the organization of data and data management systems (i.e., the applications that will make use of them). There is also a need for data governance, policies, processes, and procedures to define, design, operate, and manage the master data of the public sector, the national and local government levels, always also considering the different sectors.

- **Information systems or applications architecture plan,** which makes up the catalog of applications that support the add space after comma,services, or products that support the public sector.

- **Technological architecture plan,** which describes the technological decisions at the hardware equipment level, which software solutions make up the infrastructure, and the technological tools that support public services, public information, and applications used by public agencies and administrations. IT infrastructure, network equipment, storage, computing, databases, middleware, horizontal platforms, processes, and standards are determined.

This governing body should establish a public-private dialogue so that investments and acquisitions of supplies and services are efficient and generate economies of scale. This relationship model facilitates the participation of the private sector in the design and implementation of proposed measures and allows the government to take advantage of the private sector's knowledge and capacity for innovation.

The lead institution must lead this strategy and dialogue and must implement an appropriate management model adapted to its scope. This lead institution must have the following:

- A governance and institutional model that allows for centralized coresponsibility in common horizontal technological tools and instruments.

- Clear digital transformation objectives and a results orientation that allows the progressive and agile achievement of these (i.e., a digital transformation strategy that includes not only the digital agenda but also the road map). All this must be complemented with a measurement and monitoring process that allows the achievement of the objectives to be assessed.

- A global cross-cutting vision of technological needs, as well as sector-specific needs to determine the scope of any project in which it can participate or contribute not only investment but also technological innovation. The aim is to develop tools once and reuse them whenever possible.

- A global procurement strategy, taking into account the technological strategy that has been defined, establishing a procurement procedure that regulates services and supplies in a way that respects the objectives of the common strategy, taking into account the particularities of the specific sectors.

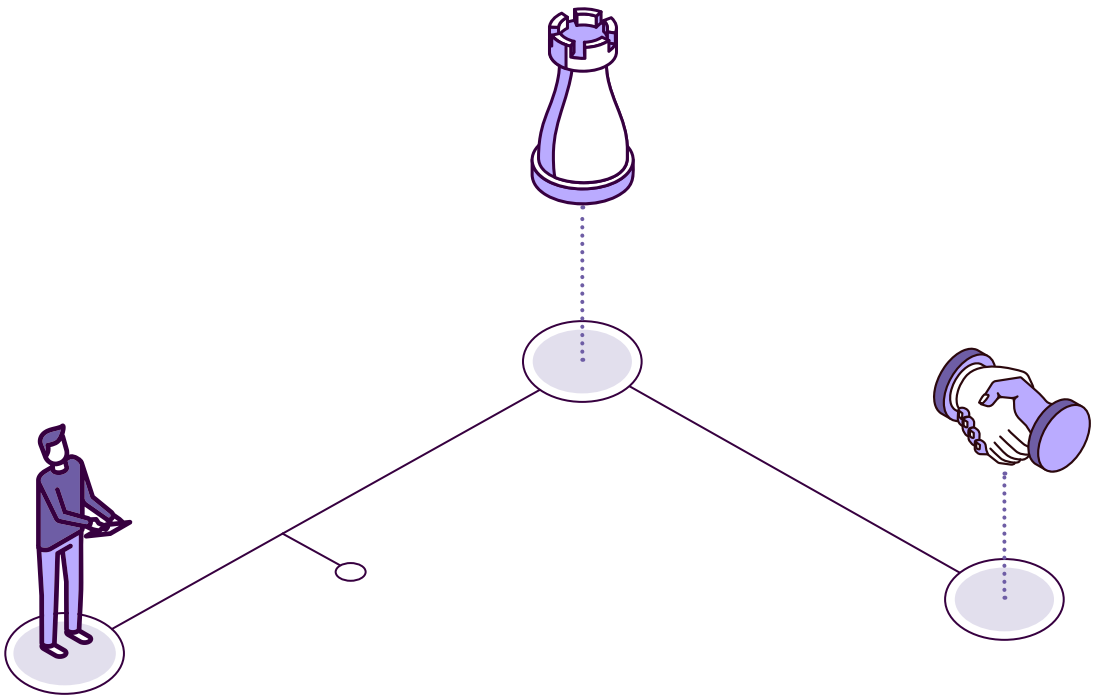
- A communication plan that informs all stakeholders of the progress of the strategy, as well as of new considerations to be taken into account. One of the fundamental aspects for the reuse of common services is to ensure their adequate dissemination.

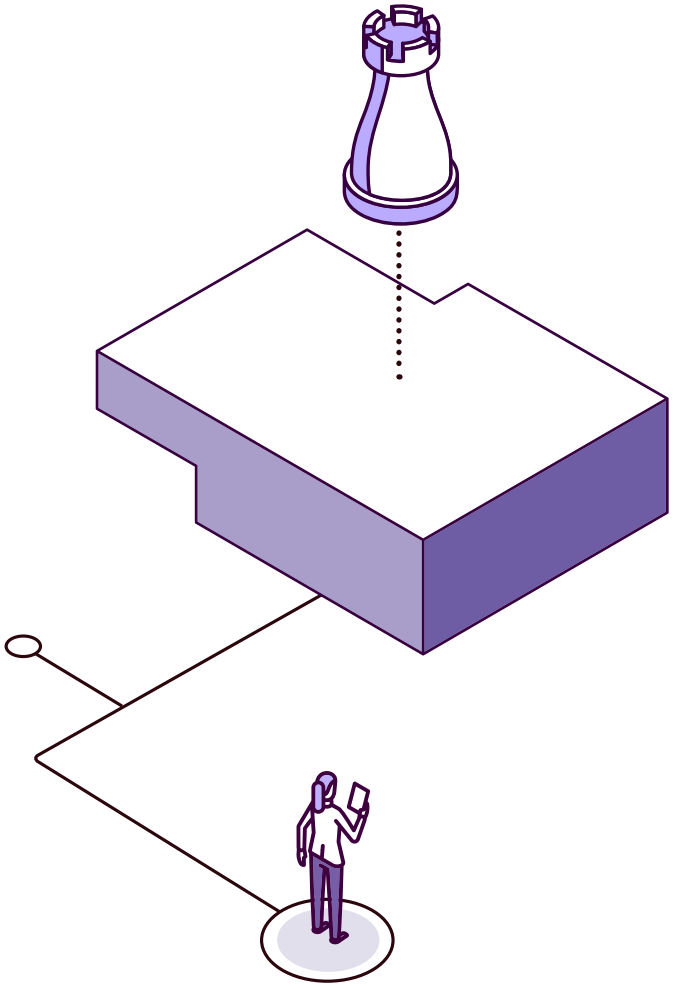
- A cybersecurity plan in all its dimensions that guarantees the implementation of a digital transformation where technology plays a predominant role and where security is taken into account from an organizational, regulatory, technological, and training point of view.

- Related to the above, a risk management plan that takes into account in a preventive and proactive way all the issues that may pose a threat to the plan, and whose materialization is a risk to be managed.

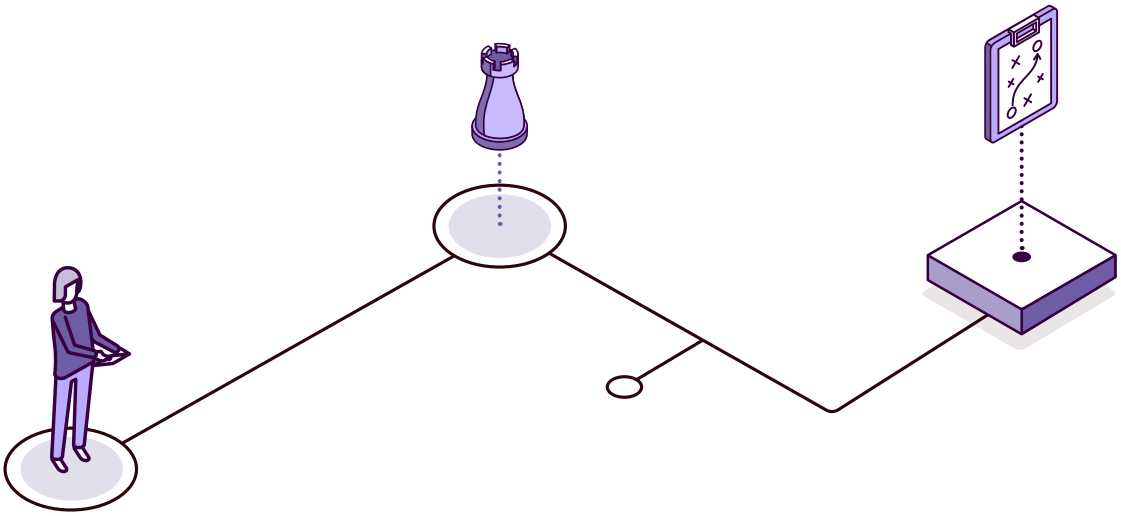
- Monitoring of the transformation strategy, which will be the tool to anticipate and manage any deviations that may arise during its execution.

- Finally, and with the dual objective of offering quality services and not "dying of success," it is extremely important to establish a good operational management model. In this regard, demand management processes, architecture, portfolio, and operation of digital services must be coordinated between the governing body of the digital transformation and the vertical sectors.





1.1 Digital transformation strategy



The national digital transformation strategy is the articulating element that defines the path toward a digital state. It sets out a holistic vision that encompasses not only the government and the various public institutions at all levels of government, but also relations with citizens, the private sector, academia and the nonprofit sector. In the end, the transformation strategy has to establish what is to be achieved, how to achieve it, and how to manage it from a communication, risk, and procurement point of view.

Normally, we talk about electronic or digital administration, about digital transformation, but are there different levels or states in relation to what an entity provides in its relations with citizens?

This paper argues that not all types of relationships are the same and that it is a problem to use the same name for different stages of progress in the digital transformation, This is a problem because in many cases the differences in the different types of relationships, which are decisive in terms of administrative efficiency and citizen perception, are lost.

Electronic administration

Interoperable administration

Automatic administration

Proactive management

ELECTRONIC ADMINISTRATION

Nowadays, what a citizen expects in relation to a public institution is to be able to carry out procedures electronically, from home, without the need to do anything through paper or in person. That is the minimum expected by a citizen who is used to being on social networks, exchanging information through WhatsApp, or making video calls through Skype.

In this type of relationship with public entities, in general, the steps of the procedures are more or less the same as those that were carried out on paper, but through electronic means, without the need to work with original documents or physical delivery to public offices.

For example, under this scheme, a citizen could request a subscription to the sports facilities of a municipality by following these steps:

- Enter the website of the municipality.
- Locate the procedure.
- Identify yourself electronically.
- Fill in all the information on a form, including scanned documents to obtain discounts for example, because of a disability that the user has.
- With the information and documentation complete, send this application to the municipal administration.
- The application is processed through the work of an official, who in many cases sends the bill for the sports activity card by email.
- The citizen can print the bill, go to the bank, and make the payment.
- Once the proof of payment made is obtained, the citizen can send it via email or through a web form to the municipality.

The officer reprocesses and verifies that the payment has arrived correctly to the municipality's account.

A card is issued to allow the citizen to use the sports facilities, which in many cases is sent by mail.

Public entities, in many cases, enjoy a monopoly regime: to obtain a card for access to the municipality's sports facilities, the citizen cannot move to another municipality; he must go to the one where he is registered. This is not always the case in the private sector—for example, with a bank: if an individual does not like his bank or if he is obliged to carry out paper or face-to-face procedures, he can change entity.

This lack of competition means that, on many occasions, public bodies do not provide this electronic service and that in some cases paper-based and face-to-face procedures are required. This is a serious problem citizens with higher expectations.

INTEROPERABLE ADMINISTRATION

Almost all countries have a regulation indicating that documentation already in the possession of public institutions or generated by one of them should not be requested of citizens, but almost all countries systematically fail to comply with it.

An interoperable administration addresses this legal requirement. Continuing with the same case above, an interoperable procedure does not require the citizen to present the document, not even scanned, that proves his disability, to get a discount. By simply marking that he/she has this condition, the civil servant can, through the interoperability of public entities, obtain these documents, data, or certificates, which will be incorporated into the administrative file, without the need for the citizen to supply them.

The rest of the steps stay the same; the only difference is that the documents are not submitted by the citizen but are incorporated into the file through requests between public entities through interoperability.

This not only has advantages in terms of improving the citizen's perception, but also others, such as the agility of the procedures, since the interoperability platforms normally return the data or certificate immediately and eliminate any possibility of fraud: it is the Ministry of Social Development itself that certifies that a citizen is disabled there is no way he or she could have forged a paper or its scanned copy.

AUTOMATIC ADMINISTRATION

It is even more interesting to reengineer procedures and take advantage of the new possibilities for automatic processing, which entails a very significant improvement in the efficiency of public entities and citizen service.

Continuing with the previous case, if the administration is not electronic but automatic, the process would have the following steps:

- The citizen who wishes to obtain the annual season ticket for sports facilities will go again to the website of the municipality in question.
- The citizen will locate the procedure, but in this case the only thing he/she will have to do is to identify him/herself to initiate it. He/she does not have to do anything else.
- As soon as the citizen identifies himself a national identification document or equivalent and makes the request, the information system will check that he s in fact a resident of the city and if he has any disability, since—thanks to the interoperability platform—this data is available so that those public institutions can consult it in automatically. As the data exchange is automatic, there is no need for the intervention of a public official. As the certificate has metadata, the information system can process it automatically, calculating the fee to be paid by the citizen.
- The system is connected to the payment gateway of the bank contracted by the municipality to allow the payment to be made immediately through the internet, under conditions equivalent to e-commerce.

When the payment is made, the information system sends a document with a two-dimensional code or a csv code (secure verification code), which can be printed out. This is also sent to the cell phone, in *passbook* format, so that the citizen can integrate it directly into his or her mobile device, if desired.

The two-dimensional csv or *passbook* code can be checked by means of a simple cell phone that the local municipal employee has at the sports facility and which indicates whether the subscription is active or not.

Under this model, small municipalities with problems establishing internet connection lines and installing in sports facilities are spared the need for this infrastructure and only need a low-end smartphone in each of the venues to check the validity of the subscriptions. This also leads to great savings for public entities, since no official has to make calculations or manage citizens' requests. Also, more importantly, citizens are more satisfied, because the public entities collect the information they need for the procedure among themselves and process it automatically.

PROACTIVE ADMINISTRATION

A further step in efficiency and citizen service is proactive administration. In many cases, it is not even necessary to wait for the citizen to request an action, a service, or a procedure. The **result can be sent directly to the citizen, proactively.**

In these cases, special care must be taken with the protection of personal data and control of the process by citizens, but being scrupulous with these fundamental rights and facilitating proactive delivery is compatible.

For example, in the previous case, if the citizen reports a change of address that involves a change of municipality, he/she can be asked if related procedures are authorized. If he/she does so, the card for the use of sports facilities can be sent directly to his/her email or cell phone without the need to request it. By simply paying the stipulated amount at the bank, he/she will get the card without having to do anything else.

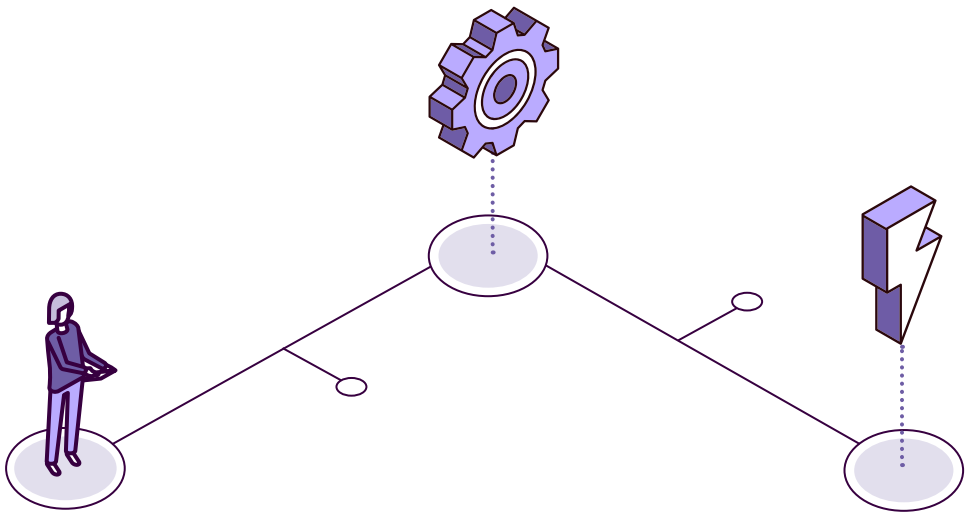
There are many examples. Consider, for example, the license to use public land for a bar on the seafront:

Instead of the employer having to submit the application every year, the competent public body collects the information automatically.

A for the license fee (if any) is made.

The automatic renewal is sent to the company without having to do any paperwork. The employer simply pays the fee or confirms on the website that he/she agrees with the renewal. If the service is free of charge, the license is automatically renewed.

These examples show that public entities can, on many occasions, carry out proactive procedures that allow them to save a great deal of money, as there are no man-hours involved, and even the tasks related to attending to the citizen's request are eliminated. But, above all, this means a radical improvement in the perception of the service by citizens and companies, which in turn enhances the image of the institutions and citizens' trust in them.



Of course, digital transformation strategies are entirely black and white. In other words, when a transformation strategy is established at the national level, or for a large sector, it is most likely that not all the actions will be aimed, for example, at e-administration or proactive administration. It is most likely that, depending on the degree of maturity of each party, each service, or each area, the progress that can be made, and therefore the objectives included in the strategy, will be different.

What is clear is that each successive strategy must continue the achievements of the previous one and include new goals that move increasingly toward excellence in the provision of digital services to citizens.

In addition, it is very important to always maintain a holistic vision of digital transformation, as well as excellent coordination with all stakeholders. At the very least, the leading institution for digital transformation in each country must ensure excellent coordination with the different sectoral institutions,, especially to prevent the approach to digitalization from being partial and fragmented at the project level, which causes two main problems:

- **Duplications:** these occur, for example, when a strategy is created individually for e-health, another for e-procurement, another for municipality X, and yet another for the digitization of the administration in the state, which implies repeating a large number of efforts that are common in many cases, so that resources end up being allocated inefficiently.

- **Incompatible results:** this problem occurs when synergies are not exploited. For example, the following cases are not uncommon:

    - The digital transformation of justice is incompatible with the administrative records used in the rest of government.

    - The electronic identification of the citizen cannot be used in both, the public and the private sector.

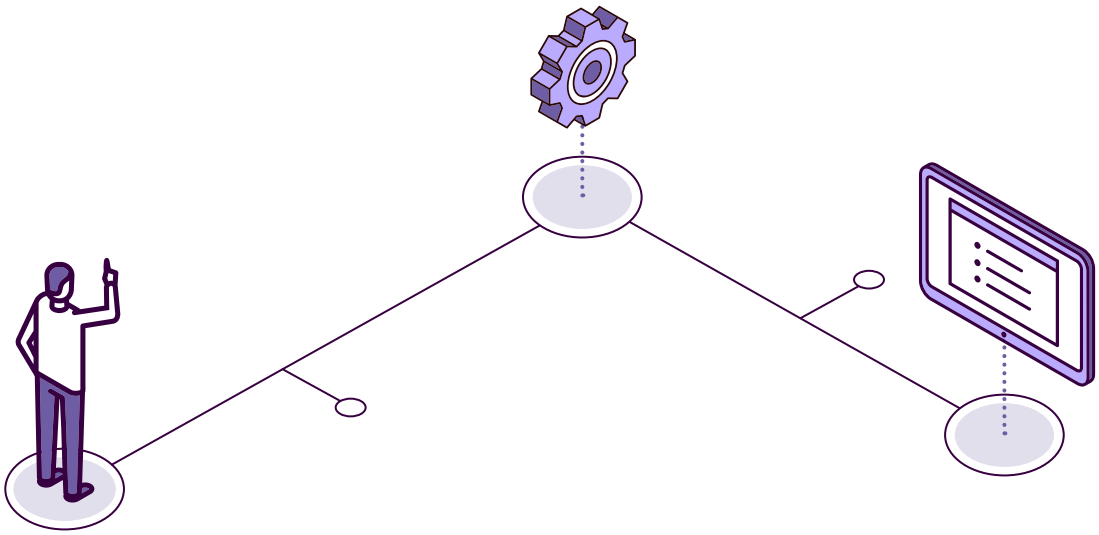
    - The information system of a municipality is incompatible with that of a neighboring municipality and does not allow the necessary information to be exchanged.

In view of the above, it is recommended to have a holistic country model. It is important to advocate for a single vision, based on broadly applicable principles and clear rules of that allow for scalability and sustainability. There should be guidelines that promote the compatibility of all the elements of the system. Based on the holistic model and associated strategy, sectoral strategies can be defined that provide greater detail and facilitate adaptation for each specific context.

ACHIEVING A HOLISTIC APPROACH—A TRUE DIGITAL TRANSFORMATION OF THE COUNTRY—REQUIRES THE PARTICIPATION OF ALL. THEREFORE, IT IS NECESSARY TO CREATE GOVERNANCE STRUCTURES WHERE THEY DO NOT EXIST AND TO INVITE ALL STAKEHOLDERS (PUBLIC INSTITUTIONS, CITIZENS, PRIVATE SECTOR, ACADEMIA, ETC.) TO PARTICIPATE IN THE DEVELOPMENT, IMPLEMENTATION, AND UPDATING OF THE STRATEGY.

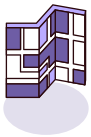
Likewise, there must be someone who coordinates and leads the strategy and is accountable, as it will be difficult for these roles to be distributed. It would be impossible to think that each sectoral area is going to create its own digital transformation strategy and that, when they are all put together, they will be aligned and share interests. Moreover, who would be in charge of unifying criteria and scopes, and making common services and components available? This is where the digital transformation governing body becomes especially relevant: not only to provide common technological components but also to bring coherence, and uniformity, to sectoral strategies with a view to achieving a single vision for the country.

On the other hand, it is common for strategies to become declarations of intent or documents that never grow beyond: the written word. To achieve results, one must always act with ambition but, at the same time, with a strong sense of reality. It is essential for the strategy to be accompanied by documents or elements that detail the operational plans, as well as the monitoring plan, in order to keep track of performance, make necessary adjustments, and orient strategies towards results.



A complete **digital transformation strategy** must include at least the following:

Digital agenda: establishing the objectives to be achieved, as well as the metrics associated with them, making it possible to measure success.

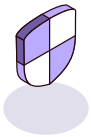


Road map: a detailed plan of all the necessary actions to be carried out to achieve the objectives, through programs and projects—in other words, how the objectives set by the agenda are to be achieved, what actions are to be carried out, and in what chronological order.

Technological strategy: to unify the technological criteria and the principles with which the different solutions will be built to provide a technological response.

Procurement plan: to plan in parallel, and with a joint vision to the road map, not only purchases, but also procurement of talent or personnel.

Communication plan: if the strategy is not communicated, it does not exist. A strategy is much more than paper. It is a feeling of achievement of objectives by those involved. To achieve this, everyone must be fully informed at all times.



Cybersecurity plan: to ensure that digital services will have the appropriate levels of protection, since today they are one of the most important assets that government must protect.

Risk plan: every strategy, especially the more ambitious ones is full of risks, which must be managed in order to avoid them, mitigate them, or accept them, each in its proper measure. However, to prevent the materialization of any risk from jeopardizing the strategy, it is essential to draw up a management plan.

Monitoring plan: what is not measured cannot be improved, and by measuring progress it is possible to determine whether corrective measures are needed in time to ensure the achievement of the objectives set out in the digital agenda.

All these elements will be detailed in the following sections of the document.

1.1.1 DIGITAL AGENDA AND ROAD MAP

It is common that, faced with a challenge as important as the digital transformation of a country, those responsible for carrying it out wonder about the best way to do it and the steps to follow, Furthermore, it is common to have doubts about preconditions or issues that must be addressed before others.

There are two levels in relation to the sequences and actions to be taken for digital transformation. On the one hand, from a macro point of view, there are six main components to consider that are essential to any successful digital transformation strategy:

1. Strategy itself, including digital agenda and road map, as well as plans for procurement, communication, cybersecurity, etc.
2. Governance and institutional framework
3. Regulatory framework
4. Digital talent and change management
5. Technological tools to facilitate digital transformation
6. Definition of the processes and services in a digital government

It is also necessary to consider the sequence of specific actions for the implementation of technological tools and services, the associated regulations, or the governance of these, since, in many cases, there are departments that consider that it is better to implement some before others, and in some cases doing so is a requirement.

In many cases, digital transformation has been based on regulatory changes. In other cases, the focus has been on technology. Similarly, providing the country with a unit responsible for digital transformation and the governance of such transformation is a path that has been followed in some countries, although sometimes this point is the one where the least effort has been made.

A digital agenda sets out the objectives for progress toward a digital state. This agenda, together with the road map, make up the systemic instrument for the design of the steps to be followed, as well as the preliminary requirements to be taken into account.

The development of a digital agenda at the state level consists of a series of objectives aligned with the political and economic strategy of the country and must be adapted to the social circumstances at a given time. This agenda must take into account the results of previous strategic plans and projects to allow the development of a new digital agenda in a new time frame, which will give continuity to those strategies that have been implemented and whose results have been positive, as well as adoption of new measures. It is important to consider the lessons learned based on strategic objectives, the lines of action and the plans and projects that were implemented. For all this, the indicators are the analytical basis for assessing the effectiveness of the measures of a digital agenda.

A country's digital agenda usually has a medium-term time horizon and is subject to political cycles. It has objectives marked by the achievement of sustainable economic and social benefits and focused on technology as a dynamic tool. The objectives of the agenda (also referred to as pillars or dimensions) usually encompass the issues that are considered a priority for the economic and social development of the country, such as the following:

- Improving digital communications infrastructures and internet access for citizens, ensuring digital connectivity is the basis for the fight against the digital divide.
- The dynamization of a digital economy that favors the development, growth, and competitiveness of companies at the national and international level.
- The digitization of the public administration and public services as an example of technological renovation and an image of progress toward digital services for a digital society.
- The growing and necessary guarantee of cybersecurity and trust in digital media. Cybersecurity is understood as a requirement for digital transformation.
- The boost in the use of ICT in industries, as well as the incorporation of R&D&I, data analytics, and disruptive technologies (AI, IoT, *big data, blockchain, machine learning*, etc.).
- Promoting the digitalization of priority productive sectors, through sector transformation projects.

- The incorporation of the concept of data analytics or data economics, so that *big data* provides a competitive advantage when it comes to offering opportunities for business and economic growth. AI is a powerful tool in this regard.

- Digital literacy and training of new professionals in the highest-priority ICT subsectors.

- The development and publication of legal, ethical, and moral codes that guarantee the rights of citizens in a new digital model.

The digital should also contemplate the following:

- Analysis of the current situation: social, economic, productive, geopolitical, business, and other perspectives.

- Identification of the social agenda on which to focus efforts: What does the digital society expect from the State? And from public services?

- Sectoral areas on which to focus lines of work: health, transportation, justice, tourism, labor, SMEs, AI development, and others.

- Identification of the highest-priority projects.

- International strategies and commitments that involve specific lines of action such as the Sustainable Development Goals of the United Nations 2030 Agenda, environmental commitments, and bilateral agreements, among others.

With this framework for action, the digital agenda, beyond what its name may imply in terms of technology, is aimed at driving economic growth by considering issues such as sustainability, inclusion and equality, and above all making use of the synergies of the digital and environmental transitions. It is about offering the opportunities that digital transformation presents both for society and for the public or private sector. All this must be done while guaranteeing transparency and cybersecurity, which allow respect for the values recognized by the constitution of each country and the protection of individual and collective rights.

Once a government strategy is in place, the digital agenda is therefore articulated in a series of strategic axes that are decided on the basis of the results of previous plans and driven by the current context. Each axis is then developed with a series of measures designed to achieve it, as well as the planned investment. Each measure or objective has a detailed justification to enable implementation

within each axis. In addition, indicators must be defined that are associated with the objectives in order to be able to monitor throughout the life of the agenda whether it is on schedule and, at the end of its execution, to be able to evaluate whether or not the objectives can be considered achieved.

A fairly widespread framework on the characteristics that the objectives to be defined should have is that of SMART objectives. These characteristics are:

- ***Specific***
- ***Measurable***
- ***Achievable***
- ***Relevant***
- ***Time-bound***

Moreover, recently, and depending on the context, we are starting to hear that the objectives have to be SMARTE—that is, adding a final characteristic:

- ***Ecologic***

The definition of these indicators a fundamental step in the development of a digital agenda, as well as the associated measurement and monitoring system. It is this measurement system that will make it possible to assess the progress of the measures and the effectiveness of the plans and projects implemented to achieve them.

The indicators must be aligned with the measures, the axes, and the digital agenda. They can be quantitative variables whose purpose is to provide information about the degree of fulfillment of a goal.

In order to establish the number of indicators to be used, it is important to

- cover significant aspects of performance.
- privilege the most relevant objectives of the institution.
- ensure that the amount of information they provide does not exceed the analytical capacity of those who use them.

AT LEAST TWO OR THREE INDICATORS PER DIGITAL AGENDA MEASURE ARE NEEDED.

Finally, it is important to consider the relevant dimensions of the performance of the indicators. As mentioned above, it is essential to quantify the impact that shows the effect produced on the economy, society, etc., as a consequence of the results of the actions implemented. Thus, the following should be considered:

- **Impact:** The indicators should reflect the percentages of results obtained compared to those expected.
- **Effectiveness:** Degree of compliance with the objectives set (i.e., the extent to which the area, or the organization as a whole, is meeting its objectives, without necessarily considering the resources allocated for this purpose).
- **Efficiency:** The relationship between the physical output of a good or service and the inputs that were used to achieve that level of output.
- **Quality:** The organization's ability to respond quickly and directly to the needs of its users.
- **Budget performance:** An organization's ability to adequately mobilize financial resources to meet its objectives.

Generally, measures are included that contemplate the renewal or development of a new legal framework to cover the underlying digital transformation, as well as measures to reinforce certain areas with personal resources, digital training, or technological investments, or measures to improve cooperation and governance at the public and private levels and the necessary public-private collaboration. In short, governance, regulatory, organizational, strategic, and tactical measures are taken, leaving the more operational ones for development in the project plans that make up the road map.

As an example, the axis focused on the digital transformation of public administration could have indicators on the following:.

- simplification and automation of administrative processes and procedures.
- improvement of digital competencies.
- modernization of public services,

On the other hand, something very common and that should not occur is to confuse the digital agenda with the road map. On many occasions, unintentionally, due to confusion or semantic error, it is possible to hear both terms used to refer to different issues that should be separated:

- **The digital agenda** should establish the *objectives to be* achieved, as well as the **indicators** that will be used to measure the achievement of these objectives. For example::
  - "increase the use of digital health service".
- **The road map** establishes the sequencing or parallelism of the actions to be carried out to achieve the objectives. For example:
  - Providing medical patients with a digital identity.
  - Implementing a virtual assistant to assist users in digital processes.
  - Building a statistical and monitoring scorecard to establish corrective actions.

In other words, the definition of the objective is separated from the initiatives to be carried out to achieve it. Thus, the road map must establish the initiatives that respond to the objectives set and, at the same time, give an account of their timing. There will be occasions in which the different initiatives must be sequential; in others it will be possible to parallelize them; and in others the dependencies will draw a critical path between them, and it will be possible to intersperse them.

This document is based on the idea that all components must be subject to balanced progress. For the goal of a deep digital transformation of a country, all components have to be considered and acted upon, and if any of them is not managed properly, it will generate problems that will cause the digital transformation to not have all the capabilities it should have. Therefore, the country that is ambitious and intends to have a deep digital transformation has to be aware that it will have to take actions in these components.

Equally true is the fact that any of these components, individually, can have beneficial effects in advancing the country's digital transformation; thus, if a government, for example, enters into a minority and cannot bring about legislative reforms, it can make advances in digital transformation by implementing technology or improving governance. At some point, it may encounter legal limits that prevent

it from making all the advances that technology or governance would allow, and the changes cannot be implemented if the laws cannot be changed. The same example applies to the other combinations.

This means that any of the axes can be the main motor for driving digital transformation. If a country has an easier regulatory development, it should take advantage of that avenue without neglecting the rest. If a country can develop technological tools that favor transformation, it should not be paralyzed because the rest of the issues do not advance at the same pace. Governance can also be a powerful driver of digital transformation.

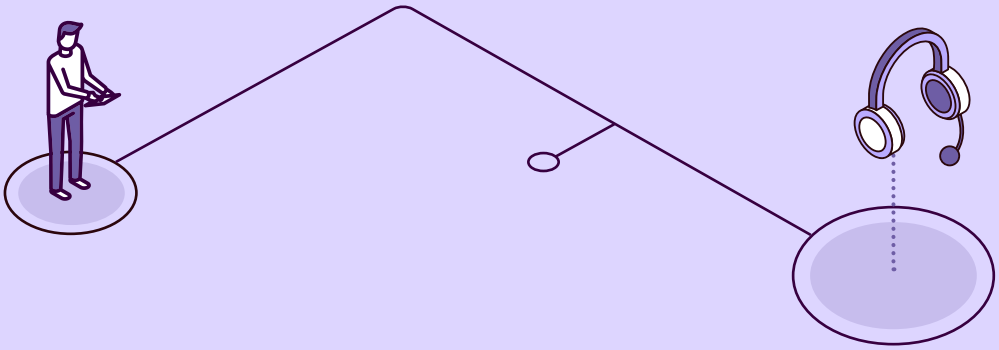
With regard to the specific components, something similar to the macro components is true: in general, most of them can be advanced independently, but ideally, to get the most out of them, there should be coherence and joint—or, in some cases, prior—progress in relation to other components.

For example, in terms of technological solutions for electronic signatures, ideally they should be accompanied by legal changes that provide legal certainty to the actors, and also by digital identity solutions, in order to have a coherent digital transformation project for the country. However, if there is no way to change regulations, or the digital identity project is paralyzed for some reason, it is always possible to achieve advances in electronic signatures—for example, on a voluntary basis, or to the point where there may be a legal or identification problem for the signer.

IN SUMMARY, PROGRESS CAN BE MADE IN ALL COMPONENTS, IDEALLY IN COORDINATION WITH THE REST, BUT OTHERWISE, ONE CAN TRY TO MAKE PROGRESS WITH EACH ONE IN PARTICULAR AS MUCH AS POSSIBLE, WITHOUT ANY POSSIBLE BLOCKAGES.

There are some exceptions to this general rule. For example, for an electronic file exchange system to make sense, the electronic file as such must exist. The components of an electronic file can change from project to project, but the idea is that an electronic file is not a chaotic collection of documents: it has a structure, data that accompanies the file and each of its documents, and standardization and security criteria, etc. All this makes up the electronic file, and if you don't have these elements in place, there is no point in starting to set up a file exchange system.

However, this is not usually the case; in general, projects are developed in a decoupled manner. This is not desireable. In reality digital transformation is an ecosystem of components. Although it is possible to move forward independently, the ideal is for there to be coherence, because in this way the digital transformation will live up to its potential.



STORIES

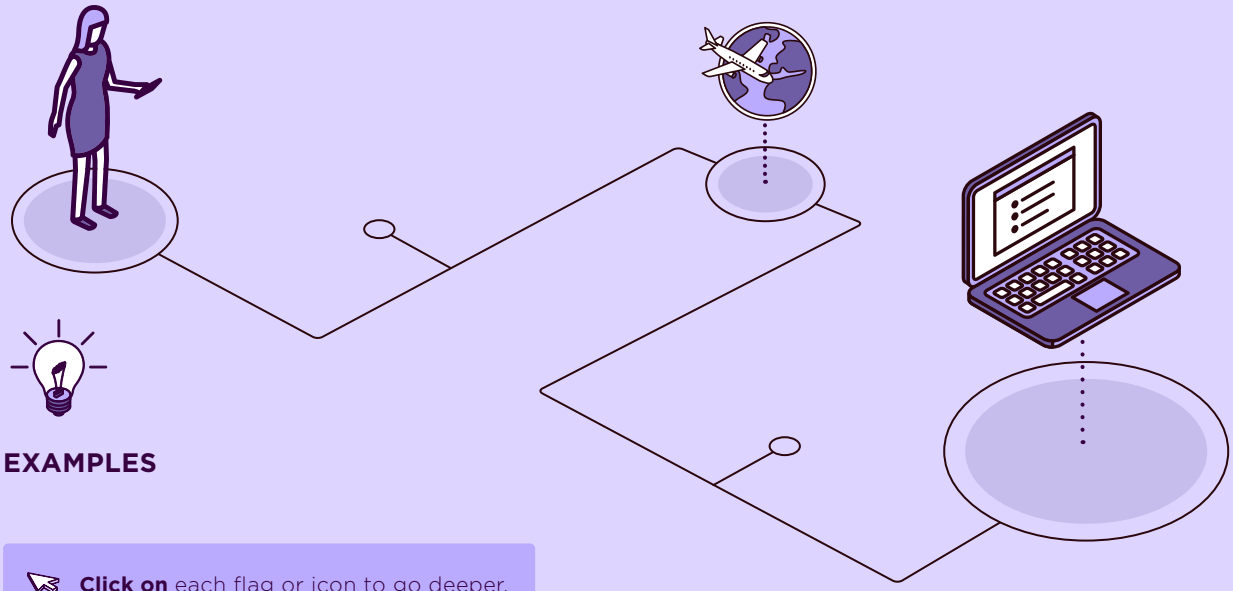
Fictitious anecdotes that showcase the concepts of this article from the perspective of different types of stakeholders

Mayor's advisor
Daniel

Daniel is interested in improving citizen service through ICT tools in the services provided by the municipality where he works, but there is no clear strategy, and he is afraid to face a blank piece of paper to propose the digital transformation of the city and make a mistake.

Citizen
Camilo

As a citizen, Camilo is overwhelmed by the management of user IDs and passwords he has, and he always forgets them. He has one for his bank, one for his electricity provider, and a few more for various public institutions. Camilo wonders how it is not possible for the private sector and the public sector to agree on a single national ID that can be used for all services.



EXAMPLES

Click on each flag or icon to go deeper.

Australia
Government Digital
Transformation Roadmap

Brazil
Estratégia de Governo
Digital 2020-2022

Chile
Desde una Agenda Digital a la
Transformación Digital

Denmark
A stronger and more secure digital
Denmark

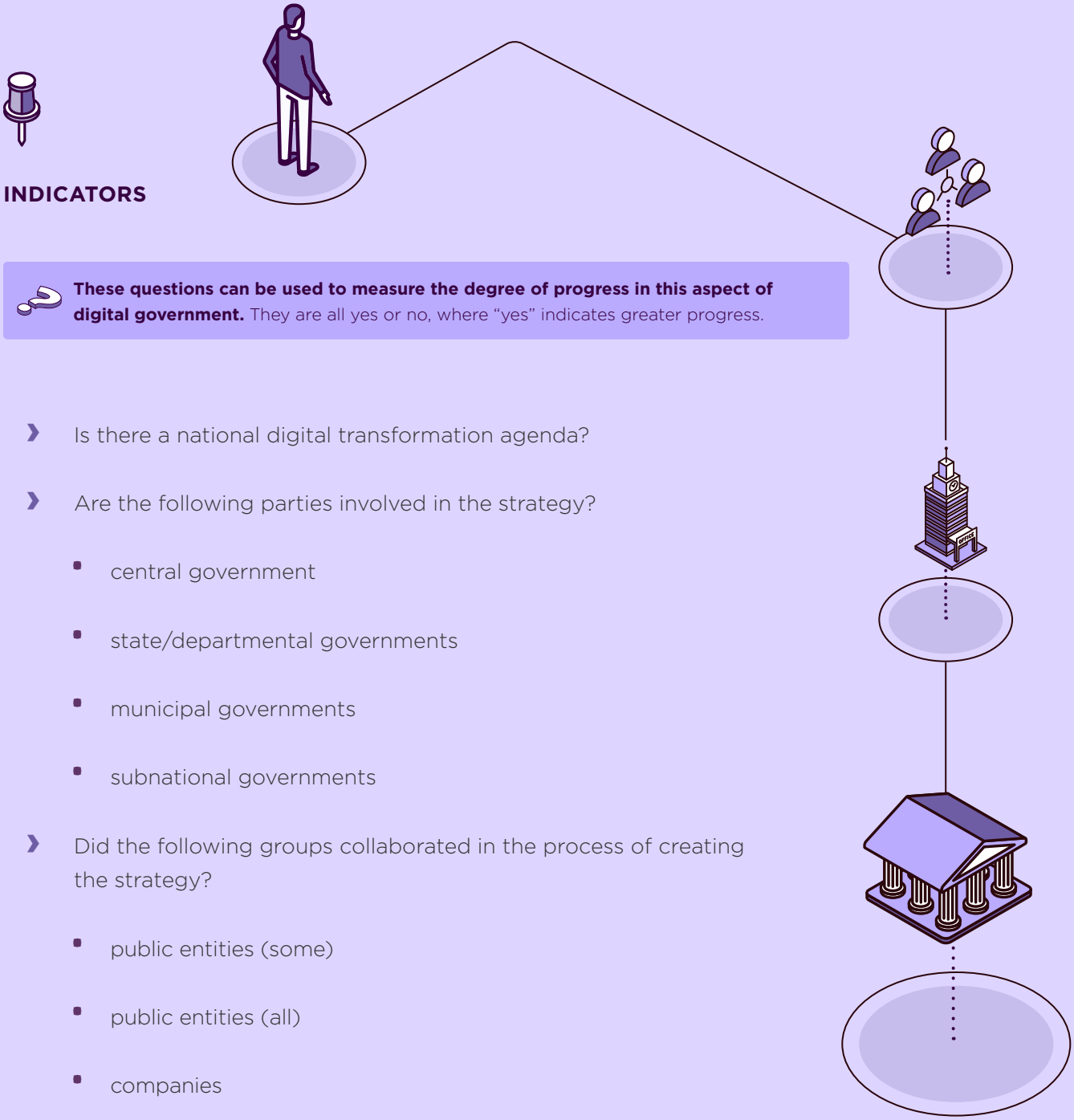
Spain
España Digital 2025

Estonia
Digital Agenda 2020 for Estonia

Portugal
Agenda Portugal Digital

Europe
La Década Digital de Europa

Uruguay
Agenda Uruguay Digital



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a national digital transformation agenda?
- Are the following parties involved in the strategy?
  - central government
  - state/departmental governments
  - municipal governments
  - subnational governments
- Did the following groups collaborated in the process of creating the strategy?
  - public entities (some)
  - public entities (all)
  - companies
  - unions
  - citizens
  - academic institutions

1.1.2 TECHNOLOGY STRATEGY

Countries face important challenges, such as the following:

- globalization
- the need to provide higher-quality public services with fewer resources
- to take care of the environment
- to be competitive in order to promote exports
- to attract foreign investment

Among the different tools available to a government to meet these challenges is digital transformation. This process promotes changes in the country's regulations and/or laws, the processes and ways in which administrative actions are carried out, and the technologies that facilitate administrative performance.

The digital transformation process must be supported by a technological strategy that serves as a reference for all the changes to be carried out by the government. When a country is determined to transform itself digitally, it usually entrusts an internal body with the definition, leadership, and governance of this transformation process. These plans are quite complex as they have to align different ministerial departments, each with its own special characteristic,, and make them all converge on the same transformation path with a series of milestones.

Exemplifying this:

- A government should identify a ministry or agency in the country as the lead entity.
- This governing body will be responsible for defining the strategy to be followed in the country's digital transformation process and the impact it will have on each of the ministerial departments.
- The different ministries—Justice, Employment, Health, Finance, Defense, etc.—will have to carry out an internal transformation program in line with the milestones set by the governing body. It

is important that this transformation is aligned with the milestones set by the lead institution, since the value sought through digital transformation often requires the digital services of several agencies. For example, in order to process a worker's sick leave, it may be necessary to do the following: (i) start on the website of the Ministry of Labor; (ii) Launch a query from Ministry of Labor's systems to the Ministry of Health; (iii) in the event that everything is correct, send a communication to the Ministry of Finance to reduce the taxes owed by the employee during the sick leave. If any of the links in this chain fail, the value of digital transformation as perceived by the citizen and public institutions, will be greatly diminished.

To govern this whole process, it is necessary to articulate different actions in a technological strategy. The objective of this strategy is to provide carry out the technological initiatives necessary to meet the objectives set by the government.

HOW TO START ESTABLISHING A TECHNOLOGY STRATEGY?

The first step in defining the technology strategy is to identify the objectives set by the government, such as the following:

- Reducing healthcare waiting lists
- Modernizing the country's justice system
- Facilitating access to the labor market for disadvantaged groups

These objectives must be analyzed by the entity in charge of the digital transformation, so that it can develop the technological strategy that will support it.

All technology objectives must be oriented to the achievement of one or more government objectives. If during the identification phase of the technology objectives it becomes evident that one of them will not contribute anything to the achievement of the government's objectives, it should be automatically discarded.

Some examples of technological objectives may include the following:

- Eighty percent of public services for other administrations, citizens, or companies must be available electronically in the next three years.
- The use of digital identity will be mandatory by 2025 for all companies and public administrations, and will be actively promoted among all citizens.
- All services offered by public administrations must comply with accessibility standards in order to facilitate access to groups with disabilities.

These general objectives must be transferred to each ministerial department in order to adapt them and incorporate them into their corresponding strategic plans. These specific plans must take into account the reality and complexity of each of the departments, as well as adapt to the specificity of their field. Although each department will have to do its own adaptation of the technological strategy, it should converge in certain milestones that will allow the whole government to advance in digital transformation in a coherent way.

HOW TO MEASURE THE PROGRESS OF THE STRATEGY?

The indicators selected are particularly important, since they must be used throughout the life of the technology strategy to verify that the technological actions are providing an adequate response to the actions defined by the overall digital transformation strategy. These constant measurements will help to ensure that monitoring is effective and, therefore, corrective actions can be taken. However, one should not make the mistake of only specifying end-goal indicators, as in this case unpleasant situations often arise when it is too late to redirect technological actions. For this reason, intermediate measurements are particularly important.

For example, if a metric is established to indicate whether or not a particular information system has been completed, the intermediate metrics would be the "percentage" of construction with which it is progressing, but this is an inaccurate and misleading metric—inaccurate because saying that a system is at 35 percent or 40 percent is usually quite relative, and misleading because the fact that the system is 100 percent built does not mean in any case that it is available to users. In fact, once built, it will have to go through technical testing, then acceptance testing, then performance testing, and finally production. In addition, a possible training period for users should be added, if necessary.

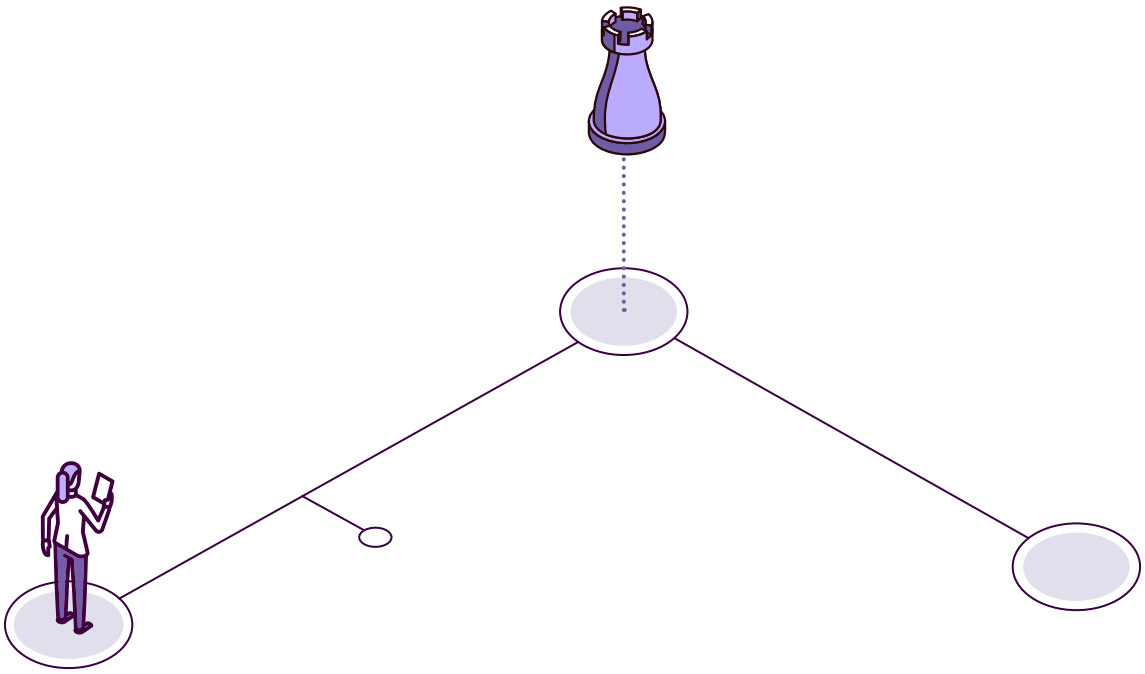
In this simple example, it would have been much more effective to use a milestone metric:

Milestone 1	**Milestone 2**	**Milestone 3**	**Milestone 4**
System built	Tests performed	System implemented	System being used

Thus, if each milestone is assigned to a point in time, it is much more accurate at the time of monitoring.

THE PRINCIPLES

A technology strategy is usually supported by the definition of principles, which are a basic governance tool. They are a set of guidelines that are maintained over time and inform and support the way in which the digital transformation is to be carried out. The definition of the principles facilitates the work of the lead institution, as it provides a general guideline for the different ministries and reduces conflicts and the need for oversight. In addition, on the part of ministry managers, the use of the principles greatly facilitates decision-making when dealing with different technological projects.



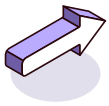
By way of example, some technological principles used in digital transformation processes are identified and will be developed below. These are merely indicative examples - the appropriate principals vary by context.

Open-source software shall be used

Buying products is preferable to making them.

Reuse whenever possible.

An agile development methodology will be chosen.



Use horizontal services whenever possible.

Public services must be accessible.

Services will always be provided on the premises of the public administrations themselves.

Teams will be encouraged to be made up of in-house and not outsourced personnel.

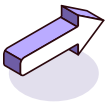
Open-source software shall be used

This principle states that the government will generally opt for open-source software when implementing a technological solution. This principle can have an important influence when approaching digital transformation, since any proprietary application or system will be discarded. In addition, it must be taken into account that, at present, many tools that are launched as open source software are bought by large technology corporations that tend to change the nature of the tool from open to proprietary.

Reuse whenever possible

This principle encourages all ministerial departments that are involved in digital transformation to try to reuse existing applications, systems, components, etc. This has two advantages:

- This principle encourages all ministerial departments that are involved in digital transformation to try to reuse existing applications, systems, components, etc. This has two advantages: (i) by used a proven component, the risks of using a new proprietary component (which has a stabilization phase in which errors will undoubtedly emerge), and of not meeting the planned schedule, are reduced. Governing bodies often create web portals that facilitate technology[5,6] transfer, as well as collaboration spaces that facilitate the collective design of technological tools.[7]



Use horizontal services whenever possible

The technological foundations of digital transformation are potentially the element that implies the most radical change of concept with respect to the status quo in most countries. Until now, the tendency in governments has been to promote technological development mainly in the vertical sense (i.e., within a single organization). However, digital transformation requires the addition of an important horizontal development: the establishment of tools that are generated from a central entity but serve a wide range of users, both institutional and individual, inside and outside the government. These tools have various names: horizontal services, cross-cutting services, common services, platform services.

Horizontal services (and all its synonyms) encompass the development, implementation, and operation of shared and reusable tools that offer a common functionality necessary for the completion of multiple procedures or the delivery of different services. These types of services allow for the leveraging of technology to achieve greater quality, efficiency, effectiveness, and transparency in public management. At the same time, they lead to a comprehensive improvement of the citizen's experience with public services by eliminating unnecessary procedures, reducing the amount of information requested from the citizen, and offering integrated and uniform interfaces.

---

5. Technology Transfer Center Public Administrations Spain, - https://administracionelectronica.gob.es/
6. Catalog of Transferable Applications in the Field of the Spanish Administration of Justice - https://www.cteaje.gob.es/cat%C3%A1logo-aplicaciones-transferibles
7. Forja CTT Spain - https://administracionelectronica.gob.es/pae_Home/pae_SolucionesCTT/pae_CTT_Forja_CTT.html

Horizontal services answer two challenging questions:

- Why duplicate a system in each institution when there can be one system that serves the entire government in all sectors?
- Why continue to do routine processes by hand when there is a system that can automate them?

Vertical digitizations can be done in specific projects that respond to the above questions. The problem is the scalability and sustainability of the system when it is a country-level project. It is possible to automate the input and output of information with citizens or companies in a process, such as taxation, for example. However, the question arises as to whether this is sustainable in the absence of horizontal services to facilitate communication between the government and citizens and businesses, or common document and electronic file services. Central governments generally have around two thousand procedures, or more. If for each of the two thousand procedures there were an information exchange system, would this be efficient for the government and easy to use for citizens and businesses? Horizontal services achieve this sustainability and scalability.

The objectives pursued through the use of horizontal services are the following:

- Improve customer service by reducing and simplifying transactions, offering services in a proactive manner, providing greater access and participation options, providing greater clarity and transparency, and acting with greater speed.
- Minimize time and money spent by public entities on tools that many entities can use by creating and/or managing them centrally and offering them free and openly.
- Maximize the efficiency of public entities by offering tools to automate routine processes.
- Depersonalize administrative management and, therefore, reduce corruption by programming the proper procedures in the automated processes.
- Filling institutional capacity gaps by providing, at little or no cost, advanced digital management tools to any entity that wants to adopt them.
- Minimize the risk of cyberattacks by creating standards and tools that protect public cyberspace.

Therefore, the tendency is to use common services whenever possible. For example, it is established as a principle that if a ministry has a time-stamping service that guarantees that data have existed and have not been modified since a specific moment in time, no other ministry will develop a similar system. The other ministries will make the necessary adaptations to be able to reuse this service and incorporate it into its systems. The provision of horizontal services poses challenges for the provider agency as it must ensure that it has the necessary capacity to cope with all the demand, ensure availability, provide support to the ministries that use it in the event of problems arising, etc.

Services will always be provided on the premises of the public administrations themselves

There is currently a strong trend to migrate services to the cloud. Establishing a principle of digital transformation makes it possible to homogenize the form of service provision and to mitigate possible future risks that may arise from uploading certain data or systems to a service provider that may operate outside the country itself or that is not obliged to comply with national data security regulations. Normally, this principle can be refined by leaving the door open so that applications can be uploaded to the cloud but not databases; development environments can be in the cloud, etc. In addition, and in line with the above principles, the governing body can promote the creation of a private cloud supported by all the country's ministries or a hybrid cloud supported by a public cloud, but controlled and governed by a single body.

Buying products is preferable to making them

This principle shows that there are some public administrations that prefer to adapt and/or parameterize a product rather than make it by other means. A lead institution may choose to reverse the principle and prefer to build the systems rather than purchase an existing product and adapt it. The typical example of customization is an enterprise resource planning (ERP) system such as SAP, which proprietary software. The use of SAP-type software makes it possible to customize and adapt the systems to suit the specifics of the public service to be implemented. Normally, it is possible to shorten the start-up time; support is available, usually for a fee; and risks are reduced since it is based on a product with experience in the market. The risks, however, are clear, as there is a dependency on the manufacturer and its product strategy. On the other hand, there is the possibility of going the other way: always having the product made by the governing body. This implies developing and maintaining with its own teams all the systems to be implemented in the digital transformation process.

An agile (or traditional) development methodology will be chosen

In the field of digital transformation, the speed with which you start delivering value to other administrations, citizens, and companies is very important. This is where *agile* methodologies come into play. These ways of working are based on collaborative work, constant communication, iterative work, and product deliveries every few months. The different services are delivered gradually, so that, for example, the service of payment of traffic fines carried out in an agile way would allow the citizen, in a first phase, to see if there is any fine; the second phase would make it possible to make the payment through a website; and in a third phase it would be possible to make a claim. In this way it is not necessary to wait until the whole system is complete, as in a traditional waterfall methodology, to be able to enjoy this service, even if only partially. Now, although the use of agile methodologies is often presented as a good option, public administrations are usually not very prepared for the *agile mindset.* The communication needs between those responsible for digital services and technicians are constant, and the difficulties of contracting as a service without a predefined scope rather than a "turnkey" service, etc., make it difficult to use these agile methodologies.

Public services must be accessible

Promoting accessibility, in particular for people with disabilities, must be an obligation, not only legal but also moral, of all public administrations. In order to ensure that no one is left behind and to prevent a person from being unable to use a certain digital service, for example, because of a visual or hearing impairment, solutions with the appropriate level of accessibility must be implemented in all public services and in a uniform manner in all ministerial departments. The governing body of the digital transformation process should be responsible for identifying the appropriate level of accessibility, as well as the national or international standards to be used as a guide.

Teams will be encouraged to be made up of in-house and not outsourced personnel

This principle is very much geared toward talent management. If this principle is followed, the different ministries will have to identify, hire, manage, and maintain the teams in charge of developing and maintaining the systems on which the digital transformation is based. Having its own team presents significant challenges, such as the time consumed in recruiting and hiring staff, ongoing staff training, etc., versus outsourcing it to a third party that can be productive "from day one."

However, outsourcing also presents problems, such as the fact that the knowledge "is outside the public administration," and, being in the hands of a company, there may be a captive client situation; the costs of outsourcing are also usually higher than in-house personnel, etc. Normally, a hybrid decision has to be made, so that a number of low-value functions are outsourced, while key profiles are provided through the public administrations' own personnel.

The principles outlined above are merely examples and are not intended to be prescriptive. It is important to emphasize that there are no good or bad principles; they are all relative. Whether a principle identifies that open source or proprietary software should be chosen will depend on the context in which the governing entity is carrying out the digital transformation initiative. What is essential is that they are adequately specified.

ESTABLISH THE STARTING SITUATION

Once the principles of the technology strategy have been established, the next step is to establish the starting situation. The initial state in the different areas such as health, defense, employment, or justice must be identified through indicators that model the current situation. The indicators must be related to the objectives of the technological strategy, so that their measurement allows information to be obtained on the state of fulfillment of the objective.

For example, in the area of the Ministry of Employment, an evaluation can be made to determine that 15 percent of the services are available for online consumption by other administrations, companies, or citizens. This data provides an initial state on which the necessary actions must be planned to achieve 80 percent of services available electronically within three years.

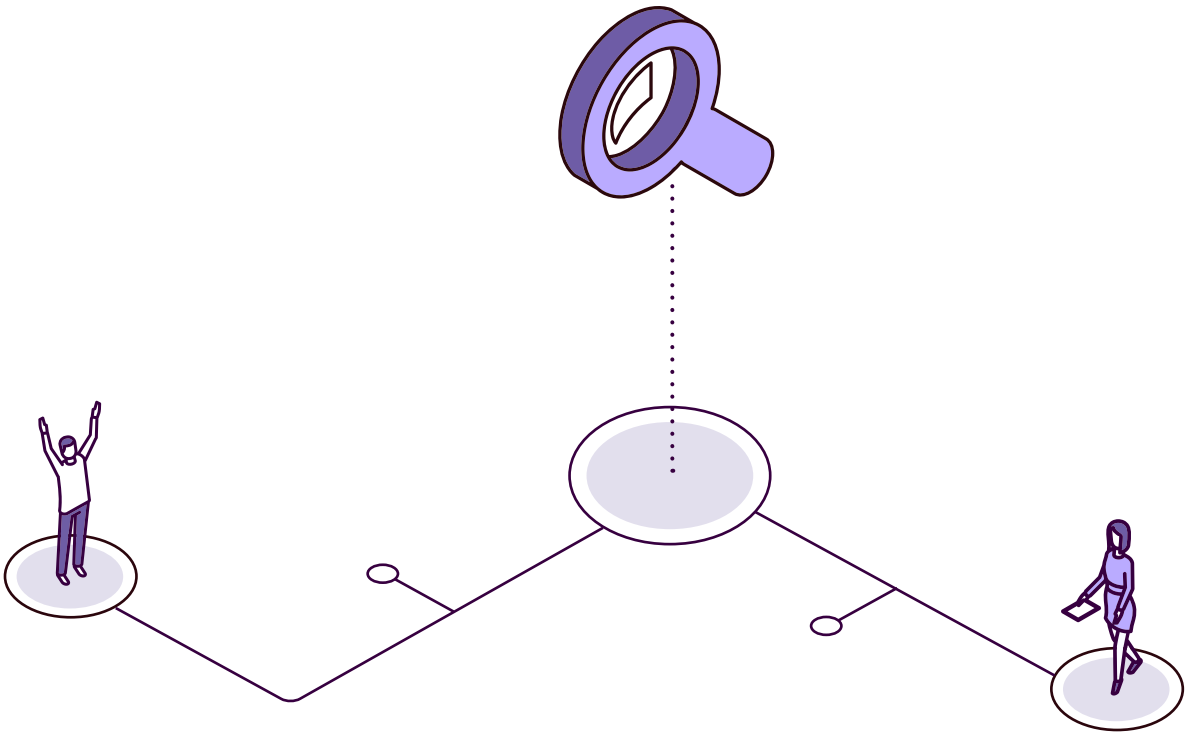
IDENTIFY ACTIONS

After analyzing the initial situation (as is) and, with a clear idea of how far we want to go (to be), it is necessary to identify the actions to be carried out both by the governing entity and by the different administrations or ministries involved in the digital transformation, with a view to meeting the given objective within the established timeframe.

The different actions must be included in a plan in which the projects to be undertaken are established, milestones are established, risk management is carried out, etc. In addition, it must be taken into account that the plan defined by both the governing entity and the ministerial departments involved will not be fixed in time, but will be subject to changes and modifications motivated by changing situations or exogenous events (e.g., COVID-19). For this reason, a mechanism must be

established that allows the document to be updated manner. This ensures that the projects are always aligned with the technological objectives and that the technological objectives are in line with the government's objectives.

As the plan progresses, it is important to check that it is "traveling in the right direction and at the right speed." Therefore, it is necessary to monitor the previously identified indicators. From this action it will be possible to draw conclusions such as the following: Are the objectives being achieved? Or, at the rate it is going, will it be possible to finish on time? From the evaluation of these metrics by the lead institution as a whole or by the ministries in particular, if deviations are detected, the pertinent actions will have to be taken to correct the problems.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara is participating in the elaboration of the technological strategy of her ministry. Among the strategic objectives is the reduction of waiting lists, which on the one hand cause a health problems and, on the other hand, cause citizens' confidence in the public health service to decline. To this end, among the different actions proposed by technology team is to optimize the time of doctors, setting up an online appointment service to minimize downtime between patients and patients and, at the same time, to promote the most efficient use of healthcare infrastructures. To undertake this project, a common appointment service used in the Ministry of Employment has been reused, which is already operational and, with minor adjustments, can be put into operation in the healthcare sector. A quick benefit for the citizens is achieved at low costs, since the assets of the public administration itself are being reused, and with low risk since it is a proven service that has been in use for years in the Ministry of Employment.

Entrepreneur
Ana

Ana has just installed and configured the inventory management system used by her municipal administration, which completely fits her needs. As her company grew, she realized that she needed to have keep track of both IT and furniture inventory to control amortization periods and make efficient use of resources. At first, she thought about market solutions, but seeing that his country had a policy of reutilization of free software, he consulted the catalog of available software and chose the inventory management system of a municipality that suited the needs of his company.

Mayor's advisor
Daniel

Daniel implemented the software reuse policy in his municipality, and nowadays the budget is mainly oriented toward hiring local companies and suppliers to make adjustments to the applications available in the software repository of public entities and adapt them to the specific needs of his municipality. Daniel is very happy with this approach because, apart from having applications that are specifically tailored to his needs, he has managed to create an ICT innovation ecosystem in the municipality that is no longer only focused on municipal projects, but also provides services to companies and institutions in other locations.

EXAMPLES

Click on each flag or icon to go deeper.

Examples related to technology strategies:

Spain
Digital Strategy

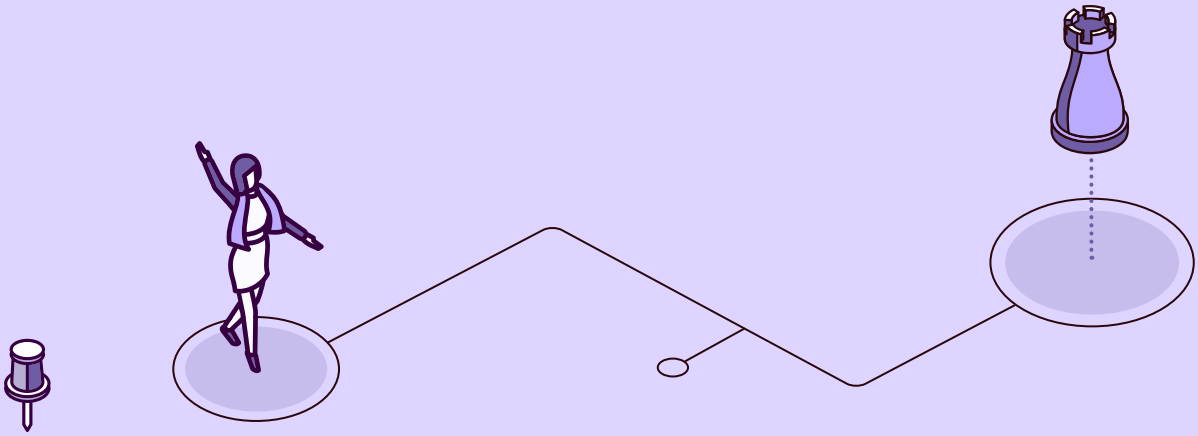
The IDB
Code for Development

European Union
Digital Strategy

The European Commission
Joinup

United States
Digital Strategy

Uruguay
Technology Transfer Center



INDICATORS

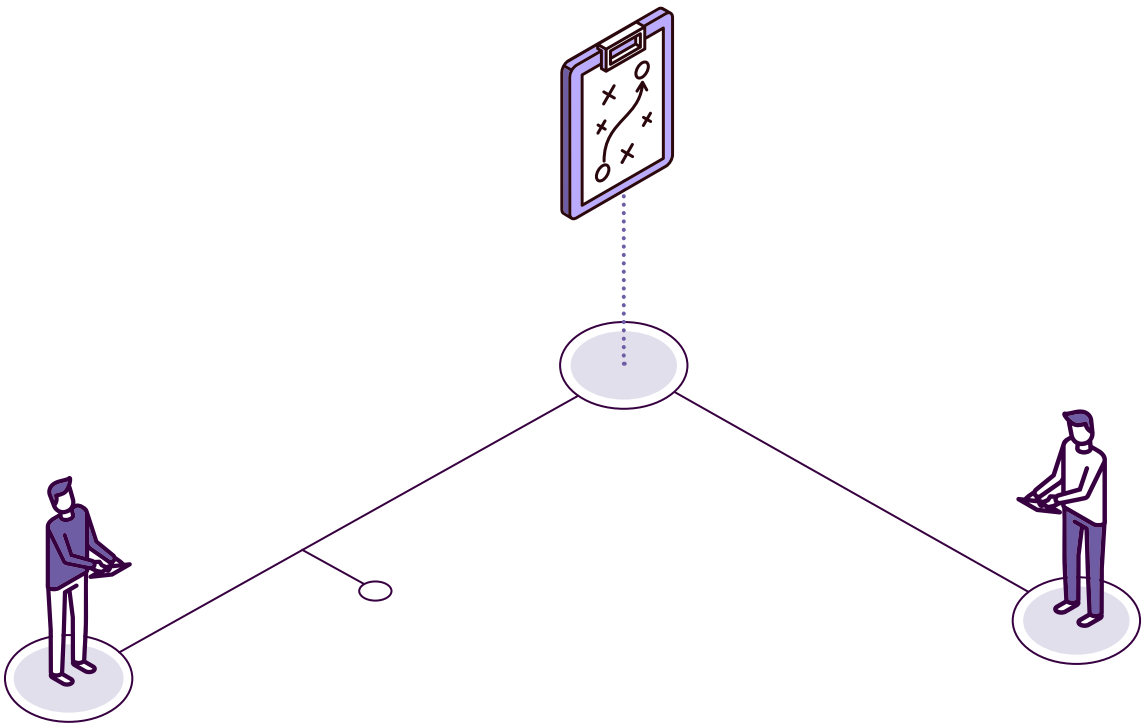
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Does the country have a technology strategy? If so,
  - Does the technology strategy mention any of the following?
    - use of common or horizontal services whenever possible, by all ministerial departments
    - access to data already in the possession of the public administration, so that the citizen is not required to present documents in the possession of the administration
- Does the country have a national open-source software policy?
- Does the country have instructions regarding the reuse of applications in public entities?
- Does the country have an open source repository that can be shared and reused? If so,
  - is this repository federated with others at the state, local, or international level?
- Is there a public open-source software license available to be applied to public entity undertakings?

1.1.3 PROCUREMENT PLAN

When a country or a large ministry decides to embark on a digital transformation process, one of the essential aspects is to develop a good sourcing plan. The term "sourcing" is no accident and is a far cry from a procurement plan. A sourcing plan means "How am I going to source everything I need to make the digital agenda a reality: hardware, software, talent, etc.?" Therefore, it is more holistic than a procurement plan.

One of the main parts of the sourcing plan is the ICT procurement strategy, which is usually carried out through a specific agency specializing in ICT procurement. The various functions mentioned below can be concentrated in that specific agency or, if there are already agencies set up with particular competencies (e-government, centralized procurement, or others), each function can be deployed in one area, as long as it is done in a coordinated manner. It should be noted that many of the recommendations mentioned here are suitable for any type of procurement—and therefore can be incorporated into the general procurement scheme of the state—but, due to the rapid evolution of technology and the pace of technological projects, they are particularly important in this area.



AUTOMATED PROCUREMENT

An interesting possibility for ICT procurement is that of automated procurement. There are already cases where, for simple contracts with objective evaluation criteria, this type of procurement can be carried out, in whole or in part. For the tendering procedure, a data model agreement needs to be reached, which includes both the publication of the request for bids and the data model of the bids.

- What are the advantages?
  - It significantly increases efficiency, since the whole process, sometimes tedious and multistep, is done automatically.
  - It allows for greater traceability and transparency.
  - There is no room for discretionary decisions.
- What is needed for these automatic models to work properly?
  - The country's interoperability system must function optimally.
  - Certain horizontal services must be in place for example: electronic authorizations, automated communications and administrative notifications, and common definitions of electronic files and documents.

AGGREGATE PURCHASING POWER OR BARGAINING POWER

In many cases, ICT suppliers are larger than small public entities, so their bargaining power is large. Even if there is a joint strategy, some countries are smaller than ICT suppliers. Therefore, it is important to aggregate bargaining power among multiple public entities.

GUARANTEE NECESSARY CAPACITY

ICT procurement is a complex activity that requires specialists, and it is difficult or impossible for all entities to have them. However, the existence of a specialized unit can bring strong benefits to the country. It covers the rules, organization, and specific functioning to make technology procurement as efficient as possible for the state.

CREATE ALTERNATIVE CONTRACTING VEHICLES

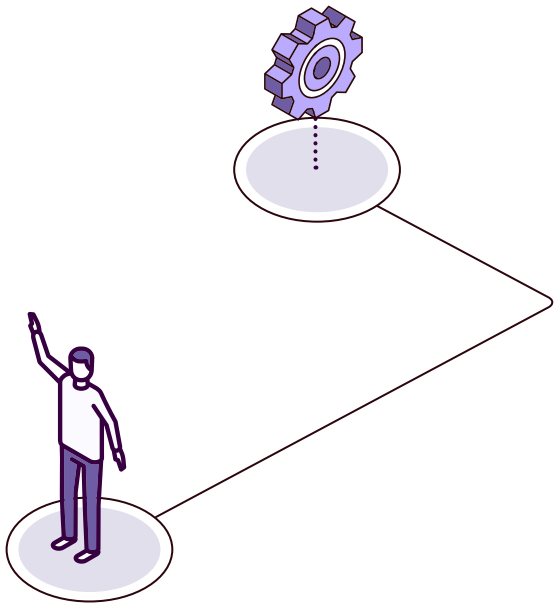
ICT purchases have several peculiarities. For example, requirements are not always defined at the time of contracting, so it is often necessary to use more flexible schemes. It is also often necessary to mobilize resources very quickly—for example, in the event of a cybersecurity problem. For these reasons, special procurement procedures are often necessary.

What is clear, and perhaps more important, is that dispersion generates incompatibility and interoperability problems, so even if the individual institutions do not experience the aforementioned problems in their purchases, there has to be a purchasing strategy so that it does not happen that a unit A purchases a system from a company that is different and incompatible with the purchase of another unit B.

ADD LOGISTICS SERVICES

We must not lose sight of the fact that in many cases it is not just a question of purchases; there are cases in which certain acquisitions are accompanied by logistical services, training, and support services. Suppose your plans include the renewal of forty thousand computers for an entire sector. In addition, you want that acquisition to be accompanied by interactive whiteboards for the meeting rooms, and, of course, you want certain people in each office to be selected to teach how to use the interactive whiteboards. In this case, it would be wise to launch a procurement that includes the following:

- the computers
- distribution logistics
- installation and configuration services
- installation of interactive whiteboards
- training services



Of course, ideally, support and maintenance services with detailed service-level agreements should be in place to address any problems in the shortest possible time.

SOFTWARE ACQUISITION

The following are the main modes of software acquisition: :

Body shopping or Time and materials: A modality in which the organization uses resources from the private sector to work and build or adapt the software under the indications of internal staff.

Turnkey: Whereby an administration pays for the construction of a system according to given specifications.

Commercial software: A modality by which you pay for the rights to use a system that has already been built.

Public-private collaboration: Through which cocreation ecosystems are generated and innovation avenues are explored by sharing resources and results.

The above, the modality that generates the most knowledge and innovation is public-private collaboration, which is discussed in detail in another section. The most inefficient, but the one that allows the most control over resources, is *body shopping*, and those that are usually the most innocuous for the administration are usually turnkey or commercial software. Of course, these are only general rules, and each organization and each project will have to establish the ideal conditions for choosing one modality or another.

TALENT SOURCING

In many cases, it is necessary to acquire new talent, which can come from different disciplines. It is necessary to act mainly on three fronts:

- **Internal to the administration:** Work with public employees to involve them in the objectives and goals to be achieved in the transformation plan and, consequently, work on the training plan.

- **Toward citizens:** To attract new talent to government positions at different levels, it is crucial to make the administration an attractive place where people want to develop their professional careers.

- **In the private sector:** Communicate the goals to be achieved in the transformation plan. Only in this way will it be possible for the private sector to align itself with the public sector and, through public tenders, to offer the most appropriate profiles, knowledge, and services.

CONSIDER THE NECESSARY LEAD TIMES

The road map of the transformation strategy must be perfectly aligned with the procurement plan, which must be multiyear. In addition, for the success of this type of initiative, it is vital to take into account bidding times so that procurements are ready at the right time. Poor planning of the procurement can derail the digital transformation strategy. Similarly, in the case of the need to recruit new public employees, it is necessary to take into account the long time frames that are usually involved in the selection processes for access to the administration.

In short, the acquisitions of hardware, software or intangible assets (knowledge, personnel, talent) must be well planned that is in line with the overall digital transformation strategy.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Mayor's advisor
Daniel

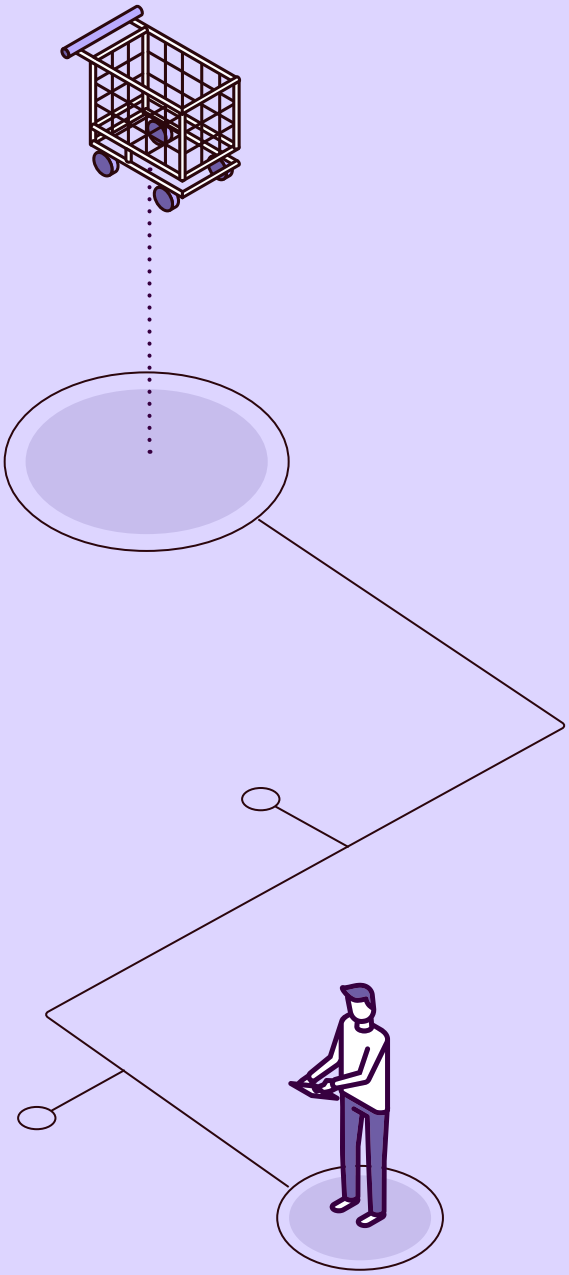
Daniel has to renew the licenses of the database used by his municipality. He feels totally overwhelmed because he has to deal with a large multinational company and fears that he has little bargaining power with them. Daniel spoke with the head of digital government and is delighted to have learned that the country has the rapid contracting system (also known as "catalog system" or "framework agreement") for technology projects. He understands the complaints of his colleagues in other countries that, in the case of technology projects, they take almost a year to contract, making the possibility of satisfactorily meeting the political, social and technological needs of their countries unfeasible.

Vice minister of health
Sara

Sara wants to kick-start a digital transformation process of the health sector. She has made a commitment to citizens to meet a series of objectives and new services with a clear road map. Once the digital transformation process is underway, they realize that no one considered that two hundred new public employees were needed in different departments. The selection process is going to take months, so Sara will have to rethink her goals. The procurement plan only included goods.

EXAMPLES

Click on each flag or icon to go deeper.



Chile
ChileCompra

Spain
State Contracting Platform

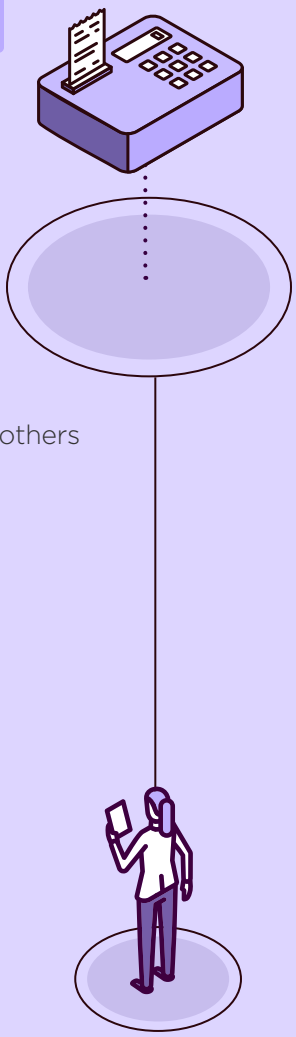
United Kingdom
Digital Marketplace

Brazil
ICT Procurement

Australia
Sourcing made simple

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.



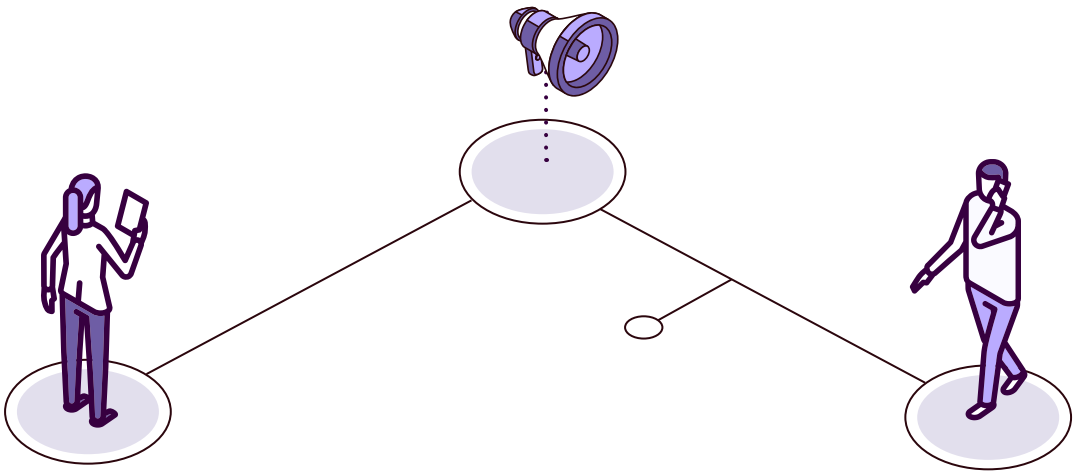
- Is there a procurement plan for the government?
  - If so, which of the following does it contemplate?:
    - Aggregate purchase of pcs and laptops
    - Aggregate purchase of printers and scanners
    - Centralized contracts for licenses, communications, packaging, and others
- In the country, do the following elements exist for ICT purchases?
  - automated contracting
  - rapid development contracting
  - standard clauses
  - framework agreements
- Is there a government procurement platform?
  - If so, which of the following does it contemplate?
    - aggregate purchase of pcs and laptops
    - aggregate purchase of printers and scanners
    - centralized contracts for licenses, communications, packaging, and others
- Is there a state billing platform?
- Is there a talent sourcing strategy?
- Is there a multiyear internal staffing plan?

1.1.4 COMMUNICATIONS PLAN

When the government is immersed in a digital transformation process, this involves the implementation of various technological projects for the provision of digital services, which translates into continuous changes that impact different groups at different times since the transformation process is dynamic. However, what is not communicated does not exist. Thus, effectively communicating the value of the digital transformation plan to key stakeholders is one of the most challenging parts of digital transformation. It is essential that communication is strengthened, and actions are properly planned and coordinated so that messages do not contradict each other and provide a perception of order.

On the one hand, the changes imply an incessant demand for information from different interest groups, and, above all, from the users of the services, whether internal (the administration itself—i.e., public employees) or external (other professionals who interact with the administration, companies, citizens, etc.). On the other hand, it will be necessary to maintain effective and fluid communication with other agents, groups, organizations, and institutions involved in the transformation, with which it is essential to achieve coordination. Likewise, it is necessary to highlight the value of the investment and effort made, both internally and externally, and both nationally and internationally.

This creates a complex communication map, which needs to be conceptualized with in three levels. In this sense, we will be talking about three lines of communication: internal communication, external communication, and communication for institutional relations. The governing body of the digital transformation, with the support of a specialized team, will lead external communication and institutional relations, while internal communication will be the responsibility of each sector.



INTERNAL COMMUNICATION

Internal communication in digital transformation is a relevant factor in change management as a tool for:

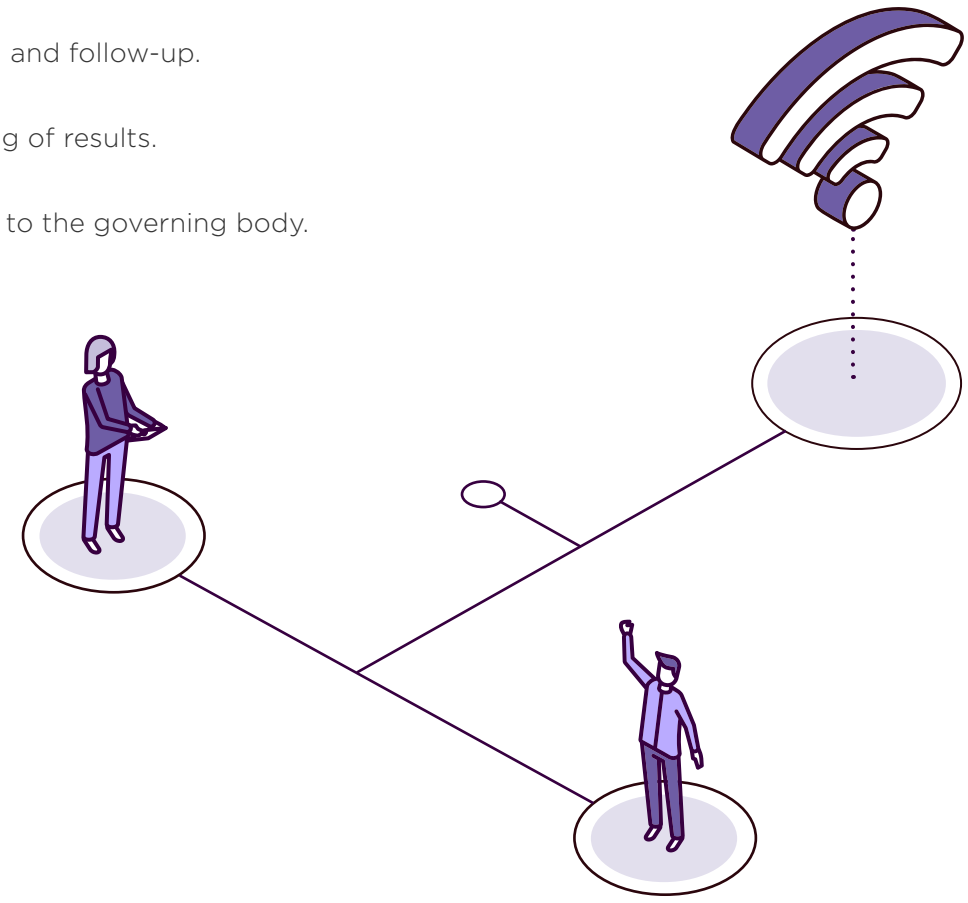
- dissemination of the scope of the transformation plan;
- awareness of the importance of the initiative;
- encouraging the collaboration of public employees.

The audience for this communication will be:

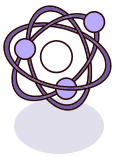
- all public employees directly or indirectly affected by the digital transformation.

The responsibilities of each sector shall be

- creation of the internal communication plan (ICP).
- execution and follow-up.
- monitoring of results.
- reporting to the governing body.



To simplify the creation of the ICP, the sectors can use a planning method to help them deploy communications for each project. This involves listing the projects and defining actions for each of the following **communication blocks**:



AWARENESS

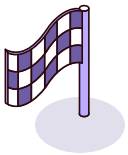
Prepare for the change.

- Show the link between strategic objectives and transformation projects.
- Provide general information on transformation projects.
- Raise awareness of the imminence of change.

UNDERSTANDING AND ACCEPTANCE

Generate a vision of process transformation.

- Create awareness of change.
- Explain process changes and their main impacts.



ENGAGEMENT AND ADOPTION

Foster enthusiasm and reinforce the idea that change is possible.

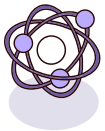
- Build confidence that they will be prepared for change with training.
- Make the results of the diagnostics known.
- Create awareness that the change must be sustained.

INTERNALIZATION

To become part of the culture.

- Reinforce the support scheme.
- Reinforce changes in operations.
- Raise awareness about the proper use of the new processes.

For the design of the ICP, the actions of each block will be crafted taking into account the corresponding communication objectives, and, for each of them, the audience, channels, frequencies, messages, types of content, and execution schedule that will serve as a guide for the development of the plan will be detailed. Each block are communication campaigns that are activated with a specific objective necessary for internal communication:



Awareness

The first campaign or launch comprises activities to bring organizations, groups and public employees affected by the change closer to the project, providing them with general information on how the project is aligned with the business strategy, its scope, and its objectives. During this campaign, the leaders of the organization and of the project deploy an official communication, so that everyone knows that the change will occur, understands the sense of urgency, and begins to get involved in the change process.

Messages will be aligned with the idea that change is beneficial and imminent. Capturing the attention of the audience is fundamental at this stage, since this is when the change agents' commitment to implementation begins. The main means (channels) for reaching audiences will be those that are most effective for the sector, since they are the ones that are familiar to all agents and guarantee the delivery of messages. Changes in other non-essential aspects of the transformation process should be kept to a minimum.

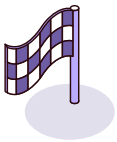
Understanding and acceptance

This campaign seeks to raise awareness of the changes the transformation will bring to the operation of the organization and the individuals involved. For this, the nature and intention of the change must be understood, so that individuals do not judge the change too harshly. . Thus, once they understand it, they will decide whether they will support the implementation or not. Acceptance will be achieved only when there is a perception that the benefit outweighs the cost.

The general goals of the campaign messages are summarized as follows:

- to make public employees see that the transformation has already begun and that the new way of working is being constructed in a way that benefits them
- to create awareness of professional approach to change in change
- to build trust

FOR CHANGE TO BE ACCEPTED, THERE MUST BE THE CONVICTION THAT TRANSFORMATION IS POSSIBLE



Engagement and adoption

This campaign aims to continue to inform about the implications of change in the short term and explain what is desired to be achieved in the long term. Since the change is still being evaluated by individuals, it can still be misunderstood or vetoed, so it must be clearly stated what actions will be taken to ensure that the change is implemented and remains in place in the long term. The purpose of launching this campaign, then, is to maintain enthusiasm and reinforce the idea that change is possible and to inform about the tools that have been made available to make it happen (training, support centers, etc.). It will reinforce the idea that the change will not be perceived as an extra workload or generate a feeling of lack of control.

Internalization

This campaign aims to integrate the change that has taken place in the culture. Communication should focus on bidirectional feedback and the valorization of results. Bidirectional feedback allows us to :

- involve change agents in the process;
- communicate the results obtained after project deployment;
- appreciate the commitment of those involved;
- solicit feedback to implement elements for improvement.

WHEN PARTICIPANTS FEEL OWNERSHIP OF THE CHANGE, THEY ARE MORE LIKELY TO BE ENTHUSIASTIC AND BECOME PART OF IT.

This campaign will be the moment when public employees will have more doubts about the use of the solution and the efforts devoted to; that is why the tangible achievements of the transformation projects must be shown, so that they recognize them as their own and understand the need for their continuity, led by them from now on.

EXTERNAL COMMUNICATION

Creating an external communication plan (ECP) can be complicated, due on the one hand to the changing environment of the transformation, where changes in strategy will continuously affect the original plan, and on the other hand due to the changing leadership of the public authorities, which by their nature vary periodically and can in turn change the focus of the transformation, the decision-making hierarchies, and even the resources allocated.

In any case, the ECP must be designed with the main objective of justifying, in the eyes of the different stakeholders, the investment in technology for the transformation assumed by the administration. Technology entails a change in the way of doing things, an increase in productivity and savings, and, consequently, an improvement in the service offered by the administration, but it is essential to communicate this externally in order to provoke a perception of the value of improved service.

There is, in addition, another objective: to transform with *transparency.* Openness means:

- keeping the citizenry and the political-administrative structures informed
- planning initiatives that promote participation and transparency
- offering open government services
- opening conversations through social networks
- using the language and forms, not of the state, but of the citizenry

The audience for this communication will be

- users of digital transformation services.
- agents or groups outside the public administration who, regardless of whether they are affected by the transformation or not, want to be informed.

The responsibilities of the governing body shall be

- the development of an external and institutional communication plan for digital transformation.

- execution and follow-up.
- monitoring of results.

Taking into account the objectives of external communication, it is advisable to follow *two lines of communication*, with complementary objectives and actions, but using different resources and channels:

1. **Continuous line:** This will use the traditional channels and types of actions, incorporating messages related to digital transformation and creating dissemination material about the projects and services of the transformation plan.

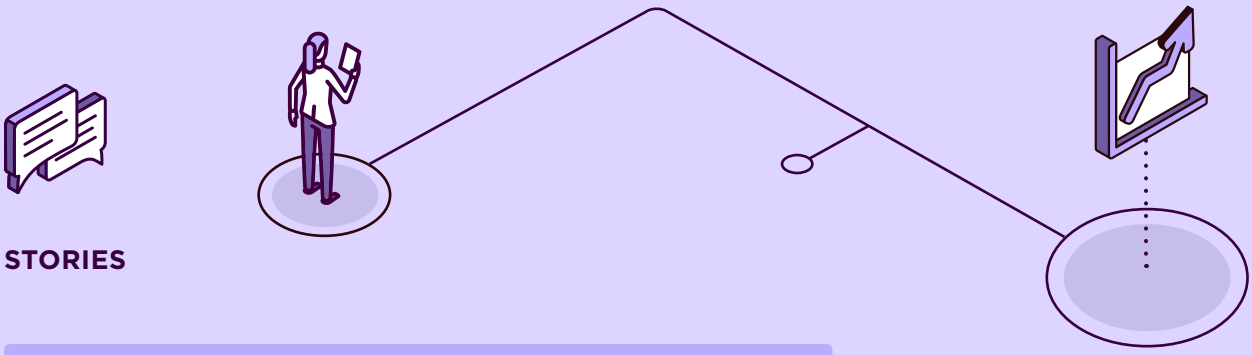
2. **Disruptive line:** The aim of this line is to carry out innovative actions with a high communication profile. The vertical sectors will propose the projects or services they consider relevant, and the governing body will select those that, due to the number of people impacted, the degree of change/transformation involved, or the budgetary investment made, will benefit from this strategic line.

INSTITUTIONAL RELATIONS

The lead agency must coordinate with all the sectors throughout the digital transformation, in a two-way communication: providing and requesting information. Likewise, it will be necessary to create spaces to promote the transfer of knowledge and experiences between the sectors and the different agencies that share functions in the transformation for each sector.

Depending on the reality of each country, the distribution of responsibilities in terms of the communication plan could take different forms. For example, communication aimed at the general public is usually directed by the governing body. However, particularly complex vertical sectors with strong groups of companies or professionals involved (justice with lawyers, health with doctors, among others) may require a change in roles (i.e., each vertical sector to be in charge of the external communication plan, with the support of the governing body, of course).

It is also advisable to plan actions that promote the participation of the governing body and those responsible for the transformation of the different vertical sectors in international environments, with the aim of positioning them as leaders in digital transformation.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo has always complained that the government's services change, and nobody ever finds out about anything, that you are on your own to navigate changes. But now things appear to be different: with the implementation of the new civil registry there has been a continuous flow of information, which he is grateful for because he had feared that it would become a paid service, but what is simply changing is where the procedures will be done and that it will be easier and without physical trips required.

Entrepreneur
Ana

The commitment to innovation in public administration is something that Ana has bet on. In the transformation portal, they published a statement in which they made a call to those SMEs that wanted to support and participate in the digital transformation. Ana did not hesitate; she thinks it can be a springboard to grow and become known in the public sector.

Vice minister of health
Sara

Sara has just participated in the eighth edition of the International Digital Health Congress in San Sebastian. This year, due to the pandemic, it was held virtually, but it was as enriching as other years, when she shared her experiences with professionals from public and private administration in the sector.

Mayor's advisor
Daniel

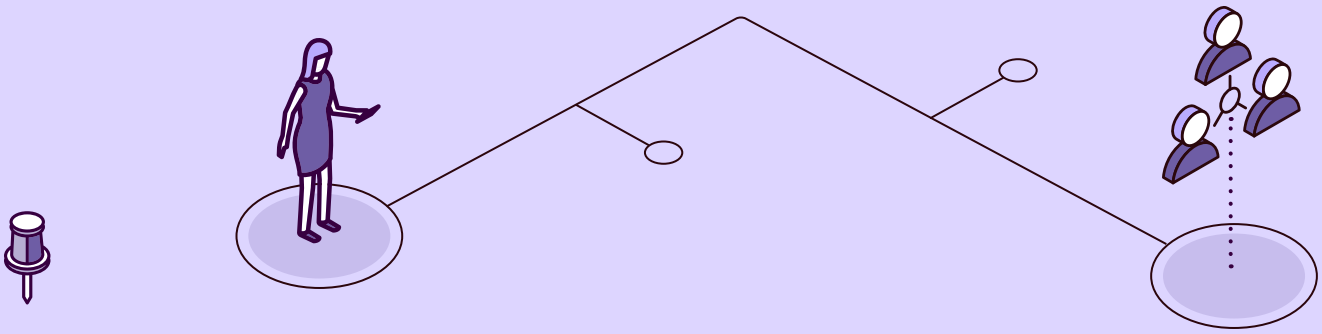
Daniel, along with other colleagues, has the objective of disseminating and communicating the digital change they are going to experience in their work environment. They know that their role is important and they are going to be in charge of internal communication following the four-block communication model he has learned. He has planned workshops sessions for the employees of the municipal government, with the aim of aligning the employees towards the common goal, to learn about the transformation and, to increase their participation in the change.

EXAMPLES

Click on each flag or icon to go deeper.

Spain
Barcelona Ciudad Digital

Colombia
Transparencia y acceso a información pública



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are internal communication mechanisms in place to reduce resistance to change? If so:
  - Does it create a sense of urgency in the organization so that staff understand the importance of the project and support the change process?
  - Does it reduce the uncertainty of change with formal, time-bound communication?
  - Does it motivate people to learn and embrace change in a clear and personalized way?
  - Does it contemplate creative strategies for each target audience, driving innovation and integrating new work methodologies?
- Do you have specific internal communication plans per project, so that the executors of the communication plan are able to receive feedback? If so:
  - Are communication campaigns included as part of change management plans?
  - Do the plans include mechanisms for incorporating feedback on an ongoing basis?
  - Does it include targeted communications for different stakeholder groups?

- Does it contemplate data-driven decision-making for communications?
- Do you have defined mechanisms to measure the impact and effectiveness of communication, as well as the degree of understanding of the messages for each of the different audiences identified?
- Do you leverage change agents to achieve a cascading flow of communication at different levels of the institution?

› Do you have a two-way communication strategy? If so:

- Does it use communication as a means to support strategic transformation objectives?
- Does it leverage the channels available to you to strengthen transformation communication?
- Does it promote the creation of internal learning networks?
- Does it promote dialogue andconflict resolution mechanisms?

› Do you incorporate actions to strengthen institutional relations via external communication? If so:

- Does it promote the sustainability of the transformation in individuals and in the institution?
- Do you establish professional contacts with other institutions?
- Do you encourage interaction between institutional relationships so that all interorganizational initiatives are known?
- Do stakeholders actively participate in debates, activities, or congresses highlighting the role of transformation?
- Do you share the positive impact of the services in international forums?

1.1.5 CYBERSECURITY PLAN

Undoubtedly, any digital transformation strategy must be accompanied by a cybersecurity strategy or plan, especially as the value of information and data is higher than ever, and cyberspace is increasingly populated by cyberattacks and cybercriminals. In addition, there is an aggravating factor for the public administration because it handles sensitive. As such, loss, theft, improper modification, and any other unauthorized action could lead to an irreparable catastrophe.

Imagine for a moment that the registry in which a country's criminals are listed along with their convictions disappears, or that the national passport database is attacked and not backed up. Not all possible incidents would have the same effect, but what is clear is that data is an asset that must be defended and protected above all else.

For this reason, it is essential to accompanyl advances toward a digital administration with cybersecurity. It would be imprudent progress with the implementation of services that do not have adequate protection in place.

The cybersecurity plan should be underpinned by a corporate governance structure in which the interests of citizens are considered and guidelines are defined to allow for effective decision-making, including the following:

- The creation of a risk management framework.
- The establishment of an internal control system.
- Acceptance of responsibility for by senior management.

THE CYBERSECURITY PLAN SHOULD BE UNDERSTOOD AS THE ORGANIZATIONAL STRUCTURE TO GOVERN CYBERSECURITY ISSUES AT THE NATIONAL LEVEL.

This plan should include the following:

- Establishment of a national cybersecurity authority. This may be an individual (cybersecurity czar) or an entity with national cybersecurity authority, which may also act as a managing entity in defining and clarifying roles, responsibilities, processes, decision-making powers, and tasks necessary to ensure effective implementation of the strategy.

- Oversight, by the national cybersecurity authority, of the implementation of the strategy and the setting of performance targets for various ministerial or government departments, institutions, or individuals responsible for specific aspects of the strategy.

- Creation of a body to exercise leadership and coordination of cybersecurity, chaired by the highest representative of the state responsible for national security policy.

- Coordination and cooperation with other countries at the international level.

- Establishment of a mechanism to identify and include all government entities affected by or responsible for the implementation of the national cybersecurity strategy.

Cybersecurity, defined as the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, including the information contained therein, to ensure its availability, integrity, authentication, condidentiality, and nonrepudiation,"[8] is a shared problem. It affects practically everyone, and everyone must cooperate to manage it. Each country must have a cybersecurity coordination body to facilitate the implementation of the national strategy hand in hand with different actors. In turn, each of the relevant actors should have a cybersecurity team to develop and implement their sectoral or contextual cybersecurity competencies and provide the dedicated attention required to mitigate the risks.

8. United States Department of Defense, DOD Dictionary of Military and Associated Terms. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

CYBERSECURITY GOVERNANCE

Any cybersecurity plan must include governance, consisting of well-defined leadership, organizational structure, and a process for protecting information. This governance is a subset of each country's corporate governance and should

- provide strategic direction;
- guarantee the compliance of established objectives;
- manage risks appropriately;
- promote the responsible use of public funds;
- monitor the success or failure of each institution's cybersecurity program.

The different cybersecurity frameworks (ISO, NIST, and ITGI standards) establish a series of basic pillars to establish cybersecurity governance:

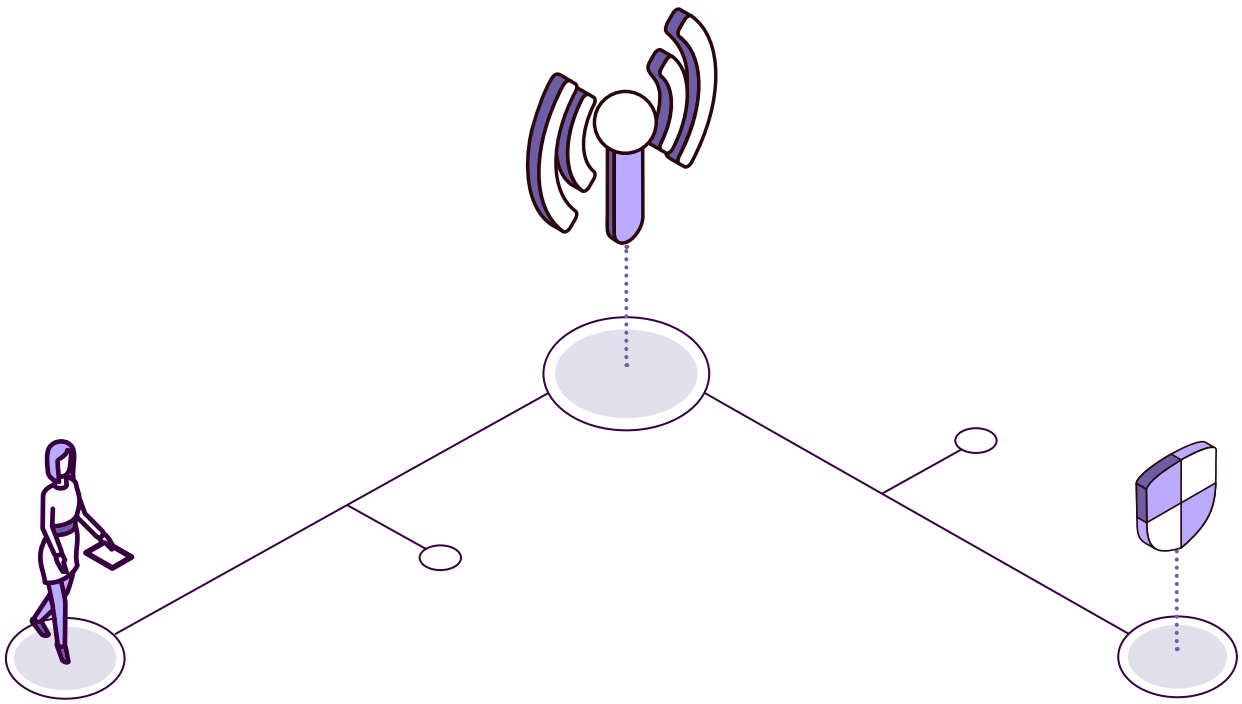
- ISO standards:
  - strategic alignment
  - risk management
  - resource management
  - performance measurement
  - delivery of value.
- NIST standards:
  - strategic planning of information security
  - security governance structure.
  - definition of key roles and responsibilities within the government
  - development of policies and guidelines
  - constant monitoring

As a first step in addressing the development of a cybersecurity plan, the following cybersecurity governance structure should be defined:

- Senior management: In charge of defining the cybersecurity strategy (i.e., the organizational objectives with which public administrations must comply).

- Security committee: Responsible for reporting to senior management. It is in charge of managing the risk associated with the cybersecurity strategy and defines security requirements.

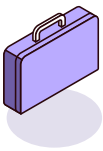
- Appointment of the chief information security officer (CISO): In charge of reporting to the security committee. His or her role will focus on defining a security action plan, as well as the policies and standards necessary to ensure cybersecurity within the organization (or government). His/her work program is based on the definition of a security program, its correct implementation, and compliance with objectives.



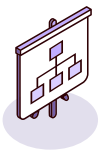
SECURITY COMMITTEE

A cybersecurity committee can have the following elements:

Principles



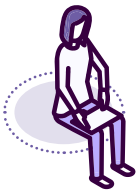
Functions



Competencies

Structure

Implementation plan

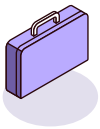


Principles

The following principles are recommended for the organizational and operational model of the cybersecurity committee:

- Contribute significantly to the transformation of the public service, ensuring cybersecurity through innovation, the application of best practices, and the necessary regulations for the effective implementation of cybersecurity norms and standards.

- Actively promote the cogovernance of cybersecurity with public administrations and other relevant institutions, avoiding inefficiencies, duplication, lack of coordination, or conflicts in the design, development, deployment, and operation of information systems.

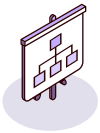


Functions

The following functions for the committee are proposed:

- governance
- deployment of best practices and standards
- technological risk management
- incident management
- audit and certification
- awareness and training

In order to carry out the aforementioned functions, the cybersecurity committee, which will supervise and direct the cybersecurity activities, must be strengthened. In order to formalize this work, a regulatory document should be developed that sets out the competencies and areas of action of the cybersecurity committee (terms of reference), which should be formally approved.



Competencies

With a view to improving the responsiveness of the cybersecurity committee, the following competencies of this body are proposed:

- Supervise compliance with the government information security policy, establishing a common regulatory and procedural body, adapted to the current context of cybersecurity, taking into consideration lessons learned.
- Analyze and approve, where appropriate, the use of certification schemes as a facilitating element to increase the level of security of public institutions and the public display of their compliance.
- Define and prioritize strategic security objectives, weighing their relevance and need for resources.
- Analyze metrics and indicators regarding cybersecurity in the different institutions, as an aid for decision-making and the definition of objectives in this area.
- Determine and supervise the implementation of training and awareness-raising activities for all public administration groups.

- Define and follow up on the technical audit plan that defines the surface exposure of public administration systems, the results of which will make it possible to act accordingly to improve cybersecurity.

- Assess cybersecurity risks with respect to public administration systems and their interconnections, defining and approving general mitigation plans for them.

- Define and monitor the activities of a cybersecurity operations center (SOC) for the public administration of each state (supported by a CERT) to, among other things, receive continuous information on the global state of cyberthreats and collaboration in the aspects deemed appropriate.

- Define the increase of surveillance, detection, and response capabilities required in the different networks and electronic sites supported by the different public administrations, together with their continuous follow-up, based on the results of risk analysis and reports on technical audits, monitoring, and intelligence applied to the analysis of threats and vulnerabilities.

The responsibilities of the cybersecurity committee should include be provision of services, solutions, and tools for the improvement of digital security in the following areas:

Preventive services

- Facilitate the establishment of a cybersecurity program that will enable the various institutions receiving its services to apply it and become certified, based on the experience of the existing regulatory and technological framework.

- Provide a service to measure the surface exposure by identifying configuration deficiencies and detecting vulnerabilities of the affected information systems through information services and vulnerability support, auditing, and continuous monitoring.

- Provide tools that enable a state's institutions to monitor compliance with the aforementioned cybersecurity program.

- Provide tools to enable certification of compliance with the cybersecurity program and the issuance of the corresponding badges.

- Carry out awareness-raising and training actions for all personnel involved in the use, operation, management and maintenance of the information systems of public institutions in order to prevent malpractice.

Detection and surveillance services

- Provide solutions that increase the capacity for surveillance and detection of cyberattacks, supported by the SOC, and that can be integrated with the detection capabilities of the national CERT.

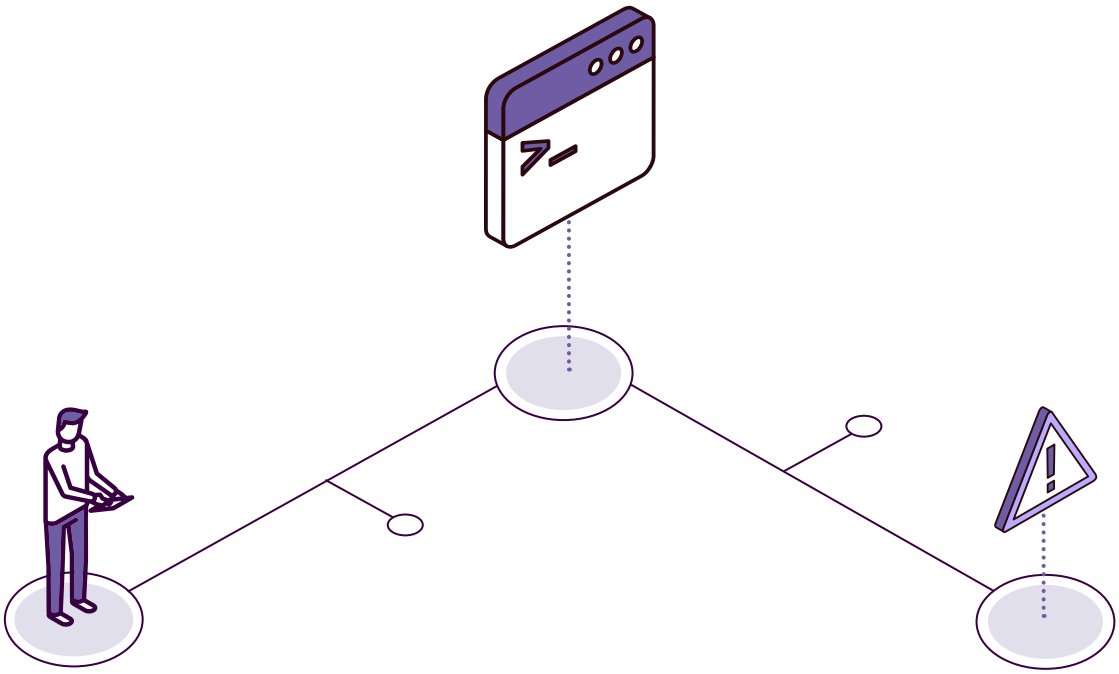
- Promote the creation of detection capabilities in the public institutions and facilitate the exchange of cyber incidents and cyber threats with the CERT.

Integrated response services

- Provide advanced capabilities to automate the response to any cyber-attack.

- Create the capacity for forensic analysis and information exchange of institutions affected in the provision of services of the corresponding public administration.

- Have capabilities to respond to complex cyberattacks.



Structure

Should consider establishing the following cybersecurity units, at a minimum:

- National cybersecurity coordination body, as it is necessary to have a politically strong body starting from the head of government to coordinate various public sector organizations and other entities. It is recommended that it be a civilian organization rather than a defense organization, as civilian organizations tend to find it easier to form alliances with different sectors (academia, private, civil society, and individual citizens), and can be more trusted to manage the systems of different sectors when intervention is required, as their focus is solely on promoting cybersecurity, with no other defense or intelligence interests.

- Specialized units dealing with long-term cybersecurity issues, such as legislation, education at all levels, from elementary school to professional training and continuing education, awareness raising, promotion of the local multistakeholder ecosystem, the commercial cybersecurity industry, and the establishment of standards.

- Units dealing with cybersecurity research and development issues, which would increase and improve the workforce, modernize regulatory frameworks, and create alliances with other sectors and international actors.

- Operational units, both national and sectoral, with the following functions: monitoring digital assets (belonging to the government and critical sectors), dealing with cyberintelligence and threat search, exchanging information, implementing incident response and recovery mechanisms, creating situational awareness, and cooperating at the operational level both locally and internationally.

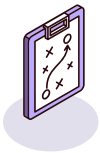
- Specific cybersecurity law enforcement units to monitor cyberspace and identify instances of crime, investigate them, prosecute them, and assign judges with appropriate training to handle these cases.

- Specific units within defense and intelligence agencies to protect the country from attacks in cyberspace originating from state or nation-state actors, or that may have domestic consequences.

- Specific units to protect critical national infrastructures against cyberattacks.

- Specialized units within specific sector regulators, such as health, transportation, finance, telecommunications, energy, water, and other critical sectors.

- Units within organizations in charge of the cybersecurity of their own systems. These may reside outside of information technology departments, as the cybersecurity objectives of CISOs are different from those of CIOs (chief information officers) and sometimes conflict.



Implementation plan

For the improvement of the cybersecurity of each country's public service, it is recommended to plan in light of the following considerations:

- The goals, principles, areas, and lines of action and measures for improvement should be established in advance and serve as a guideline for the rest of the decisions.

- The cybersecurity committee's strategy, which will be aligned with the national cybersecurity strategy, must be approved at the highest level.

- The objectives of the cybersecurity committee, its scope of application, roles and responsibilities, security measures, indicators, evaluation, audit, and accreditation scheme, which will be aligned with the cybersecurity strategy of the public service of each state, must also be defined.

- The approval of the cybersecurity committee and corresponding cybersecurity model will require the preparation and approval of a regulatory impact analysis report.

- It will be necessary to present the weaknesses with the current situation.

- It is a preliminary, high-level plan, structured in phases and activities, the details of which will have to be developed after the approval of the operating model and capabilities of the cybersecurity committee to be established.

- Once the characteristics of the new operating model and capabilities of the cybersecurity committee have been detailed, it will be possible to estimate resource requirements, both in house and external, as well as implementation deadlines.

NATIONAL CYBERSECURITY STRATEGY

Any cybersecurity plan must include a clear, country-specific national cybersecurity strategy (NCS). Taking the European Union Agency for Cybersecurity (ENISA) as a reference, a NCS is a plan of actions designed to improve the security and resilience of national infrastructure and services. It is a high-level, top-down approach to cybersecurity that sets out a range of national objectives and priorities to be achieved within a specific timeframe.

A NCS IS AN ACTION PLAN DESIGNED TO IMPROVE SECURITY AND RESILIENCY OF NATIONAL INFRASTRUCTURE AND SERVICES

The NCS is should be updated periodically as changes in preparedness and cyber threats occur. A common timeframe for reviewing and updating a strategy can span four to five years.

By the year 2021, most developed countries, all European countries and approximately half of the LAC countries had adopted a NCS. Some of the countries that have approved such strategies have demonstrated significant progress in implementing their respective action plans, while several others have made no progress.

Cybersecurity is an emerging field. Two truisms are: firstly, threats are constantly changing, requiring countries to continually update to mitigate them, and secondly, that no country is perfectly positioned at any point in time to deal with all threats. A NCS will always provide an updated high-level plan for the country to maintain its capabilities and acquire new ones, and thus improve its ability to cope with cybersecurity incidents.

NCSs serve the purpose of aligning the objectives and actions of all relevant stakeholders in a country, across multiple sectors, in order to meet these goals. The process of designing these strategies presents an opportunity for dialogue among all relevant stakeholders, who may not collaborate on a regular basis. Strategies serve as a benchmark to measure a country's current situation and its progress over time. They are also useful tools for different stakeholders to make a public commitment to the actions they are responsible for undertaking.

The development of an NCS is a process consisting of the following stages:

- Collect data and assess the current situation.
- Hold discussions about current issues and objectives, and how to achieve them with a

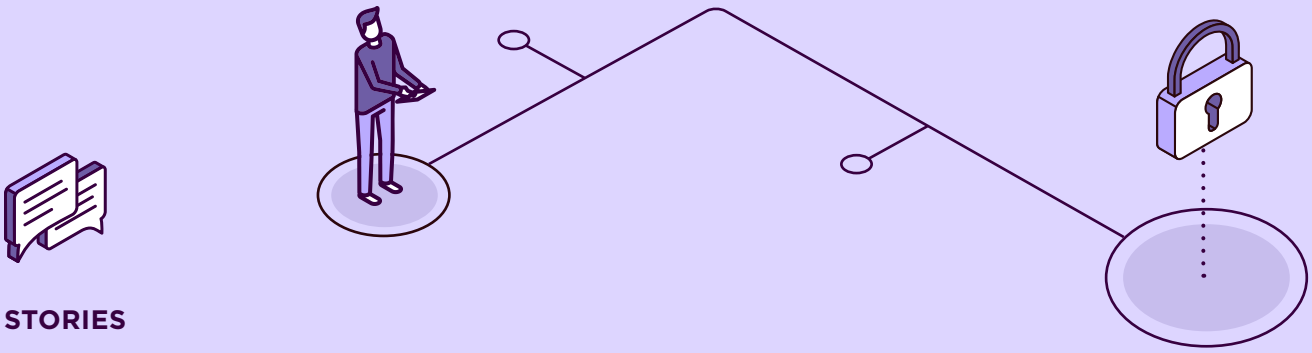
broad representation of the different sectors and relevant actors in society.

- Devise and approve a plan.
- Implement the plan, carried out by different actors.
- Monitor and evaluate implementation.
- Repeat the process regularly (every few years).

Ideally, a coordinating body is designated at the national level to carry out the different stages of this process.

As cybersecurity should be a cross-cutting capability, the following should be ensured:

- The national authority must have the necessary skills to involve and lead all parties.
- To ensure intergovernmental cooperation, the interfaces of responsibility and communication with the other national security bodies, as well as with the authorities responsible for the security of networks and information systems, must be established.
- A committee that has a unique character for the national security system will facilitate coordination between public entities at the operational level in the field of cybersecurity, in order to respond to crisis situations in a coordinated manner with all the resources of the state.
- A mechanism should be established to identify and include all private sector entities affected by or responsible for the execution of the NCS.
- The creation of a public-private partnership forum will ensure cross-sectoral cooperation with the private sector, bringing to bear all the capabilities needed to respond in a coordinated manner to cybersecurity challenges. In addition, it may include responsibilities for talent management in cybersecurity, as well as support for national industry and supply internationalization.
- The national, public, and private Computer Security Incident Response Teams (CSIRTs) should also have mechanisms to coordinate competencies and actions, in collaboration with international l CSIRTs.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo is especially concerned about the security of his computer and his cell phone, since a virus recently infected the former and caused him to lose a lot of information. For this reason, he is going to enroll in one of the online courses on basic protections for citizens that have been created as part of the country's cybersecurity strategy.

Entrepreneur
Ana

Ana has just included her company in her country's "Cyber-secure business" project. Although she is not obliged to participate, as the project has been designed only for companies classified as critical, she can see the advantages of having reinforced support for the protection of her IT systems, as well as receiving immediate alerts in case of any risk that could impact her information systems.

Vice minister of health
Sara

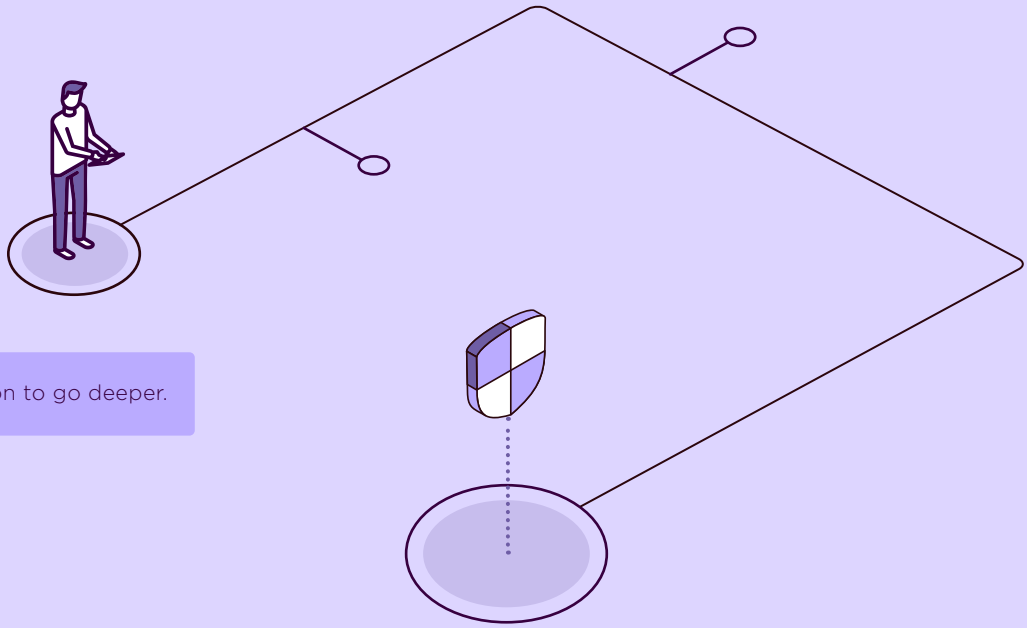
She has made the Ministry of Health part of the pilot for the implementation of security measures promoted by the Ministry of the Interior and the digital government office. It is especially important for the health sector to be resistant to attacks because of its importance for the country.

Vice minister of justice
Verónica

If there is one thing that keeps Veronica from sleeping, it's the idea that a cyberattack could crash her country's justice system. She knows from the press how previous attacks have affected other justice systems, so she has launched the Ministry of Justice's cybersecurity strategy, coordinated with the Ministry of Interior's country cybersecurity strategy.

Mayor's advisor
Daniel

The municipal government does not have cybersecurity specialists, as there are not many people in his municipality with these skills. The only way to secure his municipality's information systems is by participating in the "cybersecurity municipalities"s project promoted by the national directorate of digital government, which offers training and technological resources.



EJEMPLOS

Click on each flag or icon to go deeper.

National strategies:

Chile
National Cybersecurity Policy

Spain
National Cybersecurity
Strategy 2019

United States
National Cybersecurity
Strategy 2018

Israel
Cybersecurity Policy

United Kingdom
National Cyber Security
Strategy 2016-2021

ENISA
National Cybersecurity Strategies

The International Telecommunication Union (ITU)
A guide for the development of a national cybersecurity strategy

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a national cybersecurity coordination body?
  - Does this agency coordinate public and private sectors?
- Is there a body responsible for the protection of national critical infrastructures?
  - Does this agency coordinate public and private sectors?
- Is there an agency responsible for law enforcement in the context of cybercrime?
- Is there a body responsible for cyber defense?
- Are there organizations responsible for cybersecurity in specific sectors?
  - government
  - telecommunications
  - financial
  - energy
  - health
  - justice
  - education
  - water
  - end users (children and adults)
- Are the following functions performed by the government?
  - Long-term planning and research on cybersecurity issues (thus increasing and improving the workforce, modernizing regulatory frameworks, creating alliances with other

sectors and international actors, promoting the local private sector ecosystem, creating awareness, etc.)

- monitoring of digital assets (belonging to the government and critical sectors)
- cyberintelligence and threat search
- exchange of information
- incident response and recovery
- awareness
- operational cooperation at the domestic level
- operational cooperation at the international level
- monitoring of cyberspace and identify instances of crime, and investigation and prosecution of them.
- treatment of digital evidence
- law enforcement in cybercrime
- crisis and emergency drills and exercises.

› Is there a national cybersecurity strategy? If so:

- Was it approved by the current government?
- Was it drafted in consultation with key stakeholders, including central and sectoral government agencies, the private sector, nongovernmental organizations (NGOs), academia, and other relevant stakeholders?
- Does it include guidelines for critical sectors?

› Is there an action plan, including goals, dates, resources, and responsibilities, to facilitate the operationalization of the strategy by the different stakeholders?

1.1.6 RISK MANAGEMENT PLAN

Public administrations and lead institutions in charge of digital transformation have to serve citizens and businesses in an uncertain and constantly changing scenario. This is a major challenge as circumstances internal or external to the public administrations themselves can pose significant challenges that make it difficult to achieve their objectives. An example is the challenges posed to public administrations by the global pandemic caused by the COVID-19. In order to be able to deal with this type of situation with solvency, the lead institution and the different government ministries, departments, and agencies must carry out adequate risk management.

Risk management is not based on managing problems once they occur, but rather on working in advance to have a plan to reduce the probability of these risks materializing and, in the event that they do, to minimize the impact on the organization. To manage risk it is important that an exercise is carried out by the entities involved so that risk tolerance levels and the limits of these levels can be established.

Spending time thinking about what can go right or wrong in a digital transformation process is an exercise that can make or break it. By anticipating potential problems, it is possible to create strategies to prevent them from happening and to control their impact. It is also important to identify positive risks (they exist, and are called opportunities) in a timely and appropriate manner in order to promote them.

If a public institution ignores risk management, it is left to fate and to the responsiveness of those in charge once problems occur. The question is not whether serious problems will occur that will jeopardize all or part of the operation of a public service, but when they will occur. A lack of preparation will lead to improvised responses.

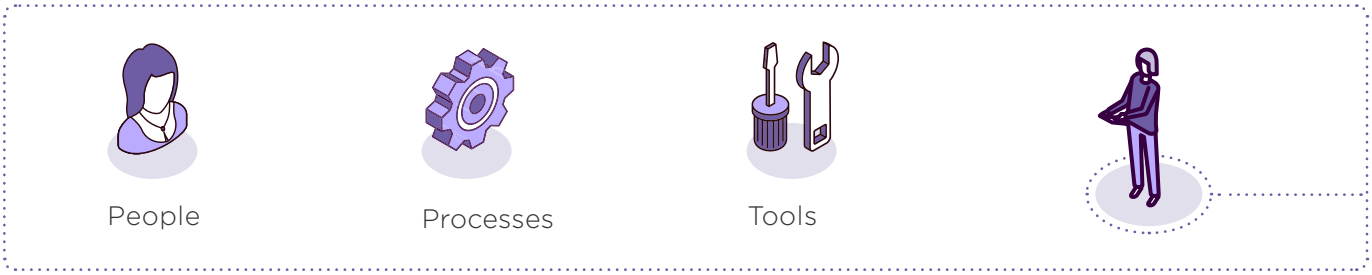
Take the case of a public institution that has had to face the Covid-19 pandemic. If that institution had identified that due to a force majeure event (flood, pandemic, terrorist threat, etc.) its employees could not come to work in person to the office, it would have been identified that, although the possibility of occurrence was low, the impact on its operation would be very high. Therefore, although nothing could have been done to avoid the occurrence of this force majeure event, it would have been possible to take actions to mitigate the impact, such as the establishment of teleworking plans, implementation of videoconferencing solutions andtraining for telework, etc.

A key aspect to be addressed in risk management is uncertainty. Identifying uncertainty and dedicating resources to explore it in depth has a positive impact on risk management by increasing knowledge about potential problems and clarifying unknowns.

Obviously, there will always be risk. It would be impossible to predict all possible circumstances that could occur and to have a plan to mitigate them. The key to risk management is to find the balance between the risks to be managed and the investment required to do so. A governing entity is capable of preventing a large number of risks that may occur. Thus, even if it were only able to prevent 60 percent of the risks, management would be positive since it would have 100 percent of its time to deal with 40 percent of the unmanaged risks.

RISK DIMENSIONS

Risk has to be managed in a comprehensive manner and has to be addressed in the following dimensions:



People

Both the governing bodies of the digital transformation and the different organizations that provide services to citizens must ensure that the functions associated with risk management are defined in their organization, and that these functions are assigned to specific people. In addition, the necessary skills must be identified to be able to undertake adequate management, and the necessary training actions must be carried out to be able to reach the required level. Likewise, the organizational culture has a lot to do with risk management: an agile private company culture (for example, a small software development company) has much higher risk tolerance levels than a ministry such as the Ministry of Defense, with a culture of stability and predictability that will be totally risk averse.

Processes

For appropriate risk management, a series of activities must be carried out to allow a global approach. These tasks can be summarized as follows:

- **Identify risks:** This work has to be carried out by people nominated in each public agency for this purpose. Normally, it is not a one-time process, but a living process that has successive iterations in order to identify potential problems that may arise. It is important that the risks that have been identified are documented and categorized. In the scope of a digital transformation program, it can be helpful to work with an institution that has already started this process, as many risks will be similar for both. It is also necessary to identify risks both of a general nature and those specific to each ministerial department or agency, such as those linked to electronic notifications. In the case of notifications, the entity leading the digital transformation will have to determine the risks linked to the integrity, availability, and confidentiality of these. On the other hand, the ministry of justice will have to identify the risks generated within the scope of a judicial procedure, such as what would happen if the notification system were not available on time and criminal liability were incurred.

- **Qualitative analysis:** Dozens or hundreds of risks can be obtained from risk identification. Risk management is not free; it requires the use of resources (financial, human, technological, etc.) of the public administration for its proper management. It is necessary to analyze which ones are to be managed and for which ones a response is to be prepared. A common technique for this analysis is to assess the probability of the risk occurring (very high, high, medium, low, or very low) and its impact (catastrophic, critical, moderate, marginal, or negligible), so that an orderly ranking of the risks to be managed can be established.

- **Quantitative analysis:** At this point, the governing body already has an ordered list of the risks it has to manage in terms of impact and probability. This list is used to assess the impacts in the event of the risk materializing and how they would affect the services provided by the public administration. This analysis makes it possible to generate a list of prioritized risks and the expected impact on public services for each of them.

- **Prepare risk response:** It is necessary to decide which safeguards to apply for each of the risks. The actions usually fall into one of the following categories:

- **Risk avoidance:** This includes the actions necessary to eliminate the possible causes of the risk. For example, if the risk identified is that the datacenter located in a building on the coastline could be flooded due to a hurricane, the avoidance action would be to move the datacenter to a nonflood zone.

- **Risk mitigation:** Actions aimed at reducing the probability or impact of the risk. Taking the above case as an example, risk mitigation actions would be to build a wall to hinder the overflow or to reduce the impact of a possible flood in the datacenter by moving it from the first floor to the second floor of the building.

- **Transferring the risk:** This includes actions aimed at finding a third party to take on the risk. This is usually done by taking out insurance or subcontracting a service. Returning to the previous example, in this case the action of transferring would consist of contracting the services of the datacenter to a third party, who would then take the necessary measures to prevent flooding.

- **Accept the risk:** This option assumes what may happen if nothing is prepared. This usually occurs when, for example, the event is so severe that no matter what is done it cannot be avoided, mitigated, or transferred, or, if it can be done, the costs are so high that it is not feasible. Returning to the above example of the datacenter, one would have to accept the reality that if a tsunami occurred, the datacenter would be unavoidably flooded, and the building housing it destroyed, so that services could not be provided normally until it could be restored at another datacenter.

Through this basic risk management process, a governing entity can identify risks, analyze them, and take the necessary measures to reduce the probability or impact of negative events that could degrade its operation or interrupt it completely.

Tools

Although the main asset in risk management is people, tools can be of great help. When the volume of risks increases, it is necessary to have a system that allows the institution to keep in a common repository the risks, to identify the possible relationships between them, to provide assistance when performing analysis, to have a catalog of safeguards, etc. There are a wide variety of tools on the market that enable these functions to be carried out. In the field of public administration, the

Pilartool,[9] used in the Spanish public administration for the management and analysis of ICT risks, is one example.

RISK MANAGEMENT METRICS

The level of maturity of a public administration and its resilience to unplanned events is often reflected in risk management metrics. Some examples of these metrics of both a strategic and operational nature are identified below:

1. **Strategic:** Cost of managed versus unmanaged risks. Given that, in the case of managed risks, the cost is known a priori through quantitative analysis, it is possible to determine what the cost of a materialized risk would be with and without a prepared response. The quantification of this cost can be compared with the cost of the safeguards, so that the return on each dollar invested in safeguards can be calculated.

2. **Operational:** Percentage of unmanaged risks out of total risks materialized. The materialization of risks that are not managed can give an indication of how well risk management is being carried out. If of all the risks that have materialized in the last year, only 5 percent are not managed (they are identified and analyzed and have associated safeguards), this indicates that the risk management process is being carried out satisfactorily. If this percentage, on the other hand, rises to 40 percent, this may indicate that the way in which risk management is being undertaken needs to be reviewed.

RISK MANAGEMENT COORDINATION

Finally, it is important to mention a: the coordination of risk management between the governing bodies of the digital transformation and the various agencies that offer services to the citizen. Coordination is important because of the following:

1. **Avoiding duplication and maximizing synergies.** Public agencies can leverage a lot of effort related to risk management if they are able to reuse, at scale, the plans from which they can benefit.

2. **Chained risks.** Related to the previous point**,** when a digital transformation governing body offers services and components common to the different vertical sectors of digital public services, it is very likely that if a risk materializes in one of them, the rest may be affected. For this reason, management plans must be perfectly coordinated.

9. https://administracionelectronica.gob.es/ctt/pilar#.YEvznp1KguU

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

In his city there has been a terrible storm that has caused significant damage to the city's infrastructure. Camilo is positively surprised that, despite the situation in the city and the fact that the streets are impassable, so that civil servants, like other workers, have not been able to go to their jobs, the city council continues to provide accurate information on recommendations for citizens and is reporting the status of roads, schools, hospitals, etc.

Mayor's advisor
Daniel

Two years ago, Daniel was working on the municipal risk plan in case of adverse weather events. This plan took into account the phenomena that have occurred in the city in the last twenty years, such as floods, tropical storms, and heat waves. For each of these events, actions to be implemented were identified. Specifically, one of the actions that was implemented a year ago was the initiative that allowed public workers to telework from their homes in the event that they could not travel to their workplace. The city council requested that all workers who could telework do so one day a week, so that the teleworking system would be tested and known by the workers in case it had to be used. When the weather agency's storm warning came through, the mayor's office instructed them to work from home until further notice. Daniel is very satisfied, since not only has he been able to preserve the physical integrity of the municipal employees by preventing them from traveling through the dangerous streets, but also he has been able to ensure continuity in the provision of public services.

1.1.7 MONITORING PLAN

> ***"WHAT YOU DON'T MEASURE, YOU DON'T CONTROL, AND WHAT YOU DON'T CONTROL, YOU CAN'T IMPROVE."***

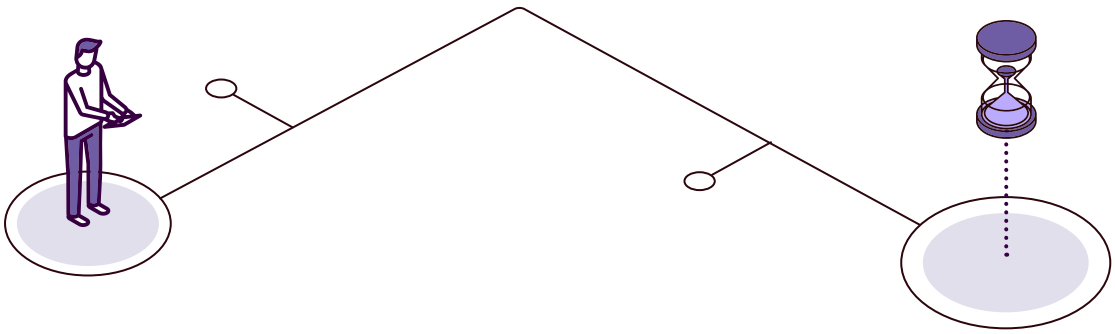
This quote by William Thomson Kelvin captures the essence of how essential it is for a government or a specific sector that is immersed in a digital transformation process to be able to monitor what is happening—both to know what results or benefits are being generated for citizens and businesses and to know what state the different ministerial departments or agencies are in.

Monitoring is the development and maintenance of a measurement capability that meets the needs of a public administration. It can be applied to the different organizational levels of public institutions:

- **Strategic level:** Provides information on the level of achievement of the organization's strategic objectives. Strategic level indicators are usually obtained from the combination of tactical and operational indicators.

- **Tactical level:** Information is obtained on the different departments of the public institution. This can come from the level of implementation of digital transformation projects, the progress of regulatory development initiatives or the progress of construction work.

- **Operational level:** This is the level closest to the service provided. It provides information on the behavior of the services as they are being provided at the moment—for example, the number of traffic penalty payments made through a website.

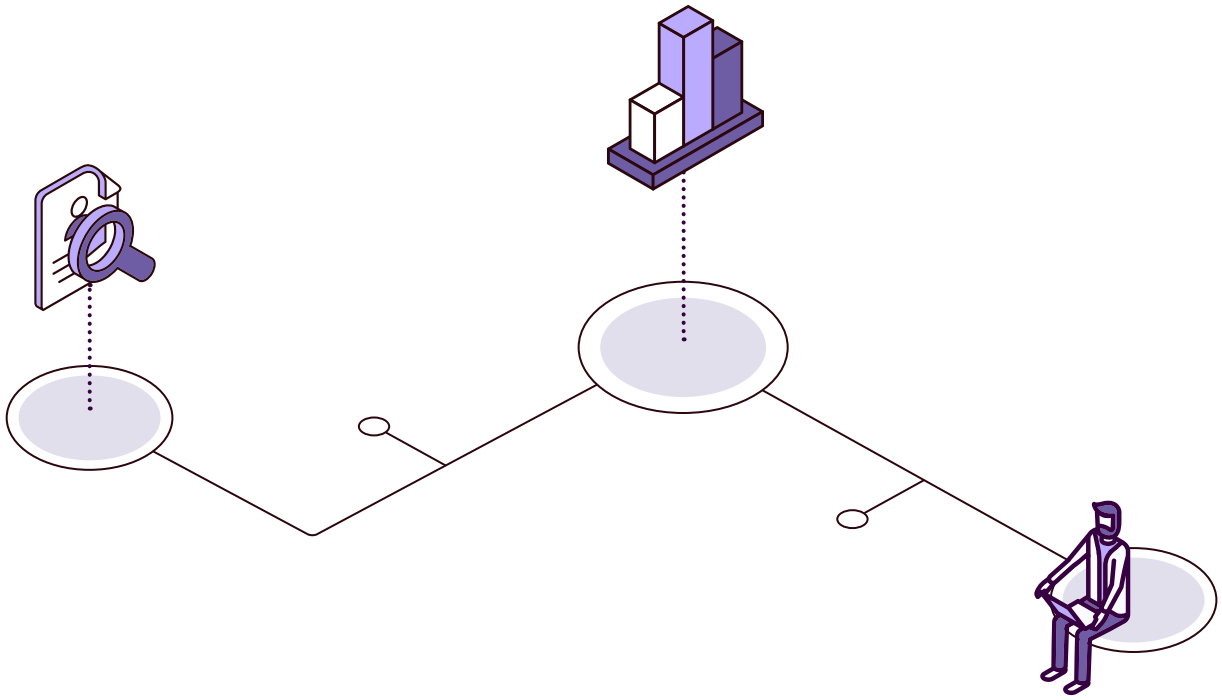


MONITORING METRICS

The indicators used to monitor an organization can be of two types:

- **Performance metrics:** These are usually results-oriented and easy to measure but difficult to improve. In the case of a digital transformation program, this could be the percentage of fines paid online versus fines paid physically at a municipal office.

- **Performance predictor:** These are usually difficult to measure and easy to influence. Going back to the previous example, a performance predictor could be the number of citizen interactions with the fines payment website.



ADVANTAGES OF MONITORING

The benefits of monitoring are evident for an institution leading digital transformation making it possible to evaluate whether the objectives set out in its strategy are being met. In addition, monitoring systems allows the institution to establish a framework for continuous improvement so that the following actions are taken:

- The current situation is monitored through the indicators that have been identified.
- Improvement actions are established at the organizational level.
- The behavior of the organization after the improvement actions is remeasured through the same indicators. These data are used to analyze whether the improvement actions have been positive and should be maintained, or whether they have been negative and should be reversed and new ones identified and implemented.

Through this process, objective measurements can be obtained in light of the indicators selected.

If a public administration is immersed in its daily operations or in a transformation plan and does not deploy an effective monitoring strategy, it will not be able to know exactly how it is doing, nor if everything is working correctly and providing the expected service. It will be extremely difficult to identify what is being done well or what area requires some adjustment. The only tool at your disposal will be the subjective opinions of the users and operators of the service, but making decisions with this level of uncertainty implies assuming a high level of risk.

On the other hand, just as damaging as not having a monitoring strategy in place is having one, but executing it poorly. If the indicators are poorly selected or calculated, a false sense of security can be generated. Returning to the example of online fine payments, if the indicator selected is "*number of fine payment procedures successfully completed via the internet*" and it provides a more or less valid figure, it can be assumed that the system is working correctly. However, if this indicator is complemented with others that provide an overall view of the problem, such as "*number of fine payment procedures initiated (regardless of whether they have ended well or poorly),*" it would be possible to check whether the number of procedures that end successfully out of the total is a high or low percentage of the total. In this way, in the case of a low number, improvement actions can be identified to improve the procedure.

MONITORING OBJECTIVES

Another fundamental aspect when determining a monitoring strategy is to establish its objectives, which will probably be identified in the strategy itself, but may also need to incorporate

a regulatory or public service point of view. For example, a public institution must monitor that the emergency telephone number is operational 24-7 and that, in the event of problems affecting availability, the service can be recovered in less than fifteen minutes.

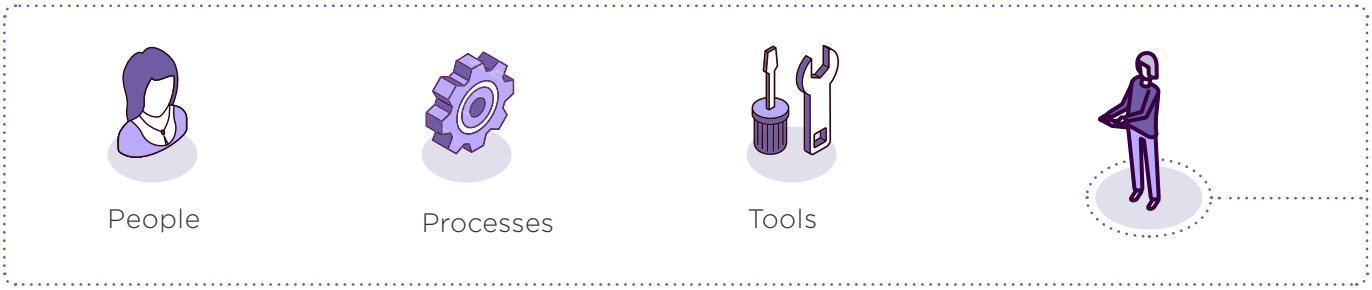
Once the monitoring objectives have been defined, indicators must be specified and transformed into quantifiable elements. A good practice in this specification is to categorize the indicators, for example, into economic, social, efficiency, etc., so that they can be managed together.

SOURCES OF INFORMATION

A key exercise to be carried out in the monitoring strategy is the identification of information sources, as this directly influences the quality of monitoring. These sources can come from information systems, surveys of users and/or workers, etc. All this collected information must be aggregated and stored, and then the data must be analyzed and results obtained.

DIMENSIONS OF MONITORING

In order to carry out monitoring, it is important to identify actions in the three dimensions:



People

Organizations need the necessary human resources to define, collect, analyze, and obtain measurements. These people, in turn, need to be adequatelyqualified and trained to perform these functions. In addition, an organizational culture that values transparency, the exchange of information throughout the organization, and the promotion of continuous improvement has an important role to play in monitoring. Therefore, it is essential to promote a cultural change toward these aspects in order to achieve efficient monitoring. It is also important to consider the need for measurement and monitoring in all functions performed in the organization. As such, a considerable number of sources of information will be readily available to cross-reference data and obtain valuable indicators.

For example, information should always be available on the types of procedures that are carried out and the number that are carried out. Thus, if a civil servant carries out paper-based procedures at a counter, he/she should complete a daily form identifying the types of procedures he/she has carried out and the number. In the case of an information system, it should provide a dashboard reporting the same data.

Process

The establishment of monitoring is usually deployed through a process. Typically, activities are grouped around two main areas:

- **Measurement and analysis:** This first point involves activities aimed at answering the following questions: What do I need to measure? How am I going to measure it? How do I extract the information? What analysis can I perform on the data collected?

- **Delivery of measurement results:** At this point, the activities that are carried out answer questions such as the following: What measurements can/need to be obtained? What do the measurements I am collecting tell me? Where can I store these measurements? What, how, and to whom do I communicate the results?

Tools

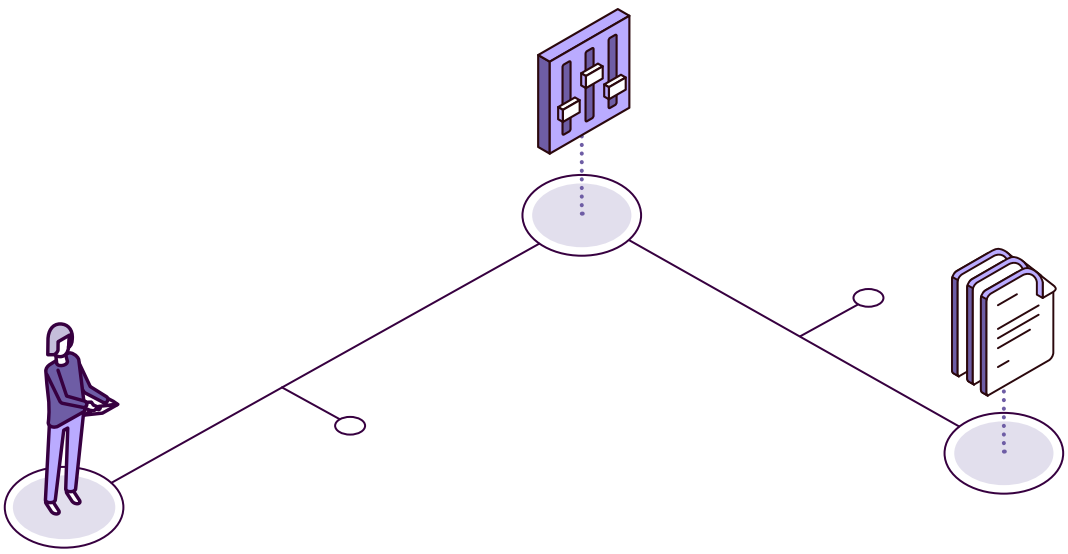
Tools are an important element of monitoring. On the one hand, there are those that allow the inventory of information needs with their details, which makes it possible to keep track of the evolution of these needs. On the other hand, specific tools are required for the extraction of information and subsequent processing of the data to ensure that the measurement is of the highest possible quality. Finally, it is possible to use a report to a control center where activity is constantly monitored. It is also advisable to use a dashboard in which indicators are displayed, and their trends are shown and compared with other periods, geographies, or situations, etc. Now, although the data-oriented part of an organization includes more aspects, it is true that monitoring provides very important information. Therefore, if compatible tools are used for both data-driven management and monitoring, the complexity of these functions will decrease significantly.

A public institution needs to identify the status and level of coverage of its monitoring. When establishing metrics, it is important that they are level-appropriate. That is, from a strategic point of view, metrics that indicate how many insertions are being made into the database are not expected. This data provides little or nothing at this level, although this same information can be particularly useful at the operational level.

The following includes some sample metrics at different levels:

- **Strategic:** Percentage of business objectives monitored. It is important that each of the strategic objectives be identified in the monitoring strategy as an element to be monitored. Based on this monitoring of each objective, it will be possible to establish the level or degree of progress of the strategy and thus have an important basis for taking data on it. Strategic indicators usually require prior monitoring of the rest of the tactical and operational layers.

- **Operational:** Average time to identify a problem on a digital public service. If a public administration is able to monitor in real time the indicators of a digital public service, it will be able, on the one hand, to see how it is behaving and, on the other hand, to validate it with the expected behavior based on data from similar periods (same day of the previous year or average of the last ten working days). In the event that notable differences appear, the necessary actions can be triggered to determine whether the behavior is legitimate or whether it is due to a problem with one of the components of the process. Through metrics of this type, it is possible to assess the public institution's ability to act proactively on indications that may affect its performance versus reacting once the problem has materialized.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

The last few weeks she has been preparing the budget for next year. Resources are scarce and do not meet all the needs she is facing. Through the monitoring system that has been implemented a few years ago, she is able to identify the impact of investment in different medical specialties in terms of reducing waiting lists. For the same investment in one specialty, the reduction in waiting lists can be as high as 40 percent, while for others it is as low as 15 percent. Given that one of the objectives of government is the reduction of waiting lists in healthcare, Sara will use this data to allocate most of the budget to the specialties that reduce waiting lists the most.

Mayor's advisor
Daniel

Daniel is working on a new municipal information system for tax management. Following the commissioning of this system, it has become apparent that in the last fiscal year only a total of one thousand requests for processing have been submitted through the system. These requests represent a very small volume, as the expected average volume is two hundred thousand requests. The monitoring of the service shows that the cost per electronic application is very high and the congestion of the municipal offices dedicated to the management of taxes has not been alleviated. To improve the use of the new computer system, a series of actions have been prepared, such as an advertising campaign and a 1 percent reduction in taxes payable if the processing is carried out electronically. Once this battery of actions has been implemented, it will be necessary to remeasure the volume presented and evaluate whether they have been successful or not.

EXAMPLES

Click on each flag or icon to go deeper.

Chile
Follow-up of the digital strategy

Spain
Traffic condition monitoring

Spain
e-Government Observatory

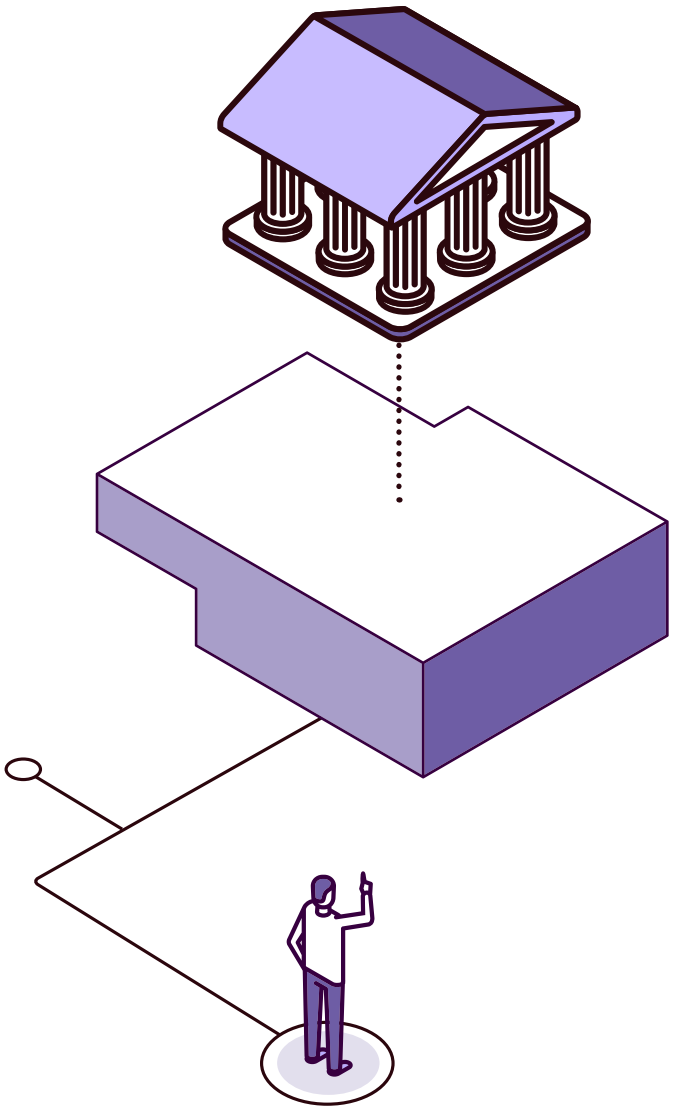
Unesco
Observatory on the Information Society

European Union
European IT Observatory – Market Reports

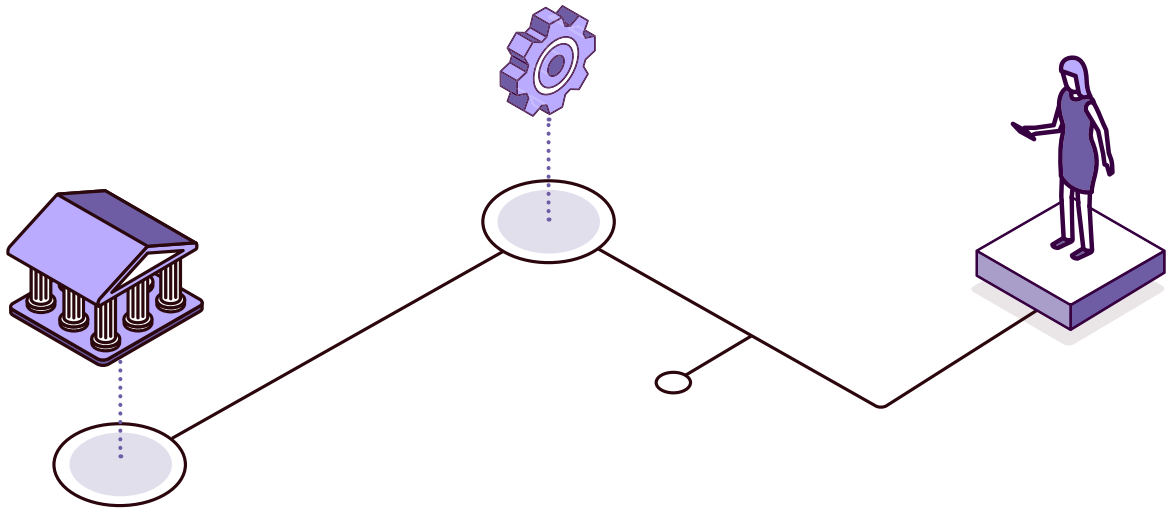
INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Have the strategic objectives for the government's digital transformation been established? If so:
  - Do the indicators allow to measure whether the objective has been achieved?
- Have tactical objectives for the government's digital transformation been established? If so:
  - Do these indicators allow to measure whether the objective has been achieved?
  - Are they aligned with the strategic objectives?
- Have the operational objectives for the government's digital transformation been established? If so:
  - Do these indicators allow to measure whether the objective has been achieved?
  - Are they aligned with tactical objectives?



1.2 Lead institution



Institutional framework and governance are sometimes the least developed aspects of digital transformation strategies, and in many cases they are precisely the most important. In general, all countries have laws and regulations related to digital transformation, since, like any other administrative area, it is regulated through norms. On the other hand, when talking about digital transformation, everyone refers to the technologies to carry it out, as well as to the information systems, so that the institutional framework and governance are often forgotten, even though they are absolutely essential to achieve a country's digital transformation.

It is a constant that in all countries that have been successful in digital transformation there is a lead institution for this process. This is no coincidence: its existence is indispensable for success. Moreover, coordination mechanisms and joint action by public institutions are the only way to achieve a coordinated country effect and not a messy amalgam of independent actions.

It is very important that the relationship with citizens and companies be defined in the institutional and governance sphere, to ensure that the steps taken and the actions carried out really respond to a demand and are useful for citizens; and because it is essential to publicize the projects of the institutions, so that citizens and companies can adapt and take advantage of them. Without appropriate governance it is impossible to align the capabilities of institutions and the needs of citizens and businesses, which is why it is a fundamental element for the success of the country's digital transformation.

The lead institution should be configured as the entity in charge of driving the digital transformation agenda, in the broad sense. This includes participation in or even direct drafting of ICT regulations, leadership of the governance of the country's digital transformation, and responsibility for the provision of common ICT services for the entire state (even if in some cases it does not provide them directly). In some countries, the mandate may be limited to digital government understood in terms of central and reusable tools, while in others the mandate may encompass cross-sectoral coordination to transform socio-productive sectors of society such as education, health, culture, and tourism.

Having coordination in the hands of a single unit allows the institution to do the following:

- Receive comments from companies or institutions for the provision of useful common services or to make adjustments to existing ones.
- Collect requests or technical possibilities and transfer them to regulatory developments.
- Have a system to oversee technology procurement within the government. This ensures alignment with digital transformation policies.

In cases where this institutional framework does not exist, problems such as the following can appear:

- **An uncoordinated policy, with duplication of expenses and solutions that should be common services:** This leads to problems similar to those in other administrative areas, related to the repetition of unnecessary investments, but in this case the problem is even more serious since it affects the service to the citizen.
    - For example, if two ministries have two contracts for the transport of boxes, a service that they use 50 percent of the time, and, therefore, it is a duplicated expense that could be shared, efficiency and public money is lost, although as such it is not impacted. However, if two ministries create two different electronic identification systems, not only do they lose money and efficiency; citizens have to register in two different systems, and this adds complexity and possible loss of public services.

- **Complexity in the provision of common services:** This not only makes ICT projects more expensive or complex for citizens; the lack of common services is also a major difficulty in relation to digital transformation. If these common services exist, the different sectors (which are the ones that really provide value to the citizen) have to create and duplicate them, which prevents services from being deployed with the speed required, impacting the service.

    - For example, a hospital is built, and the health sector itself has to build a dam and water supply, build an access road, set up a power plant, and create a communications company. Not only would the costs skyrocket, but the project could become unviable, and the public service would no longer be provided. Well, no one would think of building a dam to provide water for a hospital. The same goes for the creation of a specific digital identity for a sector, and it is something that is very common.

The importance of the lead institution is not limited to the management (with direct provision, or checking its good performance) of common services. It is also fundamental for other activities:

- It must be the institution that represents, guides, and facilitates the relationship between technologies and regulations. It must advise, to maximize the development of different public policy projects within the scope of the law, and it must also have the opportunity to express an opinion to indicate that the implementation of any of these projects is impossible or implies a high cost.

- Also, nowadays, practically all public projects and policies have a strong technological component, and the lead institution must act as guarantor to ensure that the technologies needed for public projects are ready at the time when the regulation or public policy has to go into effect. It is common that sometimes very well thought-out projects and laws fail because when they come into force there is no information system related to the project to make it viable.

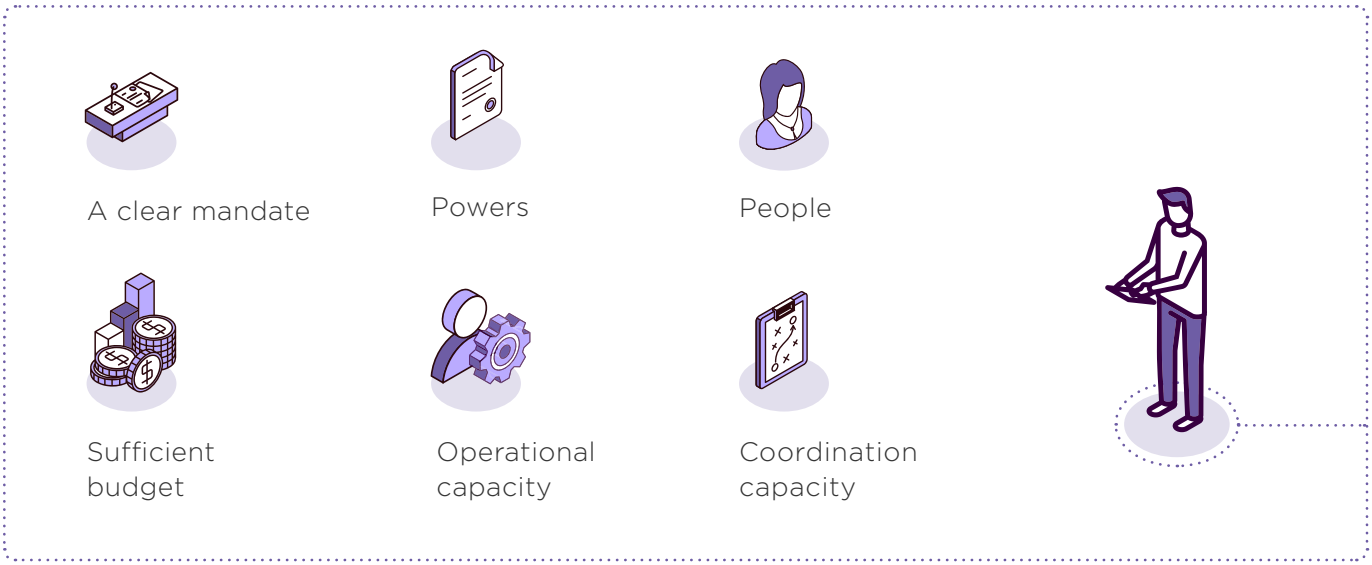
In this sense, it is not only the participation and regulatory control of high-level public projects that are fundamental. Because of the particular characteristics of technology (this is not specific to information technologies, for example; it also happens with industry, pharmaceuticals, and standardization of devices, among other cases), standards and norms are needed, in technological detail, to regulate digital transformation projects (from digital identity to the form of the electronic document; from the digitization of documents to interoperability). These standards and norms will make it possible to define the way in which multiple actors will be able to exchange information or relate to each other, or in cases where there are a multitude of options for a problem, they will make it possible to put things in order and prevent everyone from choosing what they think is convenient, since each form would be incompatible with the others. It is a matter of providing certainty (when possible) and a way of proceeding in the face of uncertainty.

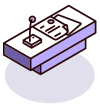
Both because of its central nature and its relationship with common services (which are the ones that most need to be standardized due to their massive use by all institutions, sectors, citizens, and companies) and governance, this unit must be able to issue detailed regulations that standardize the different aspects of digital transformation that are necessary. In the different areas subject to standardization, operational guidelines must be generated so that the different actors know how to proceed internally and with the rest of the actors.

Finally, it is necessary to have a unit to carry out the necessary coordination and governance actions, both within the institutions and with the private sector. Ideally, this unit that centralizes governance should be the one with management or regulatory development capabilities, as well as the responsibility for implementing common services, which should be supported and coordinated through these governance mechanisms.

In order to strengthen its institutional framework, avoid changes in the face of political shifts, and give a strategic and long-term perspective to something that must have this vision, the ideal is for the lead institution to emerge from the regulations, with the highest possible rank (i.e., through a law). However, this is not always possible, so in many cases the lead institution is created by second-level regulations or decrees, or it is created in the form of an agency, to give it more independence and strengthen its overall role. It is therefore important that the regulations from which the lead institution is created protect it: its role is to standardize and regulate other members of the government and other levels of government (states or their equivalents, municipalities, and other public sector agencies). The lead institution must be protected against different types of attacks and must have sufficient rank for other agencies of the same executive branch to take its decisions into account.

This institution must have several basic elements:





A clear mandate

To implement its agenda directly and/or promote its implementation in other entities. This includes direct participation in high-level regulations (laws, regulations) and the issuance of technical/operational guidelines that emanate from the above regulations. As mentioned above, as with the creation of the lead institution itself, it is ideal that the mandate is defined at the highest possible normative level, in a clear manner, and that it includes the powers that allow it to exercise its role, ranging from participation in the highest decision-making bodies to control over the hiring or management of ICT personnel, the ICT governance of the state, the capabilities in relation to the rest of the levels of government, or the areas where the institution will be able to directly generate regulations.

Powers

To promote adherence to the digital agenda, it is useful to have certain powers, such as those below (the list is not exhaustive):

- *Ex ante* control of ICT procurement, so that the state's ICT procurement must be approved by the lead institution. This ensures both strategic alignment and the aggregation of demand or negotiation capacity with suppliers by specialized personnel (something that will sometimes be very difficult to find outside the lead institution).

- Control over what is published on the government's website, in order to provide a coherent and homogeneous image, meet the criteria of usability and accessibility for citizens, etc.

- Power to generate regulations for standardization or compliance with security levels, in order to ensure a coherent and secure operation of ICTs in the state.

- Sanctioning power, so that the established regulations can be enforced.

- Functional and organizational capacity over the entity's ICT personnel, even if they are in other ministries, so that there is a coherent and efficient ICT civil servant policy.

- Exclusive authorization to participate and represent the country in cross-border ICT policy. This is important because, on many occasions, this representation is in the hands of the Ministry of Foreign Affairs, which does not always have the technical capacity for the issues discussed at the various meetings.

- Ability to establish guidelines on citizen service.

- Capacity to generate the country's data policy.

People

To manage all elements of its agenda (be it direct production, operational management of common services, supervision and/or support to other entities, or management of contracts with external suppliers), it is necessary to have people. Logically, the number and type of profiles will depend on the different competencies and powers of the lead institution, but in any case it must have a broad interdisciplinary team. In general, in some lead institutions, apart from the typical profiles of any unit providing technology services, public or private (project managers, software developers, user experience designers, accessibility specialists, etc.), there are other types of profiles to meet the broad competencies mentioned above, such as the following:

- functional specialist in public administration (including profiles that facilitate process reengineering/continuous improvement and impact on the reduction of administrative burden).

- lawyer specializing in ICT.

- specialist in ICT public procurement.

- communication and dissemination specialist (including traditional media and social networks).

- relationship manager with other public institutions, citizens, and the private sector.

- cybersecurity specialist.

- data protection specialist.

- cloud specialist.

- change management specialist.
- specialist in service centers.
- specialist in human resources management.

Sufficient budget

To finance its entire agenda, hire the necessary personnel and services, and finance or execute ICT projects in other entities.

Operational capacity

To manage common services. The convenience of having the coordination of the digital transformation carried out by a single entity is largely derived from the provision of common services required by many state institutions.

Coordination capacity

To lead the governance of the country's transformation through the forums with public and private entities mentioned in the document.

In many cases the lead institution is founded as an agency or equivalent unit to emphasize its independence, although there are successful cases in which there is no agency, but the lead institution is a standard unit of a ministry or agency. In any case, the important thing is that it has the necessary operational and organizational capacity to meet the needs mentioned in the previous points.

From the functional point of view on which the institution depends, more than from the organic point of view, it is essential that it enjoys independence. The unit will serve all ministries, all sectors, all public entities, all citizens, and all companies. If any of these actors perceive it to be too aligned with or dependent on, for example, a ministry or the presidency, collaboration with other ministries

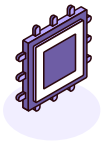
or actors may suffer, or be impacted by political changes, which may affect the functioning of the unit. These types of institutions, often due to their cross-cutting nature, and if they are recently created, are assigned to the center of government or directly to the presidency of the nation. Technical independence is key for the construction of long-term digitization policies.

In terms of work areas or subdivisions, there are several common structures in the cases studied:

Service provision area

User service area

ICT procurement area



Other areas related to ICT services

Legal area

Communication area

External relations area

SERVICE PROVISION AREA

If the unit directly provides common services, which is typical, it is important that there is an area in charge of service provision (systems/infrastructure area or equivalent). The development and creation of services must be separated from the provision of these services once they are operational, which will be carried out by another unit: the infrastructure unit. This separates roles that are distinct and require different specialties, and ensures growth and staff additions where needed. Otherwise, it would be as if the designer of an automobile were in charge of maintaining the company's fleet: they are two different jobs and have units with different specialities. One is in charge of designing or developing services or projects, and the other, in charge of providing them for use.

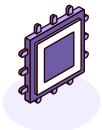
USER SERVICE AREA

Given the massive nature of common services, it is essential to have an area oriented to user service. Just as it is not good if the person who develops or creates the service is the same person who provides it, neither is it good if the person in charge of ensuring that the service is available, has good response times, meets quality requirements, etc., and must at the same time receive calls, requests, complaints, and claims from users. The unit in charge of the latter is fundamental because it represents the "visible face," the public image of the attention to the users of the common services being provided. It is typical for these common services to be used on many occasions by citizens. If this is so, it is appropriate that the responsibilities of citizen care associated with public services in general should also be part of the same institution.

ICT PROCUREMENT AREA

It is usual and useful to have an area related to ICT procurement for several reasons:

- One of the most effective ways to achieve alignment of digital transformation policies is to guarantee that no one can contract something that is not aligned with the policies; therefore, this unit can ensure that the state's ICT contracting is correct.
- ICT procurement, like any other specialized procurement (space, health, etc.), is complex and, unlike others, is necessary in all sectors, so this unit can also provide advice to the units that need it.
- This unit can perform demand aggregation. Often the companies that provide ICT services are large multinationals, with a lot of bargaining power and the ability to generate captive customers. Demand aggregation in procurement can be a powerful tool to approach a person-to-person negotiation, and with ICT procurement specialists, something that cannot be achieved with procurement broken down in hundreds of independent administrative units.



OTHER AREAS RELATED TO ICT SERVICES

It may be useful to have other organizational units. For example, one could be an area dedicated to exploring novel and risky projects. Another area within the institution that may be interesting to split off from the overall functioning is that related to the nation's data policy, in a holistic and cross-cutting manner.

LEGAL AREA

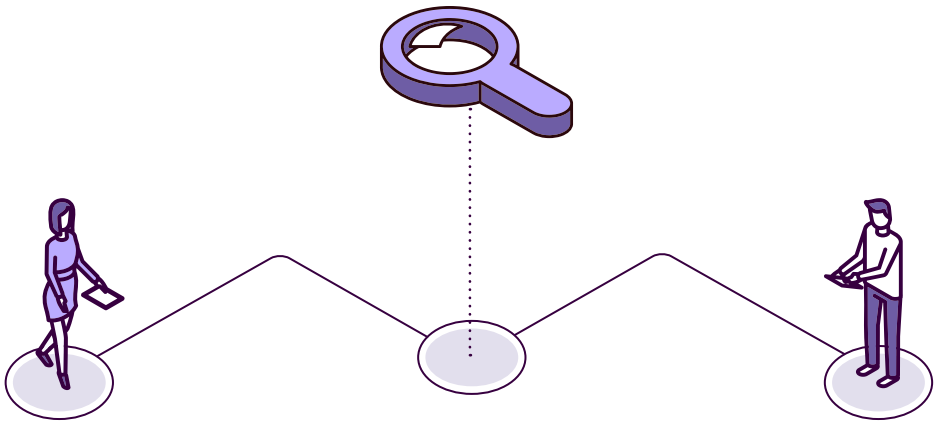
It is essential, though often difficult to find profiles with a dual legal and ICT background, or with training in only one aspect but open to effective collaboration. This area will not only be in charge of everything related to the legal needs of the lead institution; it will also provide support to other organizations, and if the unit directly provides common services, it will be in charge of the legal problems that arise in relation to their use.

COMMUNICATION AREA

This is also key because the issues to be addressed are complex, and it is difficult to communicate them well (some projects may be seen by citizens as an undermining of their rights, for example, when they may be the opposite), and because in many cases the success of the project depends on the dissemination (if the citizen is unaware of the digital identification system, it may be a failure, for example). It may (or may not) also involve the statistics and publications department, which is necessary to provide transparency to the projects themselves and to the status of the country's digital transformation.

EXTERNAL RELATIONS AREA

Last but not least, there should be an area responsible for facilitating coordination with other public entities, citizens, associations, and companies, as well as international relations.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara has to make a technology purchase to advance her goal of offering digital health services. The truth is that she does not have the ICT knowledge to face and understand the offers of the companies that can provide the service, but thanks to the news dissemination system of the ICT lead body of her country, she has used not only the advisory service, but also the aggregated purchasing service. Thus, not only has she been able to acquire the database licenses she needed with the peace of mind of having made a good purchase; she has also obtained a very significant reduction with respect to the budget she had estimated, since he has made an aggregate purchase of all the government agencies that needed this type of licenses.

Citizen
Camilo

Camilo is delighted with the announcement he has just received through social networks. He did not know that with the digital identity he already had for having done tax-related procedures, he could, from the comfort of his home, apply for the subsidy needed for the sustainable energy reform of his home offered by the Ministry of Industry. So, he decided to start following the country's digital government governing unit on Facebook, because he has seen that there are many services he did not know about that will make his life easier from now on.

Entrepreneur
Ana

Ana is celebrating in her company. Recently, a common service has been implemented in her country that allows firms to receive all notifications and communications from all public entities in one place. Moreover, apart from the web interface, her company has been one of the first to integrate its internal business management system with this common service, and the receipt and distribution of these notifications within the company is not only electronic, but happens automatically. Now they are celebrating, because the idea of this service came from their firm, in a forum on governance in which they participate together with the governing entity, and this entity, in the acknowledgements of the informative page of this common service, has recognized the role of Ana's firm in proposing and promoting this service.

EXAMPLES

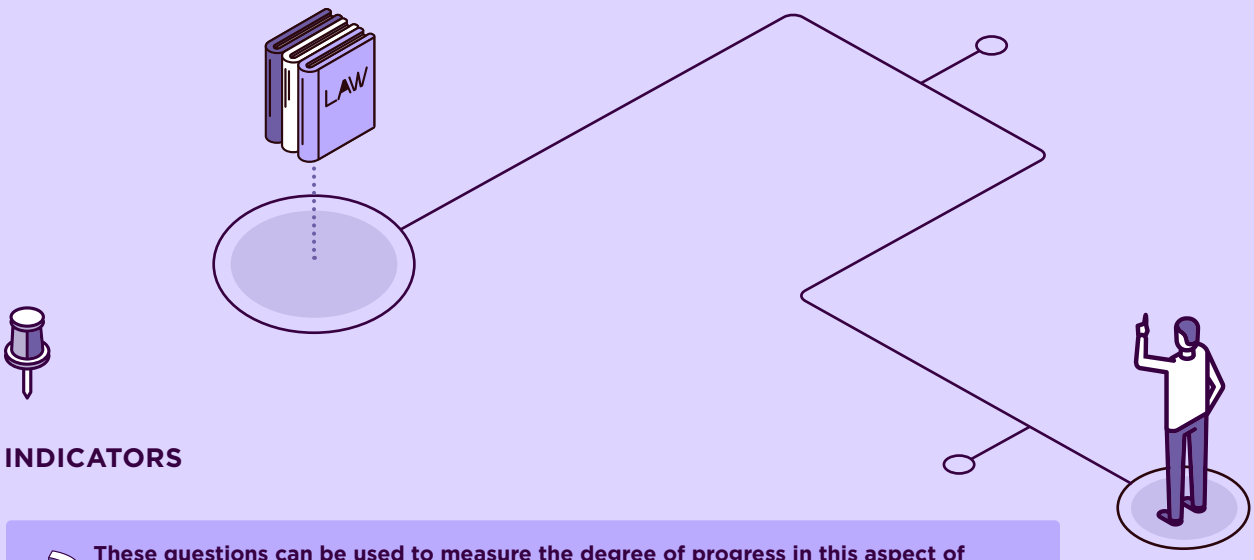
Click on each flag or icon to go deeper.

Uruguay
Agency of Electronic Government and Knowledge Society (AGESIC)

Spain
The current General Secretariat for Digital Administration (SGAD)

Panama
National Authority for Government Innovation (AIG)

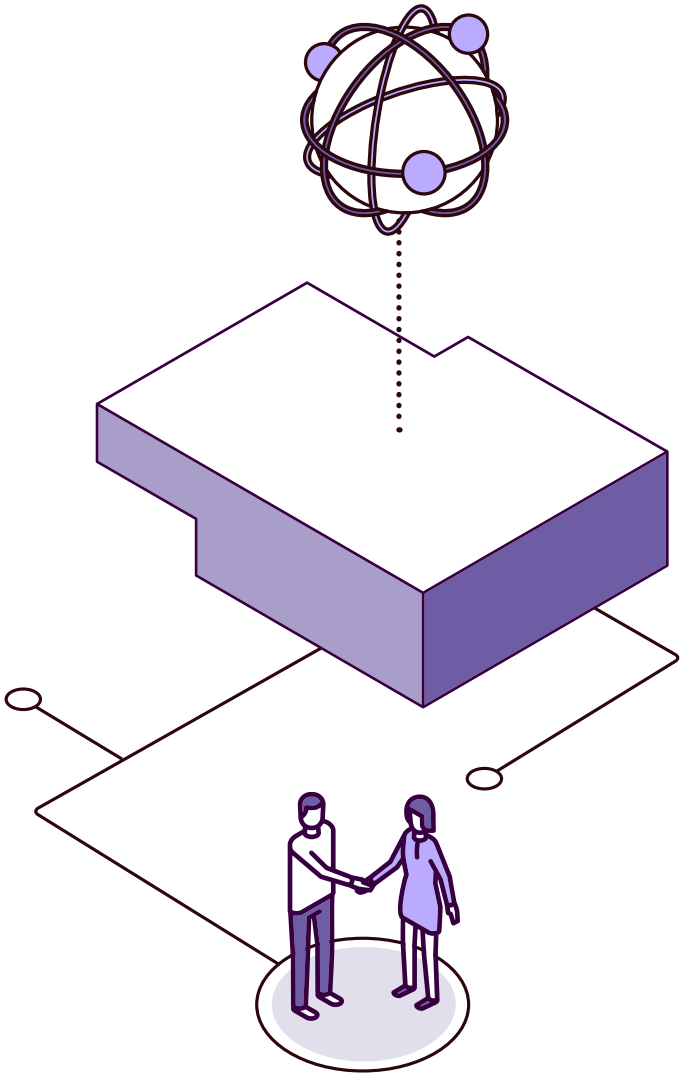
United Kingdom
Government Digital Service (GDS)



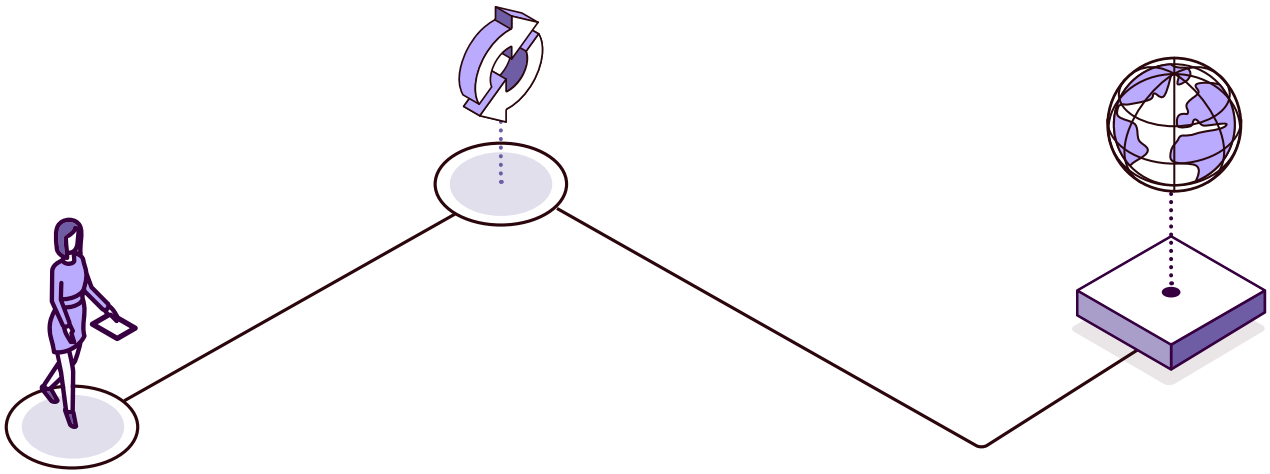
INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a regulation that establishes the mandate of the lead institution?:
  - What type of regulation is it (law, decree, plan, etc.)?
- Does the institution in charge of the digital agenda have the following powers? IF so, has this power been used in the last twelve months?
  - legal authority to intervene in the processes of other entities.
  - imposition of administrative sanctions in other entities.
  - issuance of technical regulations for the simplification of procedures or technological tools.
  - control over the publication of content on the web pages of other entities.
  - ex ante approval of ICT purchases.
  - management of competitive funds that entities can use to implement digital projects.
  - coordination of the national digital transformation agenda with public sector stakeholders.
  - coordination of the national digital transformation agenda with private sector actors.



1.3 Governance mechanisms



Large digital transformation projects, in most cases, become massive undertakings that not only involve technological aspects, but also contracting and procurement, change management, training, cultural change, communication, and logistics distribution, to name a few.

Most government units facing this type of major transformation processes think of a project office (or PMO) to organize all these tasks, but the reality is that in the vast majority of cases this is not a measure that alone will guarantee success in achieving the objectives. This is especially true when there is a lead institution for the country's digital transformation, in coordination with the different vertical sectors that make up the set of administration services for citizens.

It should also be borne in mind that major digital transformation processes usually involve different actors, some of whom depend on the organization or sector to be transformed (internal stakeholders) and others external to it (external stakeholders). Imagine, for example, that you want to transform government health services: you will not only have to take into account the professionals working in the competent authority, but also doctors, hospitals, private medicine, ambulance companies, and even other ministries or agencies that may be involved. If, in addition, it is taken into account that there may be regions in the country with competence in the matter, the challenge multiplies.

Therefore, governance mechanisms must be formal instances, with legal support, where binding decisions are made for digital transformation, both at the central government level and with the rest of the institutions. The latter is especially important in contexts in which subnational governments have significant powers.

Digital transformation and the associated technologies are subject to rapid change, as they face much faster cycles than those of other disciplines, such as law, education, or healthcare. As a result, the timelines of general regulation of public entities, where laws can last ten years or more before being replaced, do not keep pace with technological changes. Even if the regulatory framework follows a hierarchical scheme, where laws are abstract and are defined in lower-ranking regulations, technological times do not conform to typical regulatory development.

Additionally, for projects to be successful, coordination and decision-making are needed, especially when the objective is the digital transformation of the country, not limited to one sector or one entity. Naturally, these kinds of transformations have a horizontal impact on various organizational structures, affecting different stakeholders. To ensure that the changes are introduced efficiently, all of them need to be coordinated, and ICT steering committees are necessary for this purpose.

These challenges are minimized through the committees, where solutions to the various challenges of the different projects are agreed upon, minutes are taken, and their conclusions are binding. As such, problems related to the lack of knowledge of the possible challenges of a project are solved (since all the entities involved can express them) and unity of action and coherence is achieved (since it is necessary to act according to the conclusions of the committees). These committees also allow for monitoring and serve as forums for accountability.

There may be committees at different levels, of different compositions, with different mandates for different purposes. Four common committees are highlighted below.

INTERGOVERNMENTAL COORDINATION

Intergovernmental coordination

Executive level: ministerial- or vice-ministerial - level committee

Operational level

Technical working groups

Given the autonomy that many subnational governments have, coupled with the fact that they are often marginalized from central government projects, despite often being the main service providers, the inclusion and participation of subnational governments is of the utmost importance for a true national transformation.

EXECUTIVE LEVEL: MINISTERIAL- OR VICE-MINISTERIAL-LEVEL COMMITTEE

In order to reach major country-level agreements on digital transformation, it is necessary to operate at a level equivalent to that of ministers or immediately below them. For this reason, it may also be useful to have a committee to deal with issues of significant impact for the country, with that level of representation, meeting at least twice a year. This type of committee is useful because, although in general it will not deal with technical issues, it can approve state policies and demand, follow-up reports. Few tools are as effective in advancing digital transformation as the fact that a minister, in a meeting with the rest, sees that his or her ministry has lagged behind in the implementation of electronic signatures, for example.

OPERATIONAL LEVEL

Ideally, committees are legally created and have a binding character (e.g., through the figure of a "collegiate body" or similar). Due to the difference that often exists in terms of powers to exert influence at the central level of government versus the subnational levels, the presence of a committee (or collegiate body) that is more assertive with the rest of the central government (where it can "impose" more) and that is led by the governing entity of digital government in the country is desirable, together with another that is aligned with the rest of the public agencies (municipalities, autonomous communities, states, autonomous bodies), where they have less competences (due to the autonomy that these entities may have, they should proceed more on the basis of consensus). In some cases, such as that of certain federal governments, the latter should be more of a consensus committee since on many occasions, given the distribution of powers, the central government cannot impose policies on the states or municipalities. In the case of the federal or central government itself, there may be a policy steering committee, since the government should have control over its ministries or agencies. Similarly, there may be ICT operational committees by sector. These should be able to make decisions that transcend the strategic, go down to the tactical and have binding

power over other public entities. A good composition for this type of committee is that the heads of technology from each of the agencies should be part of it. This ensures the presence of a sufficient technical component, as well as the commitment of the public institution they represent.

TECHNICAL WORKING GROUPS

Finally, some issues or projects will merit the creation of technical working groups, for example, with IT specialists in charge of the documents, progress, or conclusions for approval by the operational committee. These working groups may be delegated decisions related to the types of data to be included in the interoperability platform, the technical standards for electronic signatures, the mandatory metadata for the electronic file, etc. These groups will generate documents and guidelines that will be approved by the committee, so that they will become binding for its participating entities.

A multitude of different issues can be managed through these governance structures. For example:

- activities related to operational management, such as demand management coordination or architecture management
- regulatory matters that will affect both the lead institution and the various vertical sectors in the country, such as a data protection decree or a cybersecurity regulation
- initiatives such as the technical coordination and implementation of the electronic signature service

In short, it is a matter of generating structures that are sufficiently flexible and at the same time formal, capable of addressing all those issues that can be coordinated by more than one agent involved in the digital transformation, whether they are organizational, semantic, legal, or technical in nature.

It is important for committees to have a preplanned schedule in place. The existence of an established calendar with clear milestones to be achieved can motivate the different actors to fulfill their responsibilities. Ideally, given the issues to be addressed, it would be important that at least the central government committee meets once a month. Meetings with all institutions, with binding effects, should not be less than two per year.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Mayor's advisor
Daniel

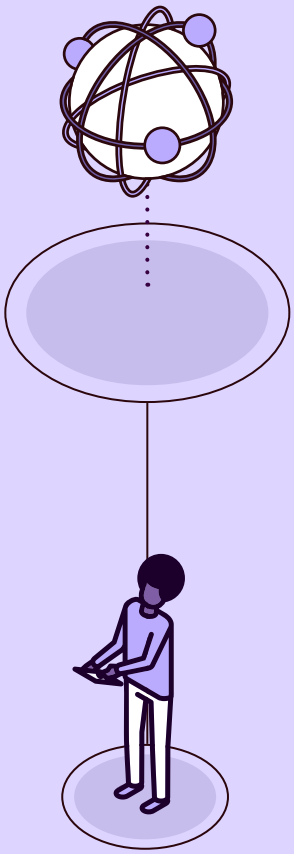
As advisor to the mayor of a municipality, Daniel sees that there is a regulation that is going to become mandatory for the entire state. He does not understand how the government has not realized that this regulation is impossible for public entities such as his own to comply with. With minimal changes, the objectives could be achieved and the negative impacts on his municipality could be avoided, but Daniel has no committee to which he can bring these proposals.

Vice minister of health
Sara

Sara was summoned to a meeting with Manuel, the country's head of digital government. Manuel has reached agreements with his fellow ministries (including the Ministry of Health) and other public entities to drive and standardize a state project. It seems that everything is fine, but Sara is concerned that, throughout the project, which will take time, there will be some body that will make unilateral decisions and generate problems in terms of the consensus reached. She would love to have published minutes that are binding on all the agencies.

EXAMPLES

Click on each flag or icon to go deeper.



Spain
Royal Decree 806/2014, on the organization and operational tools of information and communications technologies in the General State Administration and its Public Bodies.

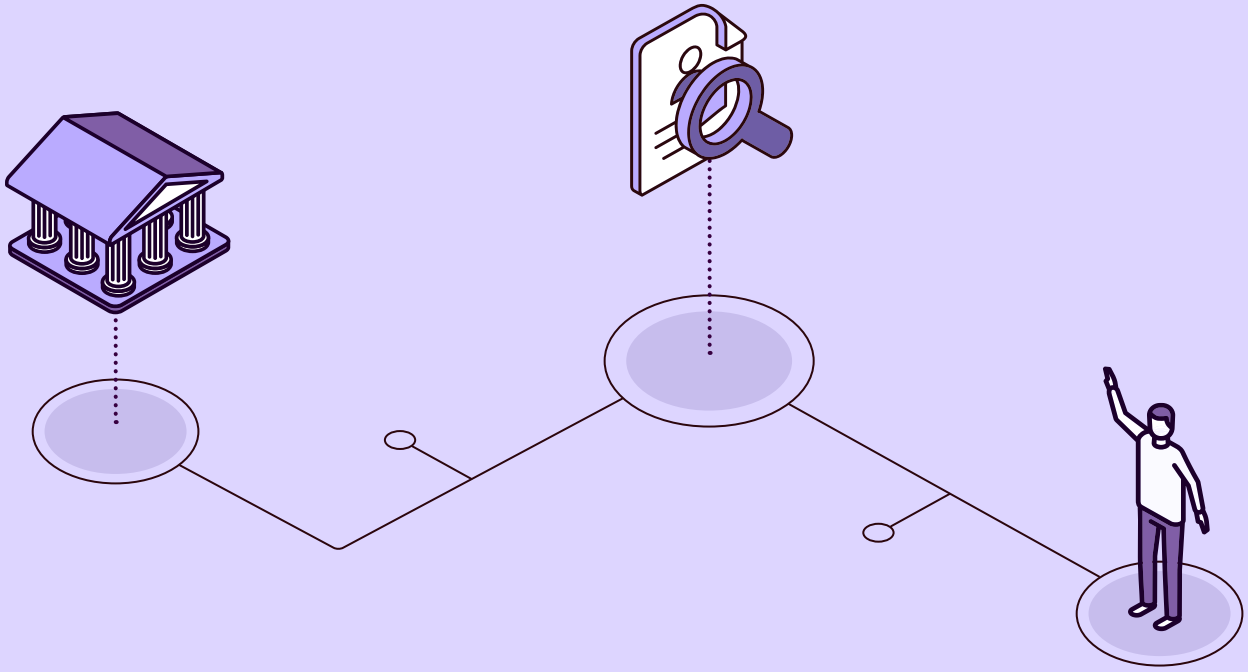
New Zealand
Digital Government Partnership

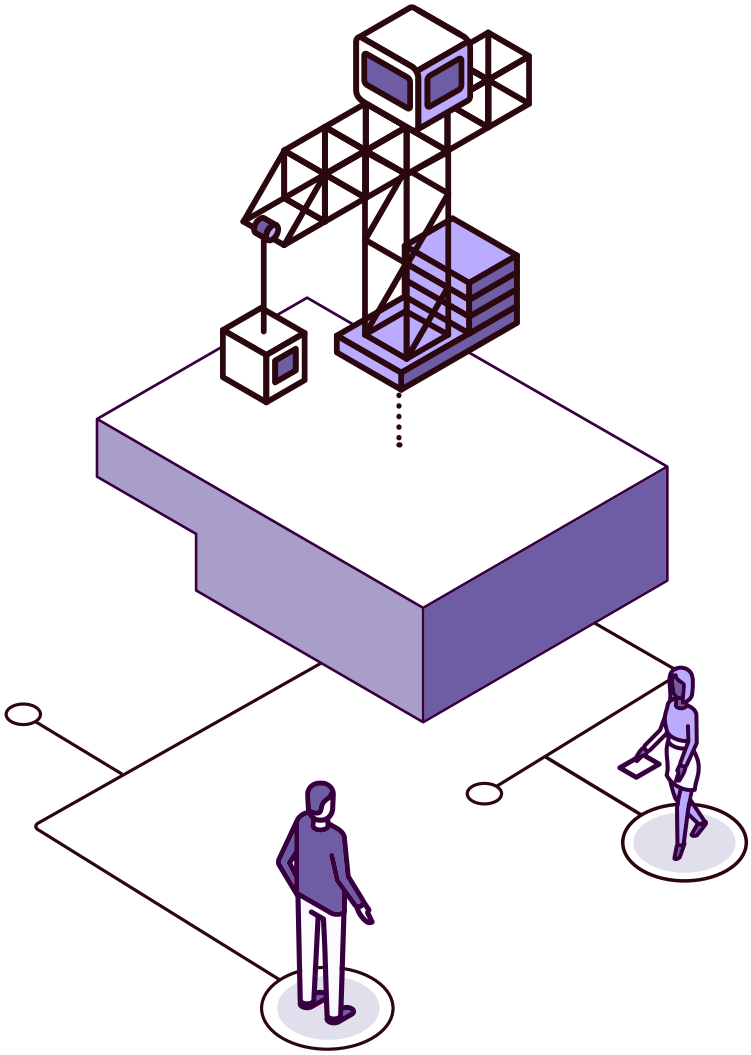
INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a formal collegiate body in the central government in which the ministers or functional heads immediately below the rank of minister are represented, where issues related to the impact of the country's digital transformation can be discussed?, If so:
  - If so, are the resolutions of this body binding?

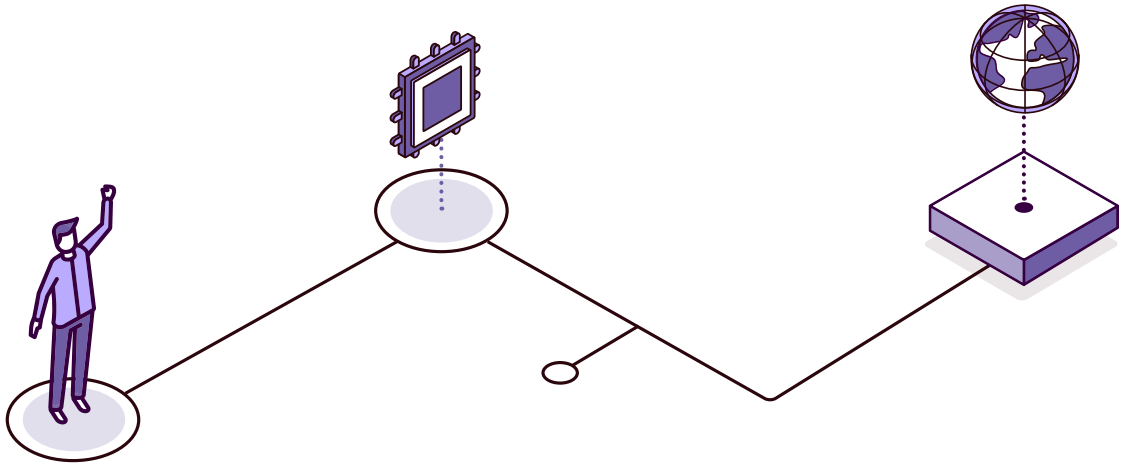
- Is there a formal collegiate body for the management of the digital transformation strategy where the heads of technology of the main bodies of all public entities are represented?
    - If so, does this collegiate body also have systems in place to ensure that messages and petitions are indeed heard in the collegiate body, and that conclusions and agreements reach all institutions, including municipalities?
    - If so, are the resolutions of this body binding?
- If the aforementioned groups exist, is information published in relation to them, including minutes and topics discussed at meetings?



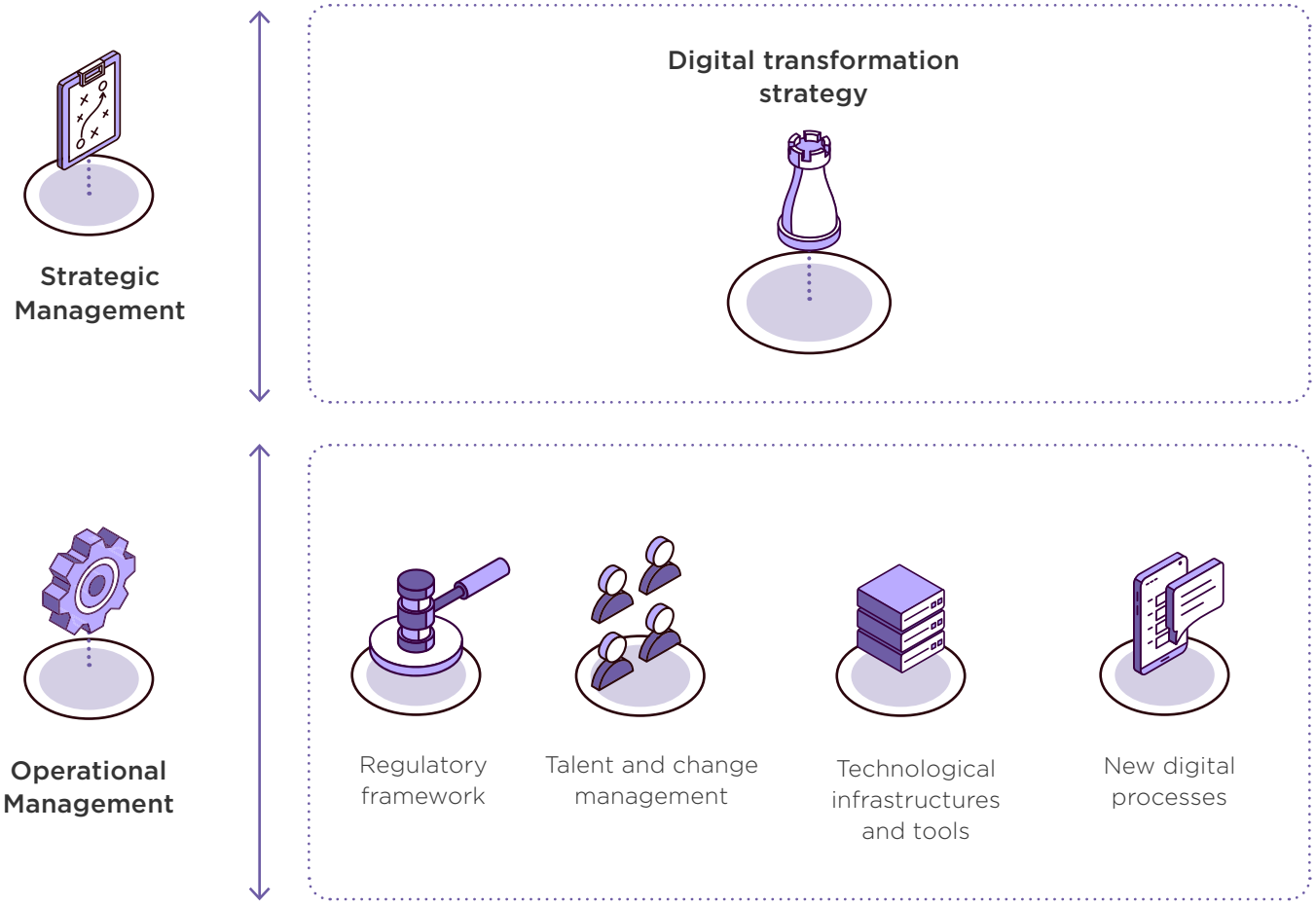


1.4

Operational management



Operational management encompasses the set of actions required to implement the digital transformation strategy. Ideally, the important issues are managed to be able to deal with all the day-to-day situations that will materialize the actions contemplated in the strategy. Thus, demand, architecture, portfolio and operational management are essential disciplines that must be addressed and managed appropriately.



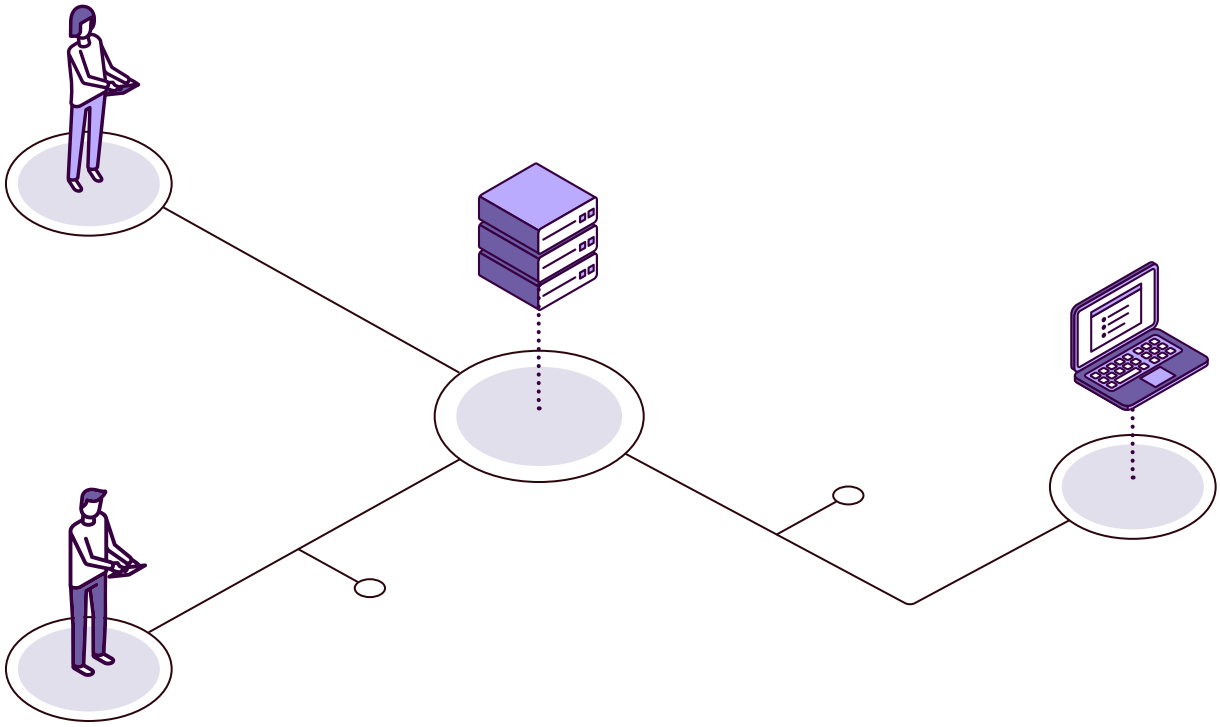
Operational management is used to manage the actions of the four main areas of action:

- **Regulatory framework:** Addresses the regulatory developments necessary to support the new digital services.

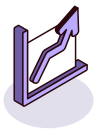
- **Talent and change management:** Human resources management as a key factor to face both current and future challenges. Special mention should be made of the need for "organizational culture management" because of the important impact it can have on both the execution of work and its results. It is convenient to keep in mind Peter Drucker's phrase: "Culture eats strategy for breakfast."

- **Technological infrastructure and tools:** The proper management of technology generates significant leverage to attain results through digital transformation. However, keep in mind: technology is never an end in itself, but a means to an end.

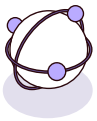
- **New digital processes:** Processes must be aligned with new standards, capabilities, and technologies. If these are not updated, the value delivered by digital transformation will be greatly reduced.



Each of these four domains is complex. Each of them can be made up of hundreds of projects, dozens of interconnected actions, high-impact risks, a multitude of multidisciplinary teams, etc. This can lead to a situation in which strategic objectives and priorities are lost, and monitoring become difficult. As such, it is necessary to execute an operational management that allows for proper governance. To this end, the **following disciplines** are recommended:



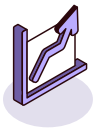
Demand management



Architecture management

Portfolio management

Operational management



DEMAND MANAGEMENT

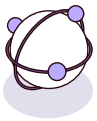
A holistic digital transformation requires a large number of operations involving:

- A significant number of interlocutors: ministers, businessmen, citizens, civil servants, associations, international organizations, etc.
- A large number of requests to be managed: the need to improve a certain public service, renew the computers in municipal offices, create a service so that companies can do business online, etc.

Therefore, it is essential to have an adequate demand management system that allows the following:

- Being able to clearly identify the channels through which requests can be made to the lead institution.

- Having a single point of approval, prioritization, and verification to ensure that the actions taken are aligned with the defined strategy. This is of vital importance in the field of public administration since, because all the measures "sound good" from the social, economic, administrative efficiency, etc. point of view, it is easy to fall into the trap of starting a multitude of initiatives without having a clear priority for them, ignoring the objectives and priorities set out in the strategy.



ARCHITECTURE MANAGEMENT

Having to address in parallel actions that modify standards, the capabilities of the team, the technological infrastructure, and the processes with which the different tasks are being carried out, it is necessary to have an architecture in place to govern these actions. It is important not to confuse the (enterprise) architecture with the technological architectures that support it, since the latter only respond to a part of the global vision that an enterprise architecture manages. Generally speaking, an enterprise architecture manages four major domains.

- **Business:** In this domain are the rules, regulations, decrees, etc. which regulate what can and cannot be done according to the law or the organization's rules.

- **Applications:** These are the systems that provide support to the different actors: citizens, civil servants, companies, etc.

- **Data:** The data available, as well as its governance, from the basics of additions, deletions, modifications, and eliminations to the more controlling actions such as defining who can access data and under what conditions or the traceability of these over time.

- **Technology:** Technological foundations on which the technological infrastructure available to undertake the digital transformation is built.

If the benefits that proper architecture management can offer to a public administration immersed in a digital transformation process could be summarized in just one, it would be to be able to identify what is available, what is the starting situation in each of the four domains, and what are the relationships that exist between them.

Although this benefit may seem trivial, in the size and complexity of a government, it is a key factor in assessing a priori the impact of a change or evolution of a law, service, or information system. For example, modifying a law requires taking into account not only the law itself, but also

whether the officials are trained to carry out the regulatory modification, whether the IT systems are capable of dealing with these changes, whether the necessary data can be obtained or are available from citizens to be able to carry it out, etc.

Changes can be made "by hand," without enterprise architecture management, but this form of action implies that there is dependence on the experience and expertise of the managers. The risk of forgetting some key aspect is high. When operating in this situation, delays and the need to improvise solutions for unforeseen situations are common.

PORTFOLIO MANAGEMENT

One of the results of implementing a digital transformation strategy is the generation of a tsunami of projects aimed at achieving the objectives set out in the strategy. These projects are kicked off and have to work in a coordinated manner to complete their objectives and thus the strategic objective. This approach is ideal and is usually maintained only during the early days of the project's life, as it is easy to lose sight of the strategic objectives in order to focus on the operational ones. Once projects start execution, they begin to face unplanned situations or problems that need to be managed with project resources.

- By way of example, the manager of project X is focused on meeting his objectives however he can: to deliver a product on time and within budget. To do so, he will probably have to make decisions that will affect both his project and three others that are running in parallel. Without proper management, project X may be successfully completed, but perhaps at the cost of the other three projects having to rework their deliverables and face delays and steep budget increases. To address this situation, it is important to manage the portfolio in order to identify which projects are being carried out, the relationships between them, the objectives they pursue, and the priorities. This will allow preventive action to be taken before problems occur.

OPERATIONAL MANAGEMENT

As important as it is to create new services, it is equally important to provide the existing ones with quality. This requires adequate operational management. The purpose of this discipline is to manage service delivery through value chains. In other words, identifying what needs to be done to generate a new service, how it is incorporated into the catalog of business services, how it is

operated, and how it is improved. In the field of digital transformation, it is understood that public administration provides value when it generates benefits for citizens, public institutions, or companies. These benefits can be, for example, reducing the time of justice processes, the online processing of tax collection, or making public administration data available to companies that can be used to generate new value-added services.

The combination of these four disciplines allows the institution to:

- increase the level of governance of operational management;
- have the necessary tools to control the status of the projects and services offered;
- make changes to projects and services;
- have a framework for measuring the different indicators, both operational and strategic.

Finally, it should be borne in mind that there are two levels at which the management of these disciplines will be replicated, and also coordinated: the lead institution in charge of the country's digital transformation and the vertical sectors that are part of a digital government.

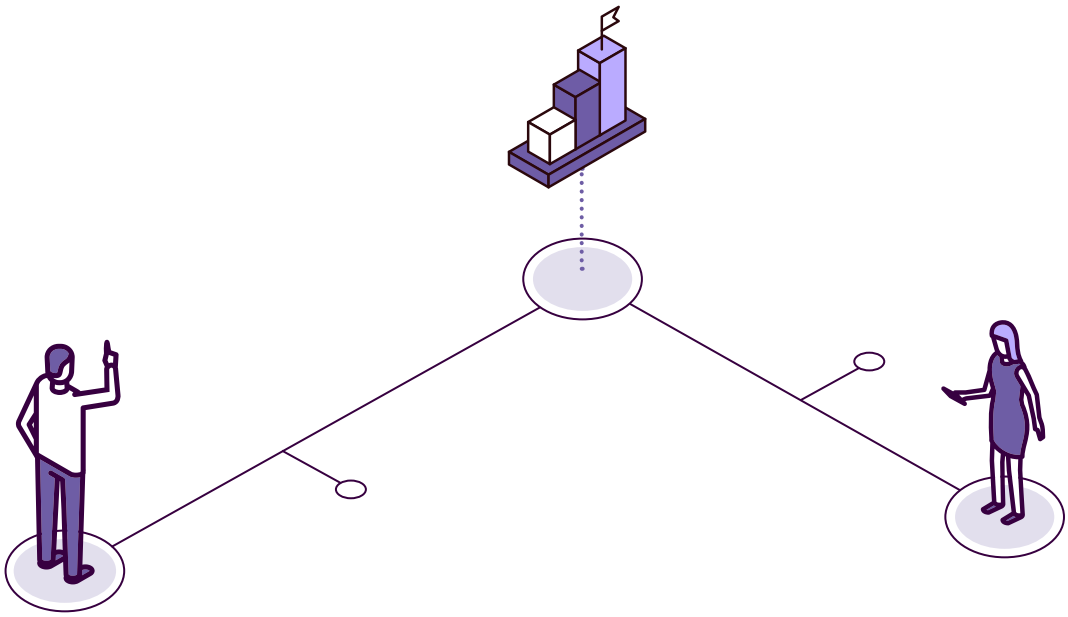
Imagine, for example, that a new digital service of applying for a scholarship requires an electronically signed receipt in "printable" format to be issued by the registry. If you also take into account that the registry being used by the Ministry of Education is a common service provided by the institution leading the digital transformation, you see a clear example of demand linkage between the two levels. That is, the IT department of the Ministry of Education will in the first instance receive the demand to issue such proof in the service described. In turn, that demand—or part of it—will be transferred to that lead institution to be handled as an evolution of the common registry. The demand, architecture, and portfolio management of both levels will be altered by this request, as well as the operational management, once the new versions of the systems incorporating the modifications reach the production environments.

1.4.1 DEMAND MANAGEMENT

Both large organizations and public administrations have to make decisions on an ongoing basis during the implementation of their digital transformation programs. These decisions have to be properly managed as resources such as time, human resources, or technological assets are limited..

During digital transformation processes, new needs are identified as the process progresses. An example of this type of request is the following:

- The minister, in a meeting with business associations, identifies the creation of an internet platform for business services.
- Pilot tests in a citizen service office have identified that the desktop computers are not fast enough, and it is proposed to change them.
- Citizens complain about the slowness of a service offered through the internet, and it is proposed to change the DPC infrastructure to provide better performance in web interactions.



The demand management function allows an organization to channel all incoming requests through a controlled and standardized channel. By using a unified flow for requests, it is possible to have control over the life cycle of these requests and to establish actions on each one, making it possible to determine whether or not it is appropriate to carry them out. This decision, as a general rule, is usually taken by a collegiate body such as the demand management committee, although in certain cases decisions regarding specific matters by area, subject, or content may be taken by a specific manager. For example, some of the decisions affecting security will be taken only by the security manager.

THE BENEFITS OF PROPER DEMAND MANAGEMENT

- **Greater control:** Requests are made through an established protocol. In a government or public administration with multiple actors/stakeholders (ministers, judges, doctors, etc.) who can request new services, changes, or improvements, it is key to have visibility of "who is requesting what."

- **Alignment with the strategy:** By having a controlled point of approval, it is possible to ensure that all actions carried out in the governing entity are aligned with the strategy and are aimed at the effective achievement of the objectives set. It also serves as a point of assurance that all initiatives or changes are aligned with the business architecture defined by the governing entity.

    - *Example*: If it has been decided that all the software to be used must be open source, and a request is registered asking for the acquisition of a commercial database, this request must be automatically rejected as it contradicts the principles established by the governing body.

- **Improved economic efficiency:** Through demand management, evaluation processes are established for new initiatives, implementation alternatives, etc., which make it possible to assess the different options from multiple dimensions and select those that promise the best results.

    - *Example:* When choosing an information system, perhaps one of the main aspects to take into account is the price. However, if a more detailed analysis is carried out, aspects such as maintenance costs, the difficulty of finding professionals for this system, whether it is based on a technology with a future, etc. can be identified. After evaluating all these actions, it may be the case that the best option is not always the cheapest one, but the one that has characteristics that are best aligned with the needs of the organization.

If demand management is not performed, there is a risk that initiatives or demands are being executed that are not controlled by management and are not aligned with the organization's strategy. Having control over these "pirate" initiatives is key, as they detract resources from projects that are aimed at meeting strategic objectives.

AREAS OF DEMAND MANAGEMENT

FOR EFFECTIVE DEMAND MANAGEMENT, THE SCOPE HAS TO BE IDENTIFIED, AS DEPENDING ON THIS THE FLOWS TO BE FOLLOWED WILL BE DIFFERENT AND MAY/SHOULD EVEN BE AUTOMATED.

3. **Strategic demand management:** This is used to manage the initiatives that are incorporated into the organization's portfolio. These are usually decisions that must be made in accordance with the management of the organization's strategy.

4. **Tactical demand management:** This is carried out through the catalog of services offered by a public institution. The objective for this type of demand is to automate it to resolve it in the most agile (the recipient of the service is satisfied) and economical way (the public institution provides the service using the minimum necessary resources).

    - *Example:* A citizen requests a birth certificate. This request can be received through a self-service website, telephone, etc. and is handled according to the flow that has been previously established.

5. **Operational demand management:** This demand is internal to the technology departments to keep systems up to date, servers active, and security updates performed.

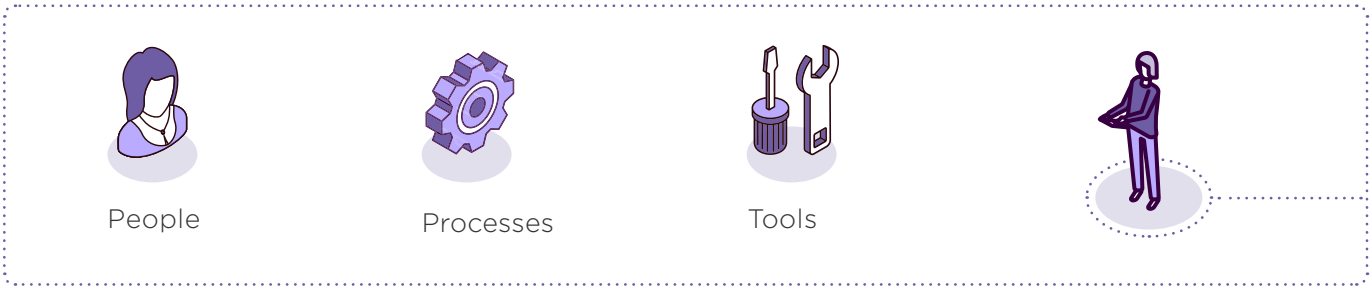
    - *Example:* It is required to keep the operating systems of the servers that are providing service to incorporate functional improvements updated. Also, the installation of security patches containing measures to block identified threats, such as Wannacry.

Demand management is necessary in all areas. However, in the event that there are not enough resources to undertake it in all of them, strategic demand management should undoubtedly be

chosen, given its importance in achieving strategic objectives. The rest of the text will refer to this type of demand management.

Strategic demand management

Implementing strategic demand management requires actions in the areas of people, tools, and processes. At a high level, the main activities to be taken into account are the following:



People

Identification of key actors or stakeholders: Once a demand has been presented, it is necessary for a demand management committee to evaluate it. This is usually composed of a multidisciplinary team that allows the demand to be analyzed from different points of view. It must also be mindful of the organization's strategic objectives, so that any decision it takes is aligned with them. The members of this committee must have profiles with authority to commit resources and budget, as well as to assume the responsibilities of the decisions.

Processes

Definition and implementation of demand management governance: The standardization of a process that manages the life cycle of a demand is a key success factor. Process orientation in a public institution offers important benefits, the most important of which is the ability to evaluate its operation and behavior in order to identify areas for improvement and optimization. The process has to contemplate the following basic stages of the life cycle of a demand:

- Demand or request registration: The different flows through which a demand can be generated must be identified, and it must be ensured that they all converge in the same source. It is essential that this allows an integrated view of all the demands made to the lead entity. In other words, the lead entity may receive requests through multiple channels from all the ministries that are affected by the digital transformation process, from political leaders, from professional and business associations, etc., but it is important to channel them through a single flow so that you have a clear view of all the requests you are receiving. Normally, it is not feasible for users to incorporate all the demands through a single portal or tool, but it is necessary to foresee the channels of incorporation and how to obtain the necessary details for processing. It is also necessary to identify who can generate demands, as well as who cannot. The strategic demand management process requires the use of valuable entity resources (especially people and time) to ensure that only authorized profiles can generate new demands.

- Processing of the demand: The demand and its "business case" must be presented. The objective at this stage is to consider how the demand meets the strategic objectives of the digital government transformation process and how it contributes to the value chain, in addition to assessing the costs, risks, and dependencies of the solution. Normally, this process has a strong relationship with the governing entity's business architecture, being evaluated in its four dimensions: business, data, applications, and technology.

- Acceptance or rejection of the claim: Once the business case has been made, it is presented to the claim management committee. This is who decides whether the claim becomes part of the portfolio or if it is rejected. In the latter case, it is highly recommended to objectively document the reason for the rejection of the claim since, if some of the conditions that led to the rejection were to change, the claim could be taken up again and all the work done could be reused.

  In the event that the demand is positively viewed by the committee, it will be incorporated into the public administration's portfolio following the established processes. It is important that there is feedback between the demands that have been approved and their life cycle. In this way, it will be possible to have traceability between the demand that originated, for example, the creation of an information system and to analyze whether the value proposed in the business case corresponds to the real benefit provided.

  Example: If a request has been approved to create a system to reduce the management time in a call center by 30 percent, and finally it is found that this improvement only reaches 10 percent, it will be necessary to analyze the causes of this deviation and apply the consequent improvement actions to improve the process of developing business cases.

Tools

Normally, the effective implementation of this process requires a tool that allows for the registration of requests and the control of their life cycle. Ideally, this tool should allow access by all participants in the process, with appropriate authorization and access management. A necessary feature is that all participants in the demand cycle have the possibility to work collaboratively on the same demand.

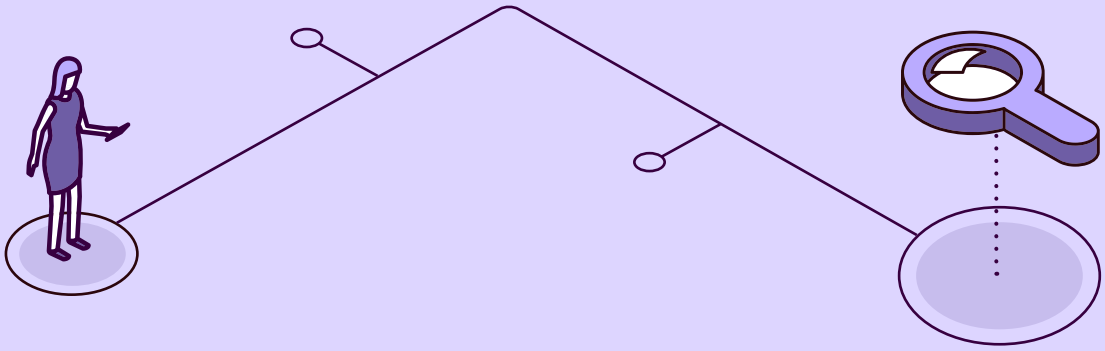
DEMAND MANAGEMENT METRICS

It is important during the demand management definition phase to identify the metrics necessary to analyze the value delivered by this function. The metrics can be strategic or operational. Some examples are the following:

- **Strategic:** The number of claims rejected for not being aligned with the strategy. Undoubtedly, this metric can show the effort and material, economic, and opportunity resources that would have been wasted if demand management had not been implemented.

- **Operational:** The time to market or time to value metric evaluates the capacity of the entity leading the digital transformation to convert an opportunity that arises through a demand into value generation for citizens, companies, and public institutions.

In conclusion, it is important that the demand management committees of the vertical sectors, as well as that of the lead institution of digital transformation, are perfectly coordinated to be able to make joint decisions efficiently. This coordination can be carried out mainly by submitting to the demand management committee of the lead institution those demands received by the different vertical sectors or organizations that require actions by common services or components or even by another sector. The same should occur vice versa (i.e., the demands that may reach the governing body and require action in a specific agency or vertical sector should be coordinated between the two committees).



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

She is immersed in the Ministry of Health's digital transformation projects. Many challenging projects are being proposed by the governing body and are starting to be implemented and to yield results. In the evaluation of the operation of the new healthcare system, the College of Physicians has requested that the electronic signatures of medical reports should not include names or personal data. This request was submitted to the governing body's demand management committee, which analyzed the impact that this change would have, the regulations that would have to be modified, and the changes that would have to be made to the systems with which it interoperates. On that basis, it chose to reject the request. Sara is pleased that the holistic analysis of this request has ruled out a change that would have had a negative impact on the other projects underway in both her ministry and other ministerial departments.

Entrepreneur
Ana

Ana is closely following the digital transformation that is taking place in her country. Among the different actions being implemented is a regulation that directly affects the chips it manufactures. The new standard admits encryption systems that in Ana's opinion are weak and that in a few months will no longer be useful. This will be a problem both for the different ministries that are undergoing digital transformation and for her, since competitors with lower security features will be able to bid for tenders. Through the association of technology companies in her country, she contacts the governing body of digital transformation and manages to generate a petition. The argumentation presented is solid, and the security problems that are generated and the costs that would be involved in betting on a less secure technology are exposed. After evaluating the business case, the demand management committee admits Ana's demand and processes it in order to update the regulations.

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a defined process known throughout the organization for managing new requests for digital transformation projects?
- When actions are to be taken, is the approval process defined?
- Is there a group of people designated to evaluate and approve, if appropriate, the requests that are made?
    - If this group exists, are there criteria used to determine whether the request is approved or not?
- Is there tracking of the delivered value of approved requests so that their return on investment can be assessed?

1.4.2 ARCHITECTURE MANAGEMENT

Government architecture is a way of designing, building, and implementing digital government solutions in such a way as to achieve an ecosystem of compatible, complementary, interoperable, and reusable technological tools, with great emphasis on the optimization of resources. The term architecture in the world of information technologies can have multiple meanings or objectives. In this particular case, it refers to enterprise architecture.

Approaching it in parts, enterprise architecture encompasses an architectural part—understood as a structure of components, their relationships, and the principles that govern them—and a business part. The latter refers to a set of departments of an organization that share the same objectives, mission, and vision. It is therefore very important not to confuse enterprise architecture with the physical or logical architecture of a network or a technological installation: although the latter may be part of enterprise architecture, it is much broader.

From the point of view of a public institution that wants to carry out a digital transformation process, the architecture must be taken into account to successfully implement the project. The lead institution must take into account the laws and regulations it has to comply with in order to perform its function. Moreover, from a government's point of view, it would have to consider the special regulations that affect sectoral departments such as healthcare, defense, or taxation. It should also be able to inventory the assets it has as an institution: What applications does it have? What citizen and business data does it have, and how can it use it? What technological infrastructure does it have? These are the assets available to an institution to be able to carry out an effective transformation.

The changes made in the architecture management framework must consider the available assets. For example, if an electronic signature system is required for all ministries, and it has been identified that the Ministry of Defense has one that they use internally, it should be determined whether this is a candidate to become the global solution for all ministries or if a new system is needed.

Broadly speaking, governance architecture can be seen as a road map to follow when implementing a new digital governance solution. This road map defines aspects such as

- technology standardization and normalization.
- shared work tools and methodologies.
- standardized solution design.
- provision of solutions for common use.

A "solution" will be defined as any tool or set of software tools, hardware, or combinations of both that, alone or integrated with others, solve one or multiple government needs. In this sense, solutions may be understood as electronic signature systems, identity management, information security, government cloud, interoperability, electronic medical records, digital records, and spatial data, among others.

THE BENEFITS OF ARCHITECTURE MANAGEMENT

From a business perspective, the proper management of the architecture allows the governing entity to

- achieve its strategic objectives.
- reduce the time from the moment a demand arises, is implemented, and begins to generate value for companies and citizens.
- reduce risks.
- increase security.

Architecture management, of course, also allows for easier management of the portfolio of solutions and reducing the risks of introducing new systems or modifying them. Architecture management

- establishes a common language for architectures in the state, promoting a better understanding of solutions.
- enhances the reusability not only of built assets, but also of best practices and methodologies.
- provides the ability to deliver new services and improve existing ones in a systematic way.
- improves the quality of services and solutions, establishing standard mechanisms for their measurement.
- allows the generation of standardized solutions and designs for cross-cutting use in the state.
- establishes a systematic way to design and build the solutions.
- generates a governance model for the state's technological assets.
- standardizes technological aspects, both for new and existing solutions.
- enables compliance with regulatory requirements.

- for all of the above reasons, generates an optimization of the state's resources.

If a public institution is not managing its architecture properly, it runs the risk of not having a unified view of the different components it has and how they relate to each other. This implies that, when the ministry needs to incorporate a new information system, for example a chatbot to inform citizens, it will not have the information to determine whether the functionality of this is already available in another system, or if it enters into conflict with other systems or principles of the entity leading the digital transformation (if it is incompatible with the existing database, if it requires having data that are not identified in the ministry, or if it requires an adaptation to comply with data protection regulations). In a ministry that does not manage architecture correctly, all these problems could not be foreseen but would have to be discovered and solved one by one during implementation. This will lead to delays and increased costs, or even to having to scrap the information system because it is determined that it cannot be implemented.

DIMENSIONS OF ENTERPRISE ARCHITECTURE

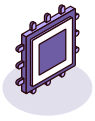
Enterprise architecture encompasses the entire public administration. Therefore, four dimensions must be taken into account:

With this approach, and returning to the previous example, the following problems should have been solved prior to the acquisition and start of the *chatbot* implementation project—and therefore

Business: Organizational structure, strategy, business processes, objectives, and standards.

Data: Data sources, data location, and data life cycle management.

Applications: All the organization's applications and how they interact with each other are identified.



Technology: All the technologies, both software and hardware, available to the organization. This dimension is closely related to the technological strategy.

at a lower cost—during the execution of each of the dimensions:

- **Business:** Is there any law that prevents providing information through a public channel about citizens? Does this *chatbot* system meet some of the stated objectives?
- **Data:** Is the data available to implement the *chatbot*, or do I have to build it *ad hoc*? If they are available, can I access them and are they sufficiently updated?
- **Applications:** Is there a *chatbot* solution available in my ministry? Does the *chatbot* have to be integrated with an application? Is this integration possible or are there any limitations?
- **Technology:** Can the *chatbot* operate with the databases I currently have in my ministry? Do I have to buy specialized servers for this new system to provide good performance, or can it operate normally with the current servers?

This small example provides a glimpse of the power that enterprise architecture allows to reduce the risk of implementing a new system, control budget/time deviations, and reduce the *time to value* of a system, from the moment it is conceived until it starts to generate value for a public institution.

ARCHITECTURAL FRAMEWORKS

The architectural framework must

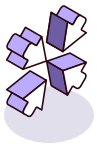
- generate a base infrastructure, including software and hardware;
- define the connectivity schemes of the solutions;
- devise common service designs, such as interoperability, user management, or digital signature;
- establish the technological standards required for the integration of solutions;
- determine a maintenance and governance model;
- define standard designs of the most common solutions, such as parts desk, notifications, customer relations;
- finally, build what is designed.

These definitions, principles, standards, designs, strategies, methodologies, built assets, and tools necessary for construction make up the road map mentioned above, and constitute the governance architecture.

For adequate architecture management, it is necessary to rely on an architecture framework. These frameworks offer tools, methodology, standards, and principles that facilitate the definition and management of corporate architecture. Currently, there are many architecture frameworks, many of which are used in the military world, such as the NATO *Architecture Framework* (NAF) of NATO[10] or the *US Department of Defense Architecture Framework* (DoDAF) of the US Department of Defense.[11] There are also governmental frameworks such as Colombia's *Colombian Enterprise Architecture Framework* (MRAE).[12] However, reference will be made here to the most common framework currently used in the market, which is *The Open Group Architecture Framework* (TOGAF),[13] which has a strong focus on understanding the business and the organization in order to generate the best-suited solution.

Although governance architecture may be based on a specific framework, this does not imply that tools and methodologies can be taken from other frameworks to generate their own personalized version. In fact, it is a good practice to review possible combinations that enrich the predesigned frameworks to better fit the reality of each government. Any government architecture framework should include at least the following points:

Architectural principles



Architecture domains

Architecture life cycle

Repository

Architecture governance

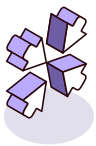
Support tools

10. https://www.nato.int/cps/en/natohq/topics_157575.htm
11. https://dodcio.defense.gov/library/dod-architecture-framework/
12. https://www.mintic.gov.co/arquitecturati/630/w3-channel.html
13. https://www.opengroup.org/togaf

Architectural principles

These refer to the motivation for the use of the framework and the regulations and restrictions that determine it. *Examples of principles:*

- Provide better quality service.
- Encourage the reuse of common solutions in the state.
- Comply with a law on administrative simplification, which may imply the adoption of a strategy, a motivation, and a set of restrictions.



Architecture domains

These are the points of view from which the solution to a problem must be approached. This separation can be as granular as desired, oriented to parts of the solution, to required profiles, or to technology. In any case, the most commonly used grouping refers to the key stages or pieces of a solution: business domain, data domain, software or application domain, technology domain.

Architecture life cycle

Refers to how the work process is organized, which—as in the case of development—can be done in a waterfall, iterative, or incremental manner, or a combination of these. The choice of the architecture life cycle must always be in line with the development life cycle of the solution, so that they are compatible.

IT IS ESSENTIAL TO CHOOSE A LIFE CYCLE THAT CAN BE COMPLIED WITH, THAT GOES THROUGH ALL THE NECESSARY STAGES, AND THAT ALLOWS FOR FEEDBACK, IN ORDER TO HAVE A CONTINUOUS IMPROVEMENT CYCLE.

Repository

All designs, strategies, documents, and blueprints, and any assets generated, should be stored so that they can be used in a timely manner. For this purpose, the generation of a repository that allows access to all relevant stakeholders should be considered.

Architecture governance

Defines important issues such as the following:

- Who owns the artifacts.
- When they are updated.
- How they are stored.
- Who is allowed to change them and under what circumstances.
- A cycle for the approval of changes.

Support tools

All of the above requires a set of tools to support it. Thus, the definition of tools should be considered for the following:

- Document

- Generate diagrams
- Manage the approval lifecycle
- Manage the organization's architecture assets

Although the generation of a government architecture implies the definition of a framework, the first thing that is required is to have a digital government strategy, accompanied by operational detail based on a diagnosis of the current situation, indicating the specific actions to be taken to meet the goals in the strategy and the capabilities and tools needed to do so.

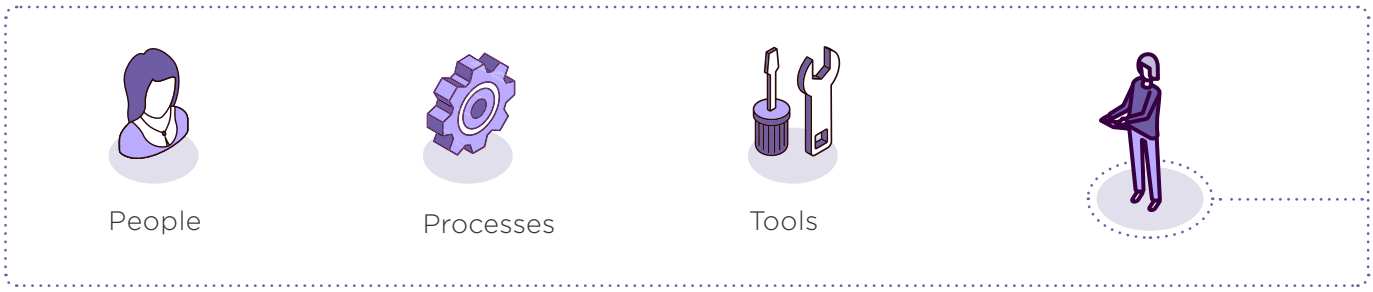
With these assets in mind, governance architectures can begin with the construction of solutions and not with the framework, always taking into account the possibilities of extension and growth. This opens the possibility of identifying problems and generating new versions of the architecture, to finally reach the governance architecture by successive iterations.

However, although the path of successive approximations is a good strategy for achieving short-term gains and minimizing the risk of making definitions that are not adequate later on, it entails the risk of starting a cycle in which a stable version of the framework is never reached. To limit this risk, it is important to be clear about the minimum or initial version of the framework and to plan the activities to make this happen.

It is often believed that governance architecture frameworks are "heavy" and involve bureaucratic cycles and a high cost of documentation, but this is not entirely true, since the framework can be as pragmatic as required, perhaps involving a sum of best practices and tools from different frameworks or adaptations of existing ones. The framework may even be flexible enough to be adapted to agile implementation methodologies. For example, the architecture design does not necessarily involve a document if the organization does not require one; it may be that the design is a snapshot of a whiteboard that reflects the working and implementation agreement that has been reached.

Another point to keep in mind is that the framework must be flexible enough to allow for the inclusion of existing solutions. For example, the governance model cannot exclude the possibility of modifications to legacy solutions. This does not mean that the framework must be created in the image of what is currently in place, but rather that it must be generated based on what is considered optimal, while seeking to achieve a balance with what already exists.

MAIN ASPECTS TO CONSIDER IN THE DEVELOPMENT OF THE ENTERPRISE ARCHITECTURE



People

It is essential to have qualified personnel in these disciplines. Therefore, before launching an initiative of this type, it is necessary to carry out an internal assessment within the organization to determine what skills are required and, if they need to be increased, to establish a plan to achieve this through internal training or hiring. For the definition of professional profiles, especially when hiring is necessary, it is useful to rely on frameworks of personal skills and abilities, such as the Skills Framework for the Information Age (SFIA).[14]

The implementation of enterprise architecture requires a change in the culture of the public institution. For this reason, it is necessary for it to be sponsored by senior officials (ministers, etc.), as well as for communications to be carried out so that all the organization's personnel know what it is, what it is for, what benefits they can obtain, etc.

Processes

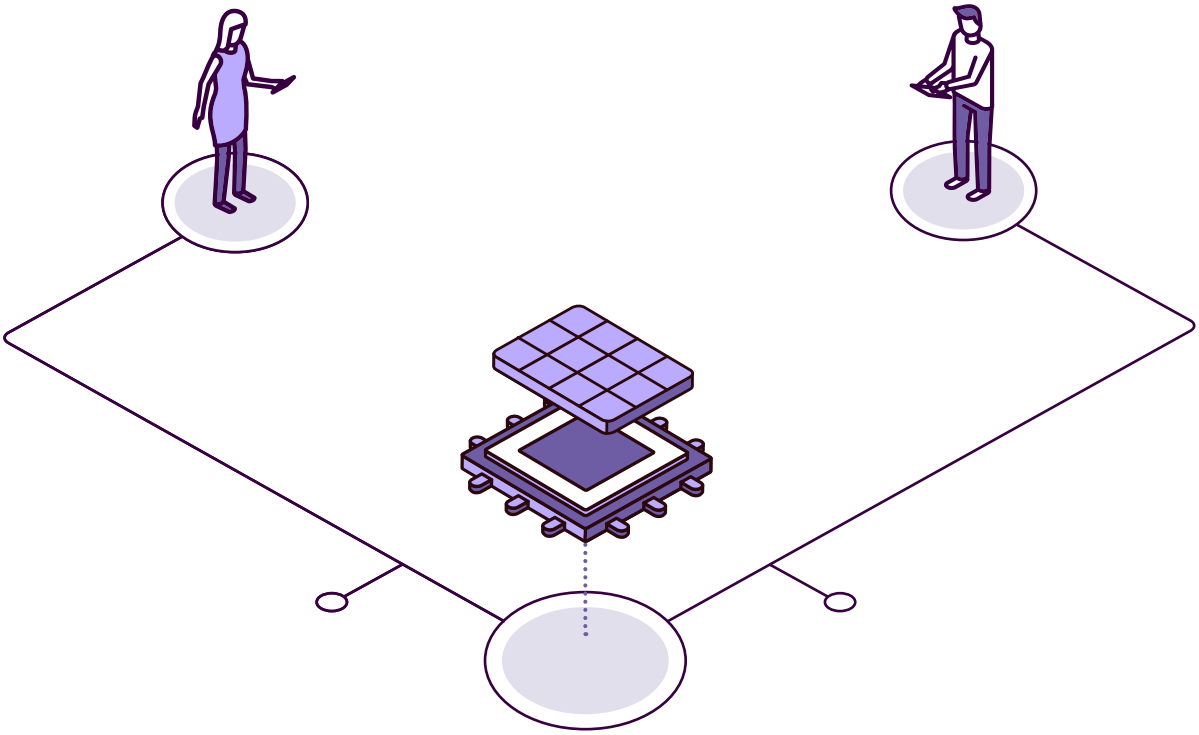
Process standardizations are key to developing, managing, and maintaining an enterprise architecture. To this end, it is necessary to define the different processes that allow each of the phases to be developed in a controlled and predictable manner.

14. https://sfia-online.org/es

Tools

No specific tool is necessary, since the architecture is based on the generation of artifacts that are nothing more than lists, matrices, or diagrams. However, to manage an architecture it is highly recommended to have a system that allows all the participants in the architecture to work collaboratively, as well as access to the "consumers" of the architecture so that they can benefit from it.

The process of developing an enterprise architecture should be iterative. While the different enterprise architecture frameworks offer great help in implementing an enterprise architecture, appropriate adjustments need to be made for each public institution. For this purpose, the iterative approach is the best suited because it allows ministries, agencies, etc. to benefit in early stages of delivering value to citizens and businesses, while making adjustments to components that do not perform as expected.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo needs to request a date and time for his grandmother and daughter to receive their annual flu vaccination. This procedure can be done online, so Camilo decides to do it on the first day it is available and get an early date. Because of his job, he can only request the appointment when he gets home from work. On the first attempt, the page loads very slowly, but he is still able to get through the initial access. Unfortunately, when you try to register, the site becomes slower and slower, until it stops responding. After that, the site goes offline for a few hours, until Camilo goes to sleep. He keeps trying for the next few days without any success, until he decides to do it early in the morning, before going to work. That day he is able to complete the registration but notices that his preferred times were no longer available. Clearly, it would have been best if the solution had attributes and had been designed with sufficient capacity for fast page loads.

Entrepreneur
Ana

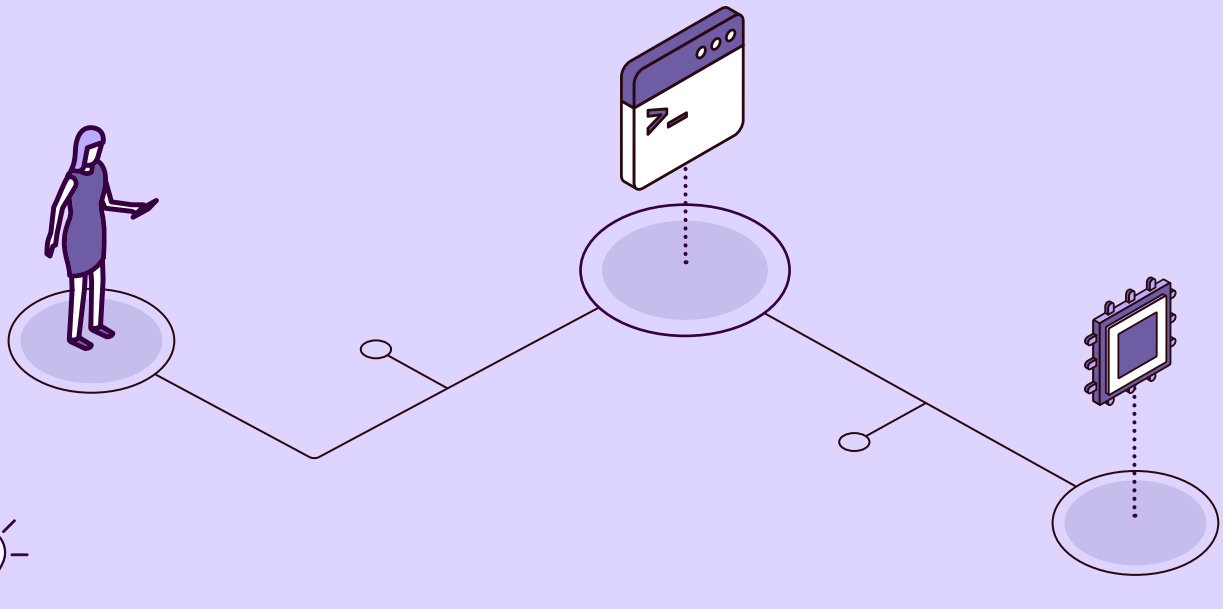
Ana has the opportunity to sell her microchips and have them included in the electric current telemetry equipment of the Ministry of Energy and Industry. In this case, her company must enter into a consortium with the company that manufactures the equipment, since they have a complex manufacturing process. A few days before she has to submit the bid, Ana finds that the ministry also launched a purchase for a software to monitor the meters. She knows this is a mistake, as her chips, like others, are not compatible with all monitoring systems, so there is a risk that the system will not be able to monitor her meters. This is likely to postpone the purchase, which is detrimental to Ana and her partners as well as to the government itself. Had the ministry had an architectural framework and a systematization of the design, it could have realized the problem earlier and taken the necessary steps to make the two purchases compatible.

Mayor's advisor
Daniel

Daniel is quite worried because the mayor has asked him to set up a website as soon as possible where citizens can register for a procurement process to be carried out by the city council. The deadline is short, and Daniel does not have time to launch a public procurement process. After analyzing the needs of the registration system, he has noticed that he can implement the system through basic components that are already being used in several departments of the city hall and that he can take advantage of for this new service. He has a web server from the communication department, an electronic signature system from the tax collection department, and databases from the security department. Thanks to these resources, Daniel is able to set up a solution that allows the electronic registrations demanded by the mayor through the reuse of components that were already available in the city council.

Vice minister of health
Sara

The human resources department has submitted a request to acquire a new payroll system. This system has a considerable cost, but provides many of the functionalities that the department has been requesting for a long time. Sara is part of the demand management committee that analyzes this request and, after analyzing it from the point of view of enterprise architecture, identifies that the Ministry of Defense has a system that meets 90 percent of the requirements. Given this situation, Sara, requests that the defense system be installed and upgraded with the missing functionality. The result of this implementation will not only benefit the Ministry of Health, but also the Ministry of Defense, as well as anyone else who wants to use it. Sara is very happy because, for a small part of the price they were going to spend on the new system, they have managed to provide their human resources department with the system they needed, as well as improving the payroll system, which will be available to all ministerial departments and companies in their country.



EXAMPLES

Click on each flag or icon to go deeper.

Uruguay
Integrated Government Architecture

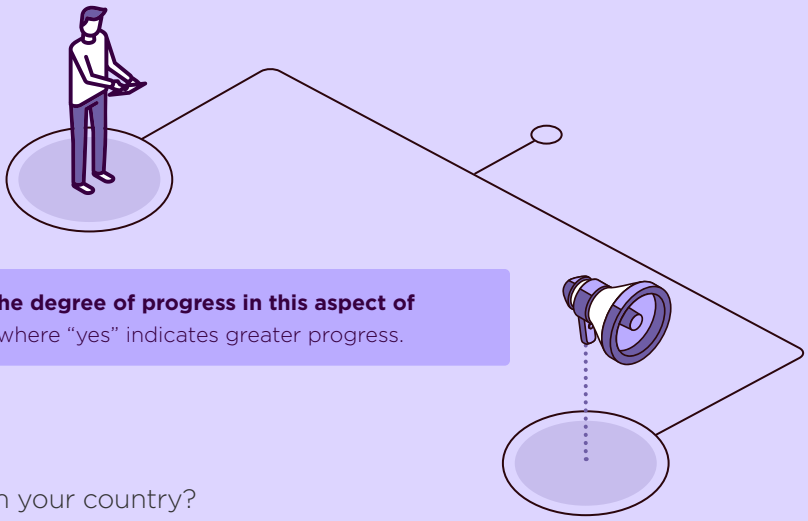
Colombia
Enterprise architecture reference frameworkl

Uruguay
Arquitecture of the national e-health record

United States
The DDAF Architecture Framework

Republic of Korea
eGovernment Standard Framework

Spain
Digital government services catalog



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

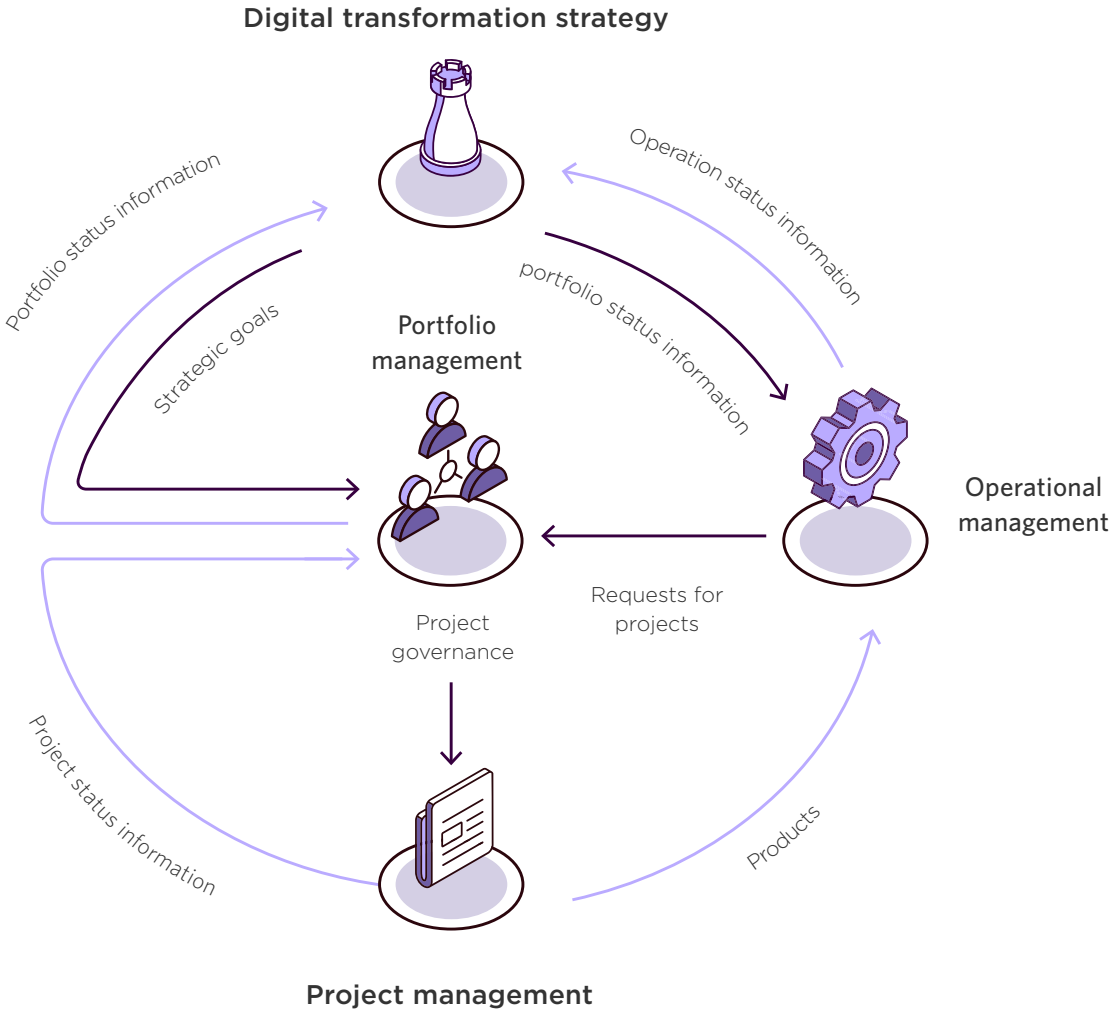
- Is there a governance architecture in your country?
- Does this governance architecture have a defined framework?
  - If so, is it based on any known public or private framework (e.g., TOGAF,[15] FEA[16])?
    - Are there any regulations that promote its use?
    - Is the framework being used in more than half of the central government institutions?
    - Is the framework being used in regional and/or local governments?
    - If so, is the framework being used in more than half of the regional and/or local governments?
- Are there reference architectures for standardized solutions at the government level?
- Is there a dissemination strategy for the integrated governance architecture?
- Are there personnel trained in architectural disciplines within the lead digital institution?
- Is there specific training for government institutions on the governance architecture of your country?

15. Gartner. https://www.gartner.com/en/documents/405453.
16. FEA: Federal Enterprise Architecture Framework of the Unites States of America. Available in https://obamawhitehouse.archives.gov/omb/e-gov/FEA.

1.4.3 PORTFOLIO MANAGEMENT

The digital transformation strategy depends on portfolio management and operational management the ability to make its objectives a reality. A portfolio is considered as the management of a set of programs[17] and projects aimed at achieving the strategic objectives of a public institution. It thus allows for an overall vision that transcends the particular vision of a project, leading to the identification of synergies, joint risk management, interdependencies, etc.

Normally, when a digital transformation initiative is implemented, the number of programs and projects is huge. It becomes evident then that there has to be a way to manage them in an aggregated way to be able to monitor them, know where they stand, and know how they can lead to achieving the strategic objectives.



17. Program: A set of projects that are managed in a coordinated manner to obtain benefits that could not be obtained if done individually.

As can be seen in the graph above, portfolio management is the mechanism available to the lead institution to generate projects and products that are offered through the operation to generate value for citizens, companies, and public institutions. Similarly, each agency or ministry should have its own portfolio management for its digital transformation strategy. Of course, both portfolio levels will need to be closely coordinated if projects are to be successful. For example, if a new digital registration service for an electronic office requires a digital signature to be provided as a common component by the digital transformation governing body, the planning associated with both must be coordinated, since the registration service cannot be put into production until the signature component is ready.

The portfolio that is defined must be coordinated with and must cover the needs of all the sectors that will participate in the digital transformation. Now, if there is a portfolio, it must be managed, and for this it is necessary to identify, prioritize, manage and track the projects and programs in order to meet the strategic objectives. At this point it is important to differentiate between two types of management:

- **Project and program management:** Focuses on how to achieve a set of deliverables at a given level of quality, within a given timeframe, and within a given budget.

- **Portfolio management:** Aimed at achieving the objectives of the lead entity.

BENEFITS OF PORTFOLIO MANAGEMENT

- It allows the governing body of the digital transformation to make centralized decisions affecting all its programs and projects. In general, this management transcends the project part and reaches the products, which are the instrument through which public administrations provide value. In this way, it is possible to define a life cycle for each of them and, thus, to plan with sufficient time the necessary actions for each case.

- Administrations can think long term, making decisions about their systems and what to do with them over the years.

    - *Example:* For a public institution dedicated to healthcare management, the health records management system is critical. It has been in operation for many years, its technology is obsolete, and, in addition, it is a very large system with very complex functionality. In this difficult situation, long-term planning is required to make decisions about what to do with this system: How will its life cycle be managed? Is it advisable to invest in upgrading it technologically? How will it be integrated with other products? These questions can be addressed via portfolio management, in a multiyear plan to adapt the state of an organization's systems to its strategic objectives.

Not having a managed portfolio means losing the synergies that can occur between the different projects. Worse still, the execution of projects may not be aligned with strategic objectives. Moreover, lacking this management means having to improvise with problems as they arise, as well as with financial planning, political programs, public procurement, etc.

THE PORTFOLIO MANAGEMENT PROCESS

The normal flow of portfolio management consists of the following steps:

- The members of the steering committee define a series of strategic objectives.
- Portfolio management must ensure that the projects undertaken in the public institution are aimed at meeting these objectives.
- If this is not the case, they will have to make a series of changes in order to adapt them.
- Once the portfolio is defined, different pieces are generated and delivered to the project managers.
- Project managers will be responsible for undertaking the identified projects.
- These projects generate products that will be incorporated into the operations of the different ministries and government agencies.

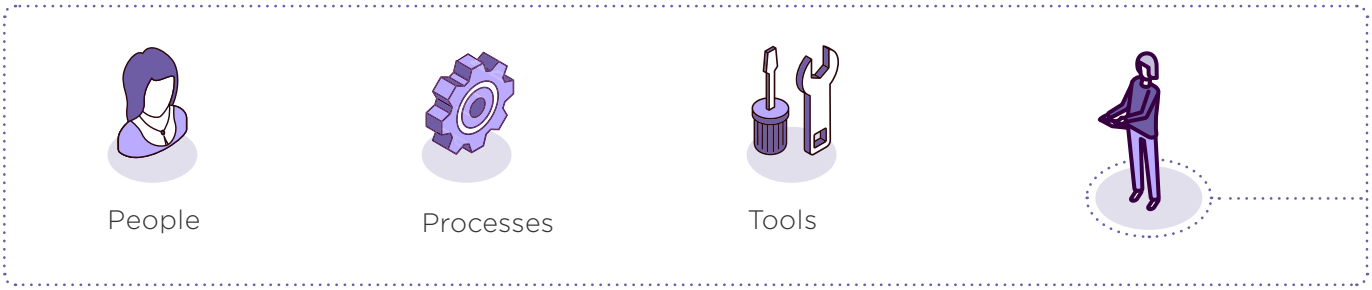
THE PORTFOLIO MANAGEMENT PROCESS IS A LIVING PROJECT, IN THE SAME WAY AS STRATEGIC MANAGEMENT.

If, for any reason, a strategic objective should lapse, the portfolio is not invalidated; it will only have to be updated, and the order to cancel the projects that were linked to that strategic objective will have to be taken.

In organizations where portfolio management is not being carried out, the mistake is often made of starting with a lot of enthusiasm and not defining a viable initial scope. This management has an important organizational cost since it requires the involvement of senior officials and the definition of processes. All this, a priori, may seem to hinder rather than help; therefore, it must be applied diligently.

A tip at this point is to use the Pareto technique and apply portfolio management, at first, to the systems that are really important for public institutions: to 20 percent of the systems that generate 80 percent of the value for citizens and companies. This can be a good starting point for the organization to increase its management capacity and become familiar with the new processes.

To implement portfolio management, it is necessary to undertake actions that include, the following:



People

- Identify the different roles and responsibilities involved. It must be established a priori who the people working in portfolio management will be, along with their responsibilities in the process. Likewise, it is not only necessary to identify who will work in this discipline, but also who is the sponsor of this function: it should be a senior official (minister, secretary of state, etc.) responsible for driving the process, as well as helping the management team to have a clear vision of what the strategy of the lead agency is.

- In large organizations, it is common for there to be departments whose functions are not known or are not clearly identified in the organization's value delivery chain. In other words, no one knows what they do or what they contribute. For proper portfolio management, it is important to know if this is the case. It is a discipline that can bring a lot of value to the governing body, but if it is not properly executed, it is easy for it to become part of the corporate bureaucracy. For this reason, it is necessary to hold dissemination and awareness sessions on the different elements that make up the value chain.

Processes

Portfolio management processes must cover two main areas:

- **Ensure alignment with the strategy.** There must be activities to identify projects, evaluate them, categorize them and take control over the life cycle of the products they generate. The purpose of these activities is to prevent the performance of tasks that are not aligned with the governing entity's strategy. It is important to understand the impact of a new project on the portfolio, especially when there is an update of the strategy.

- **Monitor the performance of projects to report on the progress of the strategy.** When a project is approved, reporting metrics must be defined. This will allow the project/program management team to update the status of the project/program and, consequently, the strategic indicators.

Tools

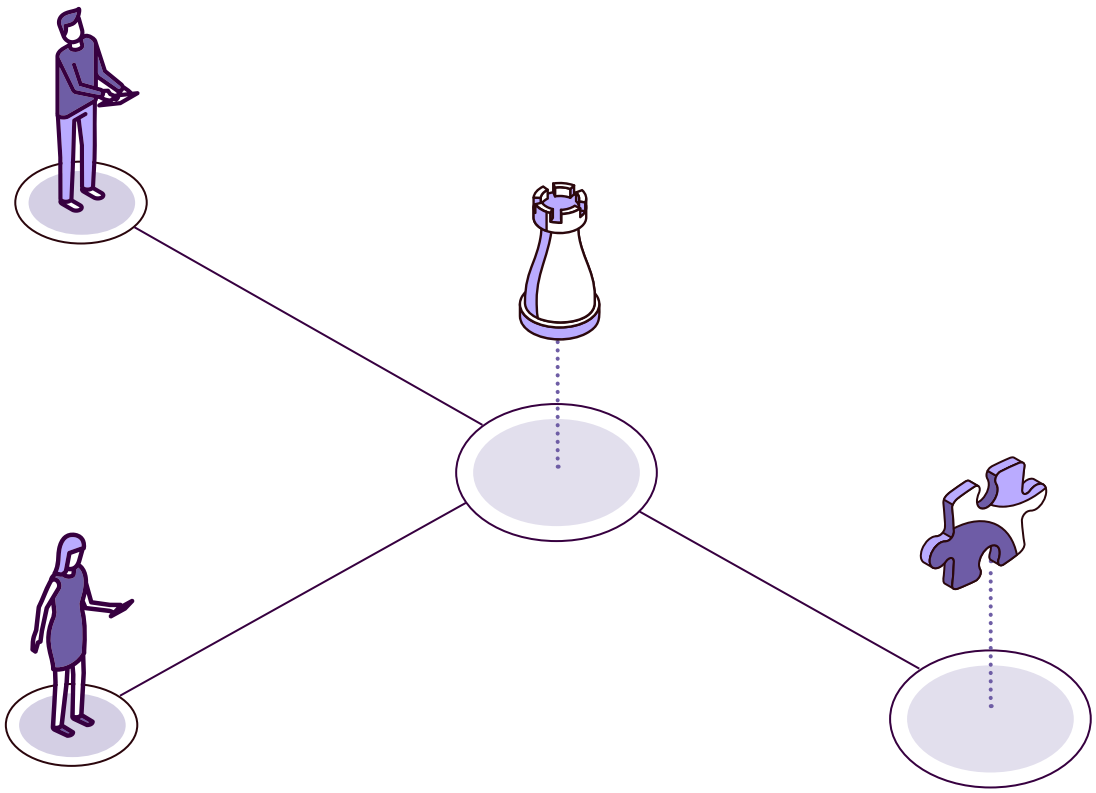
It is important to have tools that can support the process areas identified above. There are a wide variety of options on the market that offer diverse functionalities to identify portfolio elements, monitor their status and indicators, allow collaborative work, etc. However, attention should be drawn to the ease with which a portfolio management implementation initiative can be transformed into a portfolio management tool implementation project. In this case the project will get off the ground, will soon be seen as "something" that does not contribute much and generates bureaucracy, and will

end up being discarded. Therefore, it is important to keep in mind that the tool is nothing more than a means to an end.

The metrics of portfolio management are aimed at meeting strategic objectives. They answer the question, Are the right steps being taken? Some examples of metrics that can be used at the portfolio level are:

- **Strategic:** User satisfaction index. If user satisfaction is a strategic objective, it is essential to measure how the organization's projects (and products) contribute to it and to feed the strategy with this information.

- **Operational:** Estimated versus actual costs or schedules. Knowing the accuracy of schedules is an indicator that can help to establish improvement actions (in case it is not good) or to make reliable predictions (in case it is good).



STORIES

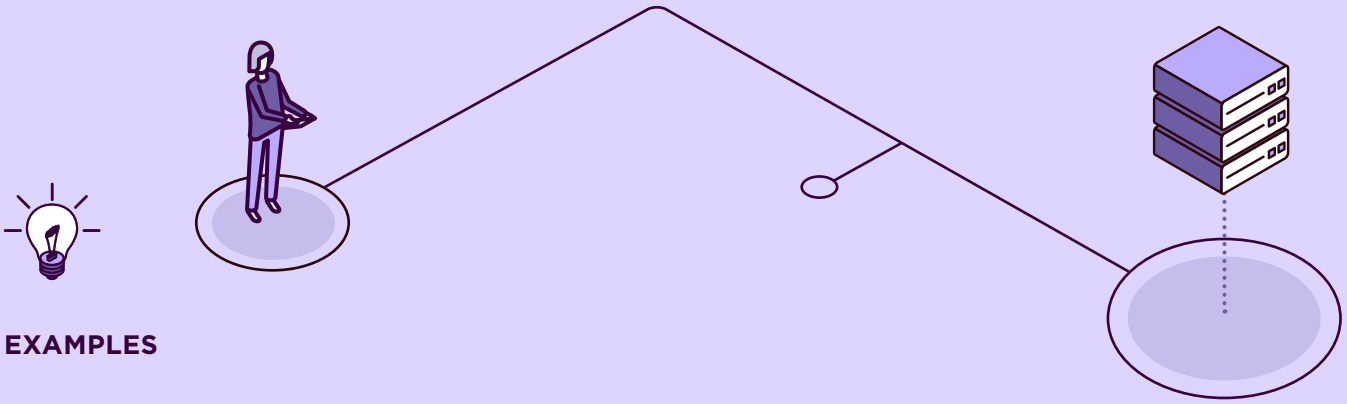
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

The medical records management system is old, complex, expensive to maintain and does not meet the needs demanded of it. The worrying thing is that in three years' time, the manufacturer will stop supporting the technology on which it is based. Sara wonders what to do: Should she continue to invest money in this system to migrate the technology on which it is based? Should she look for another product in the market? Start another product from scratch? On the other hand, one of the priorities of the government of which it is part is the use of open source software and to encourage the reuse of products between different ministries. Accordingly, she decided to launch a project aimed at generating a new system for the Ministry of Health, based on open source, to replace the current system. In parallel, projects aimed at data cleaning and migration, generation of new technological infrastructure, etc., are launched. The life cycle of the medical records management system establishes that in two years the system will cease to provide service, so that investment in new functionality is reduced to a minimum.

Entrepreneur
Ana

The leading entity of the digital transformation of her country has published the portfolio of new products and services available. Among them is the service of electronic notifications between companies and public institutions. Although in the first period the use of electronic notifications is optional, after a few years it will be mandatory. In view of this expectation, Ana decided to implement the changes in her company's systems in order to integrate with the electronic notification systems that the government will make available to be one of the first companies to benefit and thus gain a competitive advantage over her competitors by being more efficient and agile in her communications with the government.



EXAMPLES

Click on each flag or icon to go deeper.

European Union
Emerging Technology Portfolios

United Kingdom
Information on large public projects

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there any list of digital transformation projects/programs available?
- Is the digital transformation project/program management methodology defined?
- Is there a person responsible for managing the portfolio of digital transformation projects?
- Are there dashboards for project monitoring?
- Is there a written linkage of how these projects contribute to the government's strategic objectives?
- Is a record kept of the relationships between projects?

1.4.4 OPERATIONAL MANAGEMENT

Today, most organizations are torn between the dilemma of providing technological services that are stable, do not have problems affecting their availability, have predictable behavior and having agility in the implementation of new products and functionalities. Depending on the type of organization, the point of equilibrium between these two extremes will be more in one direction or the other. For example, a country's Ministry of Health offers a series of services to its citizens, and what is important is not that these services adapt quickly to any changes that may occur, but that they are known, stable, and predictable. These services are usually based on administrative procedures which ibased on laws that regulate them. This rigidity means that the provision of services in this case is not as agile as that of a cell phone company, which can, for example, change the services offered to its customers in a short period of time.

Institutions focus on providing services to businesses and citizens as well as to other institutions, generating value. Some examples of value that public bodies can provide include:

- the possibility of electronically submitting a notification without having to spend time traveling;
- the possibility of carrying out procedures before a ministry or city council through an electronic office;
- the use of a payment gateway to make payments without having to visit a bank in person.

Operational management is the set of organizational capabilities required to deliver value to customers in the form of services. This is what it has to do provide a service of value to citizens, companies, or other public institutions.

Focusing on delivering value is the prime benefit of operational management. In complex organizations it is easy to lose focus of the ultimate goal, confusing it with operational objectives. Therefore, an organization in which the operation is properly managed will be able to effectively convert an opportunity or demand into value for its users.

An organization employs a multitude of economic, human, temporal, reputational, etc., resources to generate value for its users. For example, citizens can often pay their traffic fines on the internet. If this need is not being properly managed, it is very likely that the service finally provided to users will not be delivered on time, the cost of service delivery will exceed the budget, and/or the quality will not meet expectations. Therefore, it is highly recommended that, in this case, administrations manage the operation in an appropriate manner to minimize the risks inherent in the provision of existing services and the generation of new ones.

There are currently two main trends in operational management:

- **Information Technology Infrastructure Library (ITIL)**[18] is a framework of best practices for operations management. ITIL has been for many years the de facto standard for operations management in organizations.

- **DevOPS** is an operational management model based on collaboration, as a way of overcoming the usual communication problems due to the "wall of confusion"[19] that separates the teams developing new services and the teams in charge of providing the service through the operation of the organization's technological infrastructure. This model has a strong cultural component based on agility, accountability, self-sufficiency, and collaboration, although it is not common in public institutions where structures are more hierarchical and rigid.

Value delivery is the key of both models. To this end, the role of the value chain must be understood as an operating model for the creation, delivery, and continuous improvement of the organization's services. From the point of view of a public institution, this chain must be understood as the steps that must be taken to articulate the provision of a service with the generation of a benefit to citizens.

When implementing operations management, it is important to identify the organization's assets so as not to start from scratch. Understanding the starting situation by establishing what are the processes, systems, services, capabilities, etc., gives the possibility to reuse what already exists, saving effort and moving faster in implementation.

18. https://www.axelos.com/best-practice-solutions/itil
19. Symbolizes the communication problems between the different silos of an organization.

Implementing operations management requires the participation of many teams, adapting systems, adapting or creating new processes, and so on. Dealing with all this at once can result in an excessively long time between the start of the work and the moment when it begins to bring real value to the organization. In addition, public institutions do not remain frozen while the implementation is being carried out, but evolve to adapt and respond to the challenges they face. For this reason, it is recommended to approach implementation in short phases, so that the organization can benefit from the results of each phase and be able to evaluate what works.

It is important to have a global approach to operations. In organizations, services are often complex and interrelated. This global vision, coupled with simplicity, helps to make the operation efficient and effective. Simplicity is understood not as something simple or easy to do, but as something that eliminates what does not add value, hinders, or blocks something of use to the organization. An example of this is the elimination of reports that are often generated as part of a process. These are documents that are generated but no one reads or uses, nor do they serve regulatory purposes, and they are stored indefinitely. By not identifying that generating this report is unnecessary the organization devotes resources (human, technological, and time) to do something that has no value and distracts from pursuing its real objectives.

The global approach becomes important when considering that the operation of services will be a shared responsibility between agencies, ministries, and the governing body that provides common services. For example, a service of the Ministry of Housing that offers the possibility of requesting a subsidy through the internet will be supported by a digital identity and signature system, provided by the common digital government platform. If the signature platform suffers an operational incident, this will affect all those end services that have it integrated, such as, in the case of our example, the subsidy request service.

In addition, it is crucial that service-level agreements are aligned between the components that are integrated to form a final service and that are the responsibility of different agencies. Thus, if a court filing service is 24-7 (twenty-four hours a day, seven days a week) and relies on a common service provided by the electronic signature governing body, the electronic signature must be a 24-7 service. If this alignment does not occur, there is a serious risk of encountering barriers to incident management that do not allow services to be returned to normal in an optimal manner.

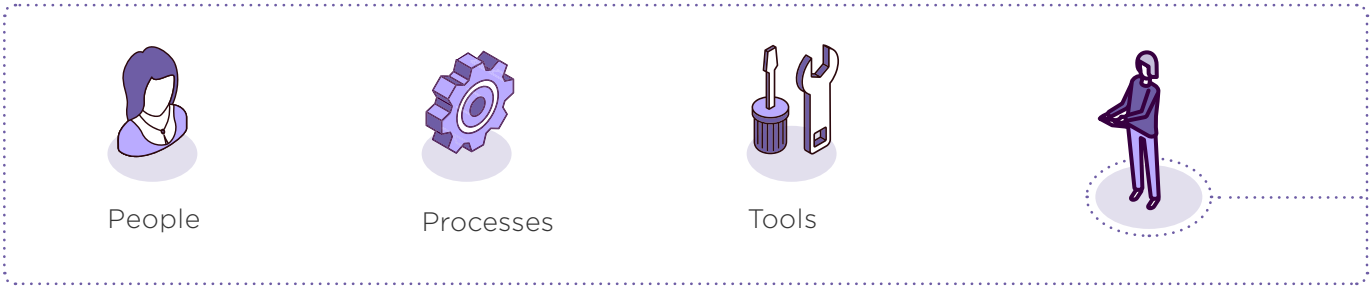
FOCUSING ON VALUE, REUSING, DOING THINGS IN PHASES, HAVING A GLOBAL VISION, AND SIMPLIFYING AS MUCH AS POSSIBLE CAN FACILITATE THE PROCESS OF IMPLEMENTING AN OPERATIONAL MANAGEMENT FRAMEWORK.

AUTOMATION

The most significant impact on the efficiency in the management of an organization's operation comes from automation. This consists of using technology to replace the participation of human workers, so that the execution of tasks is much faster, with a predictable result and quality, and much cheaper.

People's actions are based on their experience, their creativity, their knowledge, and so on. If this performance can be modeled, then the related tasks are a candidate for automation. However, although the advantages of automation seem obvious, it is always recommended to first simplify and optimize. In this way it is possible to eliminate steps that do not contribute, so that the result delivers maximum value at minimum cost.

DIMENSIONS OF OPERATIONAL MANAGEMENT



People

The organizational structure is a key aspect to manage. To this end, it is important to identify the different roles and responsibilities of the profiles, departments, and/or people. This must be complemented with a system to establish the skills and competencies required by people to operate in each position. It is also necessary to determine what is the level of competence required for a specific organizational position and what is the current level. Once these requirements have

been identified, the plan for capability acquisition must be established. There are frameworks such as the *Skills Framework for the Information Age* (SFIA)[20] that already establish a model, profiles, and levels.

The management of the operation has an important component of organizational culture. As such, it is important that the organization prioritizes motivational leadership, appropriate management styles, and powerful communication that allows information to flow throughout thedifferent institutions.

Processes

Operational management focuses on delivering value through value chains—in other words, on creating products and services that deliver value to customers. The process to be followed to achieve the objective has to be defined, contemplating at least the following steps:

- **Objective definition:** What are the expectations of the users? What is the expected cost of the process? What kind of quality is expected from this process? Before moving forward with the construction of the process, it is important to be clear about these objectives so that the result is in line with expectations.

- **Generation:** When does the service have to be available? Will it comply with all legal requirements? The service generation process must take into account the requirements to which it has to respond, as well as the different time constraints.

- **Delivery:** Is the service delivered as specified? Is the quality delivered as required? Does it deliver the expected value to the users? Once the service has been built, it is validated that it is delivering the expected value and monitored to ensure that it is delivered at the appropriate quality levels. Also, since services have to respond to the organization and its objectives/needs, they can vary over time. Therefore, the necessary change requests have to be managed to adapt the service to the new needs that may arise.

20. https://sfia-online.org/es

It is important that the processes related to the operation are evaluated and follow a cycle of continuous improvement. In this way it is possible to review both the execution and the results they have produced in order to seek improvements in quality, efficiency, effectiveness, etc. For evaluation, it is important to define metrics that allow objective measurement of the impact of continuous improvement.

Tools

When dealing with operational management, the role of tools and technology must be taken into account. Operational management is usually automatically associated with ITSM[21] solutions or service management tools, which allow, among others, the management of requests, problems, knowledge management, etc.

It is also clear that the technological approach of the organization conditions the type of management of the organization. For example, if the organization opts for infrastructure management based on cloud-based solutions, the management of the operation will be different from the option of managing on-premise infrastructure.

MONITORING

The management of the operation must be monitored since it is the "engine" of public institutions, through which the delivery of value to users through services is materialized. For this reason, monitoring is required, with a view to ensuring that the result is in line with expectations, as well as to identify problems that generate incidents in the normal operation of the system. Some examples of metrics to be used in this regard are the following:

- **Strategic:** Reduction of operating costs. Through continuous improvement processes, cost efficiency gains can be identified, which can be materialized in cost savings in human resources, technology, waiting times, storage space, quality of the final product, etc. A direct relationship can be established between continuous improvement and improved operational efficiency.

- **Operational:** Number of incidents that are resolved on the first call by the service desk team. This metric provides information on the ability to resolve user incidents in an agile manner and the quality of support being offered in the event that the service is not provided normally.

21. IT Service Management Tool.

STORIES

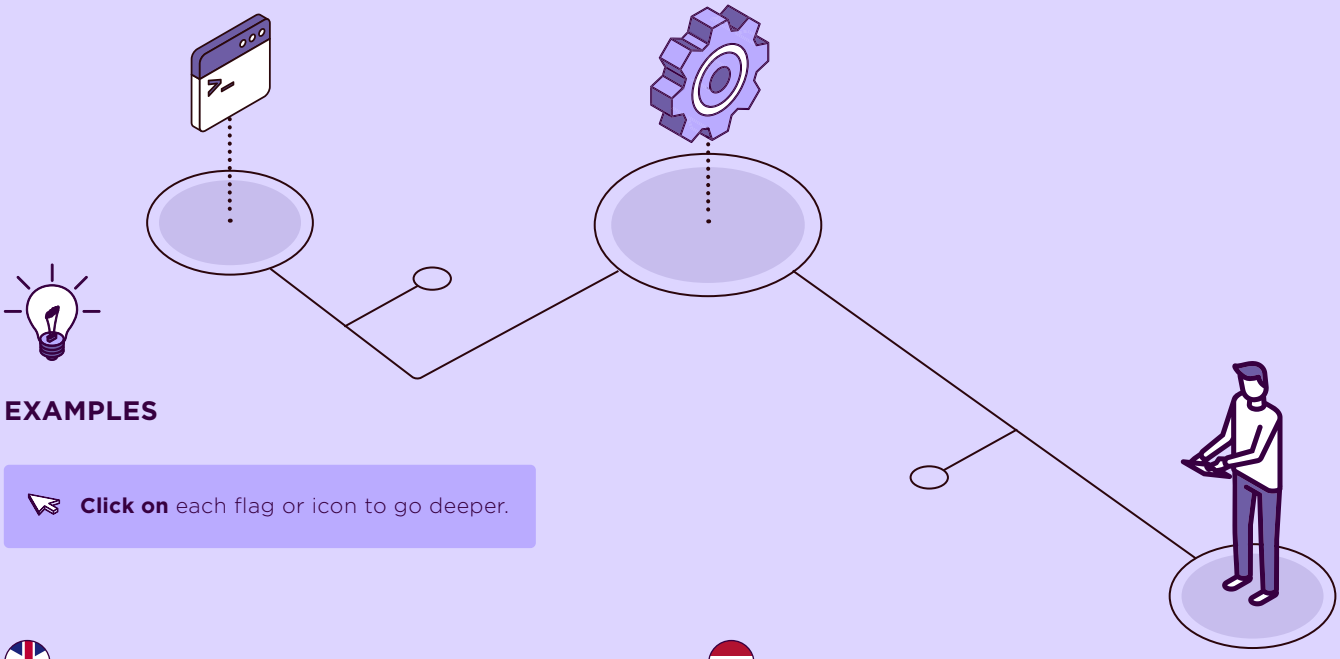
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

The tax payment period is approaching. This process used to be long and tedious as it had to be done on paper, with the taxpayer spending long hours with a calculator filling out forms. This has recently changed with electronic tax filing, as Camilo now gets a pre-filled of his tax return, on which he can make changes as he sees fit. This change in the system saves Camilo many hours of work (and, on the other hand, saves the tax administration from having to process hundreds of thousands of paper forms, saving a lot of time and money), which makes him very happy. He is also delighted with the system, since last year he had to manually enter the data for all the homes he has in his name, while this year the data appears automatically filled in. "Wow," thinks Camilo, "this system works so well... it gets better year by year".

Entrepreneur
Ana

Ana's company has to carry out all the necessary formalities with the social security administration to ensure that its more than two hundred employees are properly managed. For the large number of formalities she had to complete, Ana had a human resources department of five people, to which she had to add the cost of an administrative agency that physically handled the administrative requirements of social security. With the implementation of online employee management services by the social security institution, Ana has managed to increase the efficiency of the human resources department, since the procedures are carried out immediately, without waiting or delays, and she has also been able to dispense with the services of the agency. These savings in administrative services have been reinvested in R&D, making Ana's company more competitive and innovative.



EXAMPLES

Click on each flag or icon to go deeper.

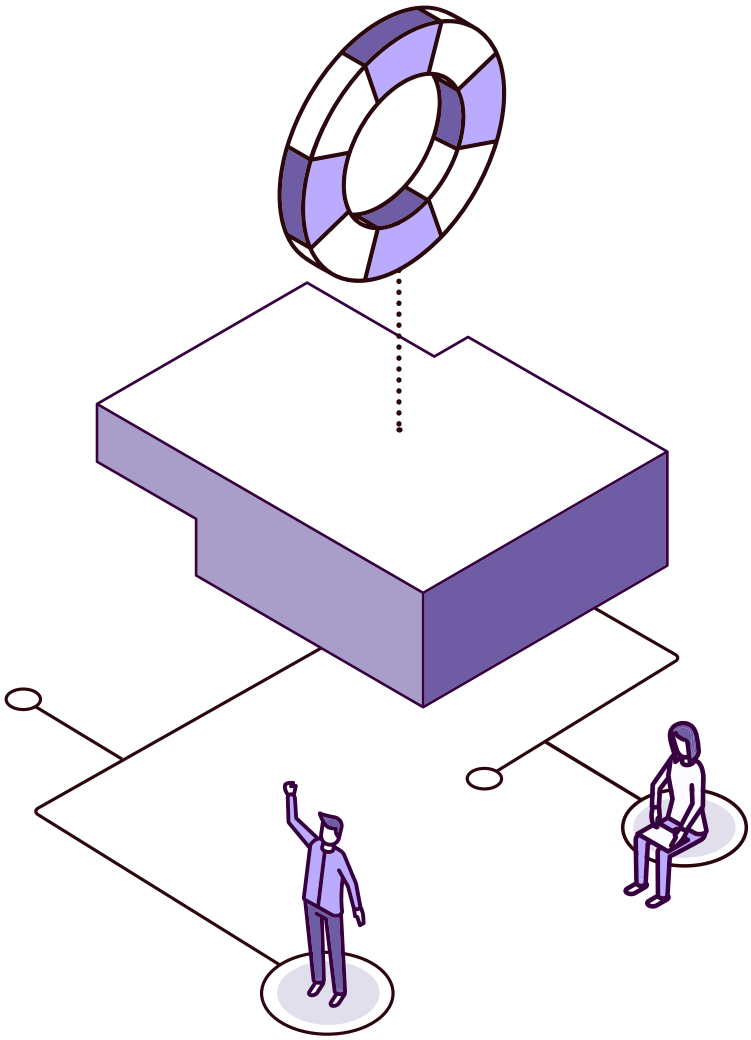
United Kingdom
National Audit Office Operational management Guide

Netherlands
Operational management

INDICATORS

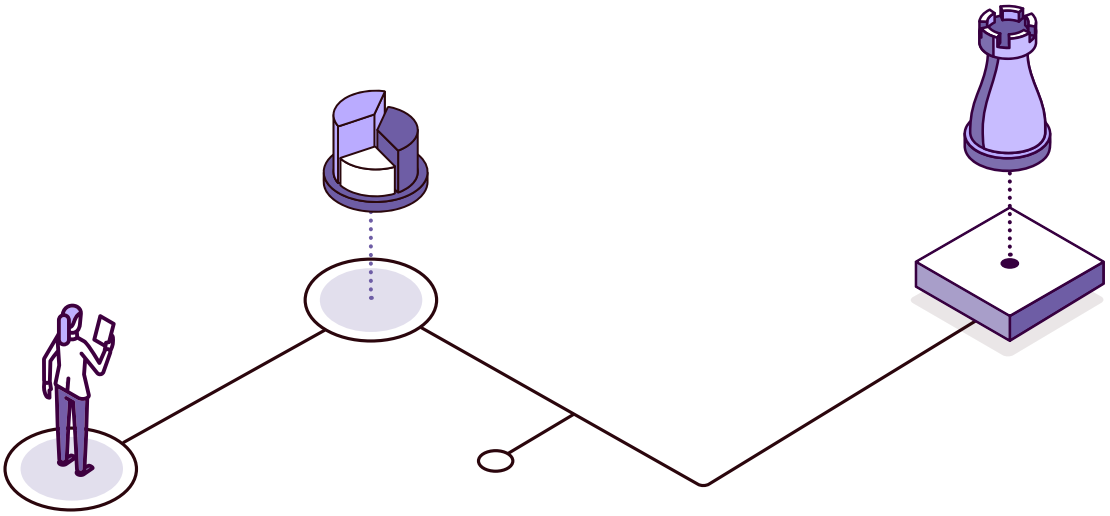
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Has the value chain that must be followed for a company or citizen to benefit from public services been identified?
- Is there a known procedure in the ministry/agency that determines what the life cycle of a service is?
- Are there people in the organization that are certified in the governance of services?
- Is there a framework for measuring the services provided?



1.5

Sectorial digital transformation strategies



The digital transformation of the country, as proposed in this document, is holistic and general: it affects all sectors, agencies, and actors within the country, as well as other countries. Up to this point, this publication has focused on common services that are useful for all sectors and, therefore, are subject to a common services coordinated throughout the country.

This vision of a means to an end is important because the ultimate goal—improving the lives of citizens and businesses—is achieved through specific issues such as:

- improved health care or education;
- good functioning of the justice system;
- improved infrastructure and transportation.

Common services are the means to facilitate the achievement of these goals. In turn, these goals are usually organized by themes or sectors. Each of them should have its own digital transformation strategy, coordinated and integrated into the country's digital transformation strategy.

Each of the vertical areas (health, education, etc.) may have a specific digital transformation strategy, which in turn may be aggregated by sector (social, economic-financial, etc.) and should be coordinated with the national strategy. Coordination teams (both internal to the institution and external, with the various stakeholders) should facilitate these coordinated strategies.

In fact, in many of the sections of this document it is explained how it is necessary that there is close coordination between the different vertical sectors and the governing entity of digital transformation. Therefore, governance mechanisms are proposed as the way to define the digital agendas of each of the sectors and, in coordination with the governing entity, align on at least key elements such as the following:

- The different road maps, to match the timing of milestones that make sense to align.
- Procurement plans, to take advantage of economies of scale in bidding processes or personnel selection processes.
- Communication plans, to offer a homogeneous image and align messages to citizens.
- Availability of common services, such as identity and digital signature, since they are basic for the construction of new digital services.
- Interoperability, to ensure that the systems of the different sectors are capable of exchanging information.
- Infrastructure,to ensure that all institutions have a means to store data and services.
- Cybersecurity, because cyberattacks must be fought together, in order to reuse defenses and knowledge, especially when government agencies share a common communications network.

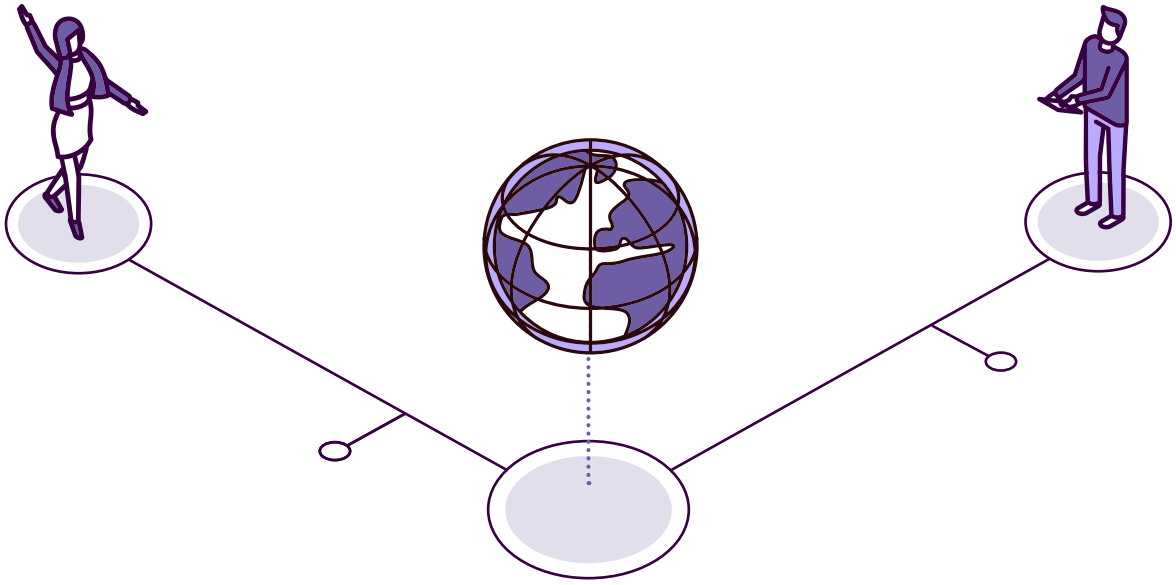
If this alignment of sectors and the governing body of the digital transformation is well done, it will undoubtedly offer better results to citizens.

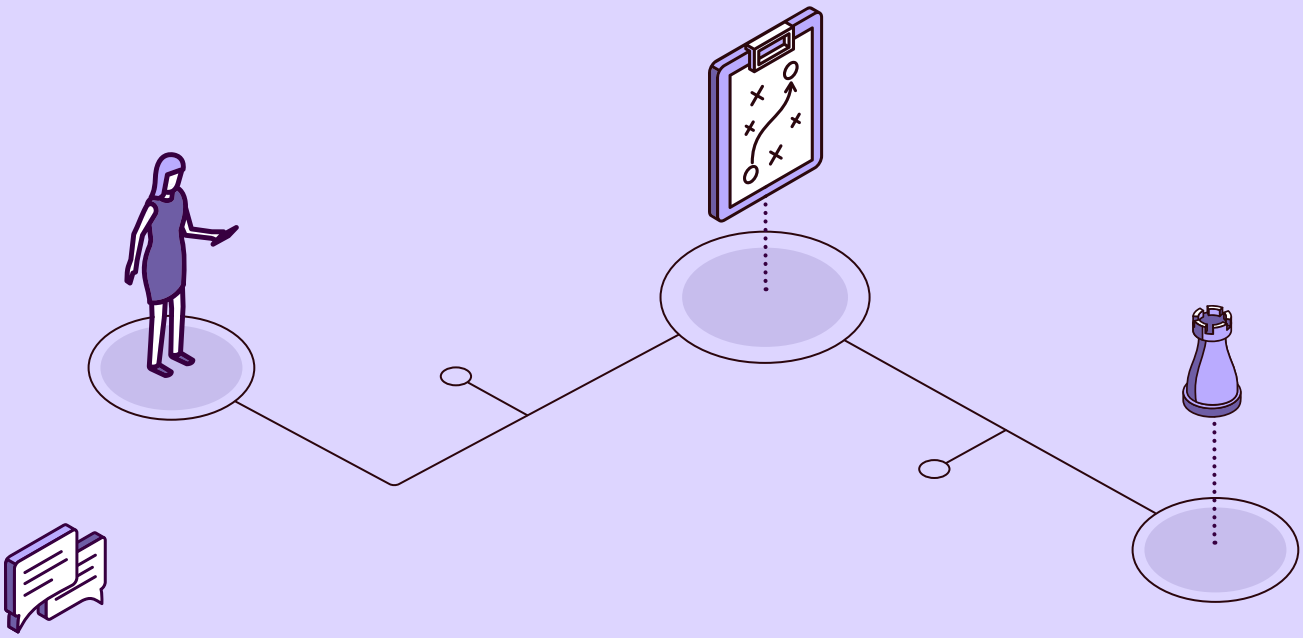
It is essential that each strategy of the different sectors be drawn up as homogeneously as possible. This will make them easier to review and to align.

In the same way that the lead agency must develop a strategy that encompasses the entire country and the common services and components, each sectoral area must focus the strategy on the problems of its sector. At the very least, they should contain the following:

- digital agenda
- road map
- technology strategy
- procurement plan
- communication plan
- cybersecurity plan
- risk management plan
- operational management plan
- change management plan
- regulatory changes
- talent needs
- monitoring

In summary, in order to provide value to citizens and to carry out a holistic digital transformation of the country, each sectoral area must establish its objectives and goals, and these in turn must be aligned with the governing body of the digital transformation and with the rest of the sectors with which they must relate.



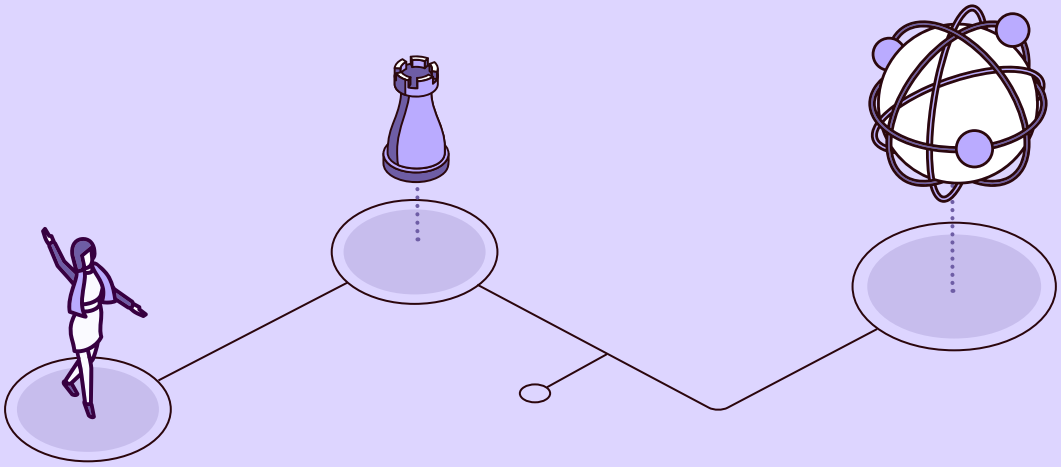


STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara is tasked by the government, like the other ministers, to work resolutely on the digital transformation of her sector. After gathering her team and defining their digital agenda and road map, they draft a digital health transformation strategy. After several meetings and discussions at different levels, making use of governance mechanisms, Sara and her team are able to make the necessary adjustments to their strategy so that it is coordinated with the rest of the ministries and with the governing body for digital transformation. This has ensured that they are aligned with centralized procurement processes and the necessary staffing levels.



EXAMPLES

Click on each flag or icon to go deeper.

Australia
Digital Health Strategy

Ireland
Digital Education Strategy

INDICATORS

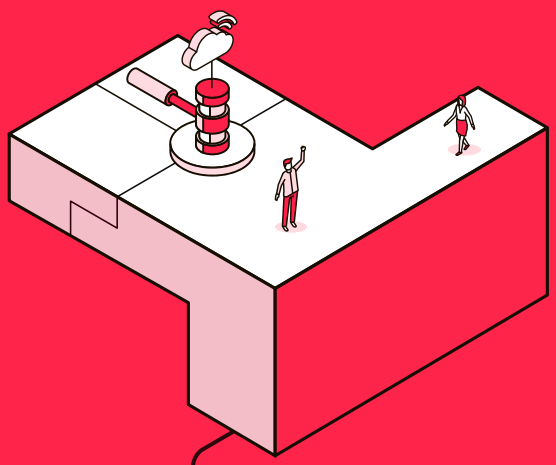
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

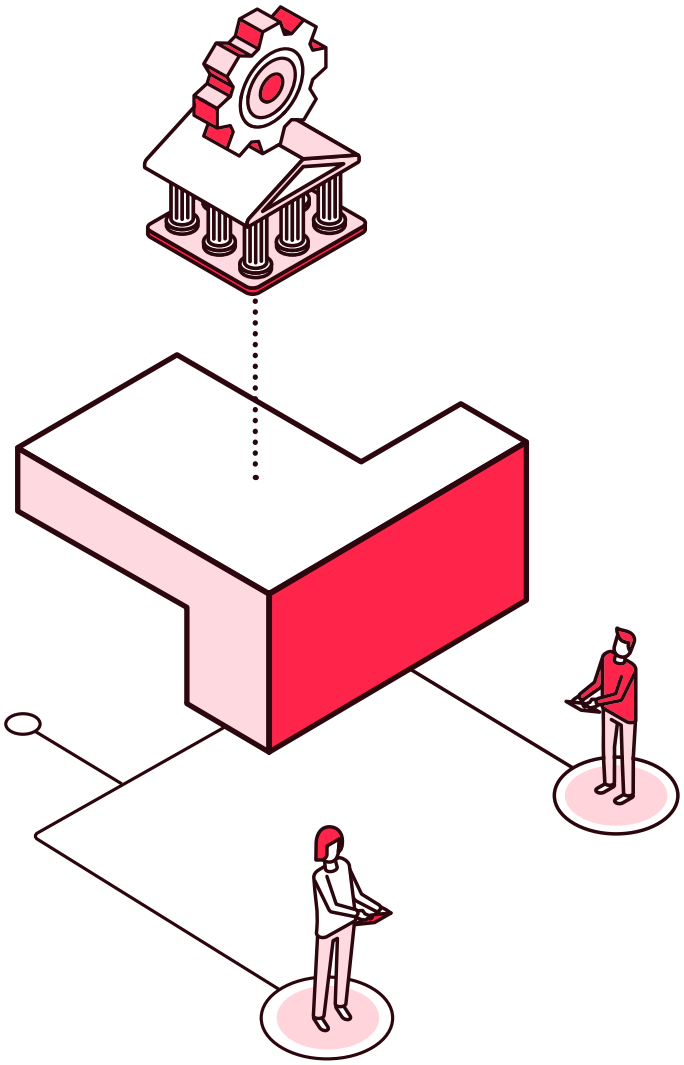
- Does each sector have its own digital strategy?
- Are these strategies aligned and cohesive?
- Is there a common country vision of the digital transformation to be undertaken by each vertical sector?
- Is there unified accountability to the governing body of digital transformation to be able to coordinate actions across sectoral areas?

CHAPTER

02

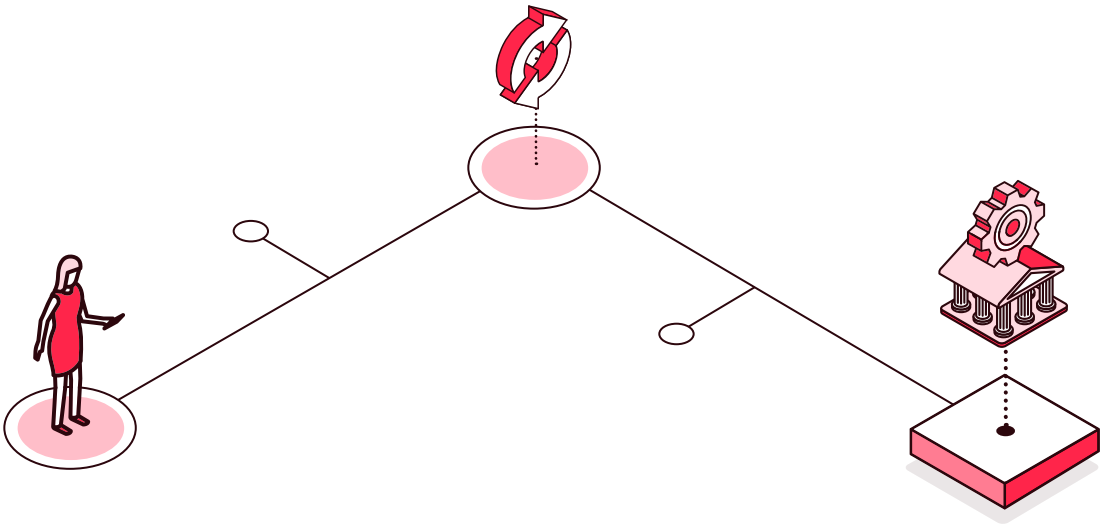
Legal and regulatory framework





2.0

Introduction



The public administration, including its interactions with citizens and companies, requires clear rules that establish how to proceed in all situations within its competence. These rules are embodied in legal instruments of varying hierarchy, such as ministerial resolutions, decrees, and laws. Any administrative field is regulated, so digital transformation must also be regulated. This is particularly important because the regulatory corpus of a country is often multiple decades old; therefore, it is not usually adapted to the new challenges and opportunities posed by new technologies, nor does it have the flexibility to adapt to rapid technological changes in the future. In fact, in many countries the public administration can only do what is permitted, what is regulated. It is therefore extremely important to develop a regulatory framework that enables the use and exploitation of new digital capabilities.

ONE OF THE MAIN REASONS WHY THE NEED FOR DIGITAL TRANSFORMATION ARISES IS THE ADAPTATION OF PUBLIC ADMINISTRATION PROCESSES TO THE NEW NEEDS REQUIRED BY SOCIETY IN ITS RELATIONSHIP WITH IT.

Depending on the country, the type of intervention (natural or legal person), and the specific service, the relationship with the public administration through electronic means must be regulated either as a right or as an obligation. In full coordination with the sectoral institutions, it will be the lead institution that will promote this regulation.

In this context, it is necessary to establish a regulatory framework that

- regulates the development and use of new technologies;
- adapts the different processes that have traditionally been developed within the administration;
- generates an environment of sufficient confidence for its adoption by citizens and companies.

THE COMPONENTS OF A REGULATORY FRAMEWORK FOR DIGITAL TRANSFORMATION

A legal framework that

- guarantees respect for the recognized rights of citizens in their digital relationship with the public administration in the same way as it guarantees it in their analogical relationship.
- ensures the public function of public employees in the execution of their jobs through these means.
- recognizes the validity of electronic proceedings before other institutions.

A technical framework that

- regulates and standardizes the technological development of the different solutions implemented.
- ensure technology neutrality and interoperability between divergent systems.

If the regulatory framework is seen as a set of rules, these are generally embodied in legal instruments with a hierarchical structure, depending on each country, but as a general rule they start with a law that regulates generic aspects, which are subsequently developed through decrees, ministerial orders, resolutions, technical norms, etc. This is particularly important because the traditional regulatory core of a country is not adapted to the new challenges and opportunities offered by new technologies. For this reason, it is vital to adapt the current regulatory framework to a structure that offers the appropriate flexibility that will be required in the future by the rapid technological changes and allows taking full advantage of the new possibilities and benefits offered by digitization.

BASIC FEATURES OF THE NEW REGULATIONS

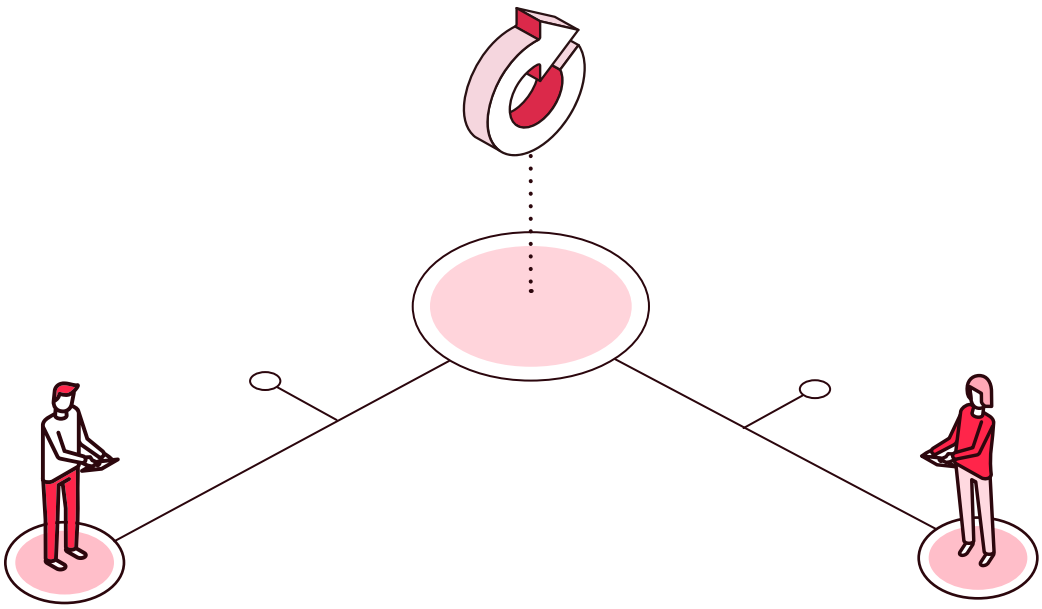
TBoth adaptations and the development of new regulations must be aimed at avoiding the complexity and fragmentation of the regulatory framework, including features that make it *inclusive, sustainable and balanced*:

- **Inclusive** because today, more than at any other time in history, the digital divide generated in the population by technology, either because of not having access to it, not knowing how to use it, or not being able to use it because of some kind of disability, is causing the physical or social isolation of some sectors of the population. It is an obligation of the legislator, therefore, to draft conditions that facilitate its access to all groups.

- **Sustainable**, by reducing the use of resources in its elaboration and maintenance, whether economic or personal. To this end, it is essential to design a correct strategy and regulatory structure that allows its management with the minimum investment.

- **Balanced** in two ways:

  - One in which thewatory framework that regulates technological aspects, or the relationship between citizens or companies and the administration, is of no use if any of the parties cannot assume them. In this regard, it is essential to understand the current and future situation of the population and the administration in terms of access to new technologies.



Not only will a sufficiently flexible regulatory structure be required to adapt to technological change and regulate it in the shortest possible time, but it will also be necessary to identify and modify/derogate the content of a large number of current regulations where expressions such as *"shall deliver in person to the citizen the certificate signed in the official's handwriting,"* so present in the traditional regulations based on the presence of the actions, are to be found.

Likewise, the regulatory framework must provide legal certainty to all the actors involved, from citizens and businesses to the public official in charge of executing the procedures. The establishment of a robust environment in terms of legal certainty will allow for the rapid adoption of change, as well as the sharing of information between the public sector, the private sector, and citizens in a climate of trust in the institutions, since it will not undermine rights or impose discretionary obligations on citizens and businesses, thus providing legal certainty to the entire system.

USE AND DEVELOPMENT OF NEW TECHNOLOGIES

The regulatory framework will regulate the use and development of new technologies and their application to the traditional processes of public administrations, transforming them into new digital processes with the incorporation of such technologies and with the redefinition of their execution and their relations with citizens, companies, and other administrations.

For example, in paper we work with the concepts of "original" and "copy," but in the digital world the "copy" becomes an attribute (metadata) associated with the "original" electronic file, since all copies, from a technical point of view, are "originals." Associated with this technological change are other concepts such as "format switching" (between electronic formats—for example, from PDF to other formats and vice versa—and also between paper and digital), which did not previously exist on paper. These examples, which may seem somewhat irrelevant, entail a series of associated changes that have an impact on document management, preservation and destruction policies, and the regulations that govern them, along with the effective implementation of so-called change management.

For this reason, a holistic view of the regulatory framework and its effects on the adoption of public policies based on digital transformation must be taken, since it not only involves the digitization of the process (doing electronically what was done on paper) but also incorporates a component of transformation and redesign of the process for its optimization and adaptation to the new digital environment. In turn, regulatory changes should be used to simplify processes, facilitate their use and access, and take full advantage of the opportunities offered by the digital world, prioritizing above all the reduction of the administrative burden of the new digital processes, both for the administration and for citizens and companies, and even eliminating procedures that will be meaningless in the new digital framework.

THE APPLICATION OF NEW TECHNOLOGIES TO DIGITAL TRANSFORMATION IS AN OPPORTUNITY TO CREATE A NEW REGULATORY FRAMEWORK IN THE ADMINISTRATION BASED ON THE ALIGNMENT OF ALL STANDARDS, WITH THE SOLE PURPOSE OF OFFERING A QUALITY PUBLIC SERVICE.

SOLUTIONS IMPLEMENTED

The regulatory framework must also regulate the technological development of the different solutions implemented through the development of technical regulations, guaranteeing technological neutrality and interoperability between systems, and creating a secure, stable, and innovative environment where both the administration and the private sector feel supported. This will provide a robust technological framework that will give rise to an ecosystem of interoperable, reusable, and sustainable applications and services based on the application of harmonized standards and norms, which will result in user confidence and savings in development and maintenance costs.

As has been mentioned throughout this section, the incorporation of new technologies into public administration requires short-term regulatory adaptation and the provision of a regulatory structure that is flexible enough to adapt the regulatory framework at the same speed as technology changes. To this end, it is important to abstract those regulations that by their very nature (laws, decrees) require a complex process of change to incorporate technological details that are likely to evolve or change in the short term. It may happen that by framing in a law a provision that affects certain rapidly evolving technology (e.g., digital signature or disruptive technologies), the law becomes obsolete before the technology is fully implemented.

VISION FOR THE FUTURE

When designing high-level standards for digital transformation, a long-term vision must be adopted. Thus, the opportunity should be given to include regulatory or technical aspects that, while not being sufficiently mature at the time of drafting the regulation, have been identified as critical in the short or medium term. This inclusion can be in an abstract manner in the legislation, with a mention of its subsequent development in a lower-ranking regulation. This type of action makes it possible to provide the first-level regulation with sufficient flexibility to regulate the near future, without jeopardizing the current situation.

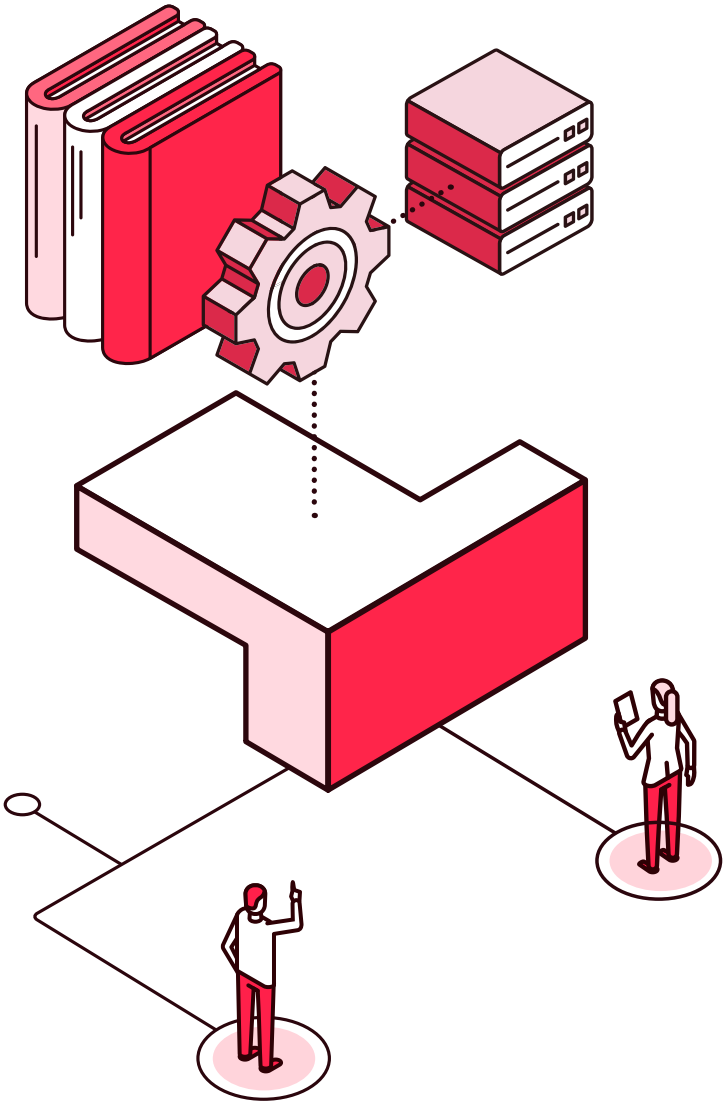
In many cases, recently published laws have not contemplated the application of technologies that, at the time they were being drafted, were not sufficiently mature but had already been identified as disruptive in the short term (artificial intelligence, biometrics, blockchain, sovereign digital identity). This has led in some cases to the immediate updating of the standard after its publication. In contrast, incorporating references to these technologies, which could later be regulated in lower-ranking regulations, into the developing regulation allows the country o have clear, easily updatable regulations in the future. These new regulations will support the lower-ranking regulation, be compiled in a single document and without cross-references between different regulations that add corrections on top of others. This is the reason why many countries have opted for a hierarchical structure, with laws to promote digital transformation that include generic country agreements and abstract ideas.

These laws are developed through regulations, decrees, or second-level norms, without going into the technical and operational issues because those detailsare subject to frequent technological changes. Technical issues are usually set out in third-level technical standards or are reflected in the form of technical guides or application rules, which can be modified and adapted to changes as they occur.

THE CREATION OF EXPERT COMMITTEES IN TECHNOLOGICAL REGULATION WITH A GLOBAL VISION IN REGULATORY AND TECHNOLOGICAL AREAS AND THAT ARE SENSITIVE TO CHANGE MANAGEMENT IS RECOMMENDED.

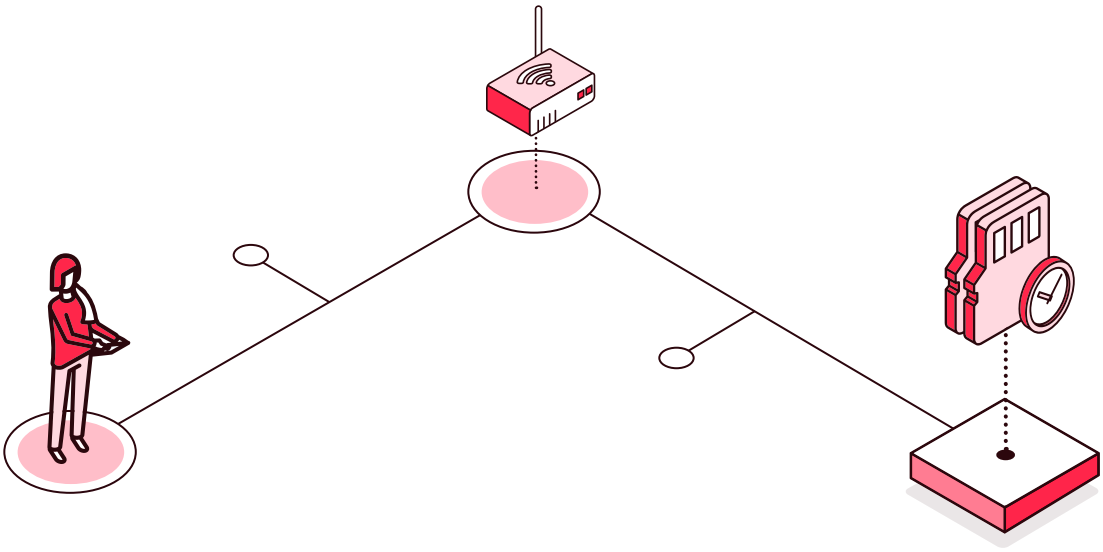
Finally, as can be seen in the following subsections of the document, the regulatory framework must regulate an infinite number of aspects within the administration and outside it. This implies the need to invest a sufficiently large initial amount of time to design a regulatory strategy to support both the traditional daily activity of the administration, which cannot be stopped and must be provided without undermining the rights of citizens, and the new digital activity that will gradually be implemented and that will coexist for a long time with the traditional one.

In this sense, it is essential to assume the double regulation that will be necessary at certain times, but a correct development strategy will make the difference between an orderly transition from the traditional framework to the digital framework or a tortuous path full of regulatory uncertainties.



2.1

Administrative simplification



Administrative regulations tend to impose information requirements or obligations on businesses and citizens, which can generate access barriers and compliance costs, in addition to the costs for the government to ensure their provision. The cost of obtaining a duplicate identity document, for example, is not only linked to the fee paid for the document, but also to the time and resource costs that it takes a person to comply with all the requirements requested by public entities (travel time, waiting time, photos, etc.). These costs are only justified for reasons of general interest and constitute an *administrative burden* that should be minimized in order to promote economic efficiency, favor competitiveness, and encourage the free action of companies, officials, and citizens.

In this sense, administrative simplification and digital transformation are complements to improve the quality of public services, to the extent that they promote the elimination and/or streamlining of processes or procedures created by the public administration with a view to regulating the granting of authorizations and benefits, or the fulfillment of obligations on the part of citizens and companies.

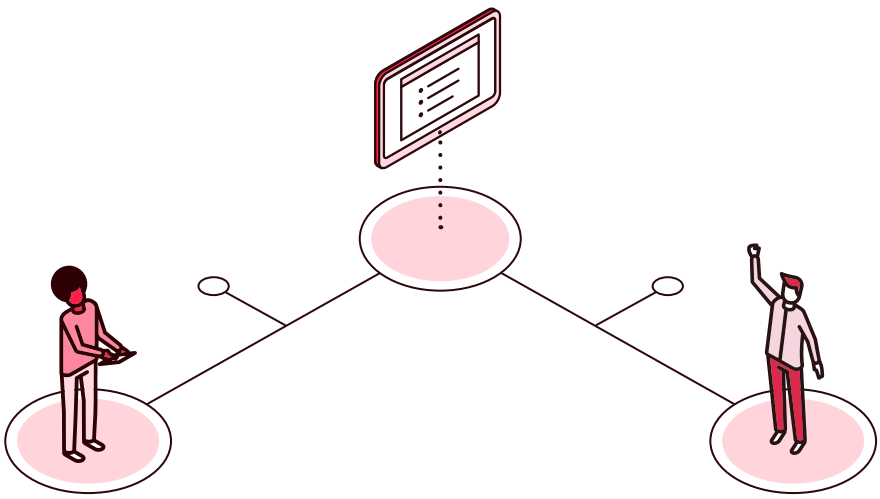
ADMINISTRATIVE SIMPLIFICATION ACTIONS

Administrative simplification focuses in particular on improving governmental procedures, since they are transactional public services that are often characterized by excessive steps, unnecessary requirements, complex regulations, and obsolete management models. Its basic principle is to generate the greatest possible value for the user by minimizing transactional costs.

Generally, administrative simplification actions can be grouped into three categories:

- **Technology:**
  - Put procedures on line.
- **Regulatory changes**
  - Adapt the norms that regulate service delivery. In a significant number of cases, modifications of this type are unavoidable since the legal structure of Latin American countries (public law) prevents doing what is not regulated. In this sense, one reform option would be to modify the general administrative procedure, which governs the actions of all public institutions vis-à-vis citizens (an example of this practice is Spain, with its 2015 administrative procedure reform).
- **Management changes:**
  - Integrate and facilitate access to the different channels (face-to-face, digital and telephone).
  - Reduce the complexity of the language that appears in the forms or instructions associated with the process.

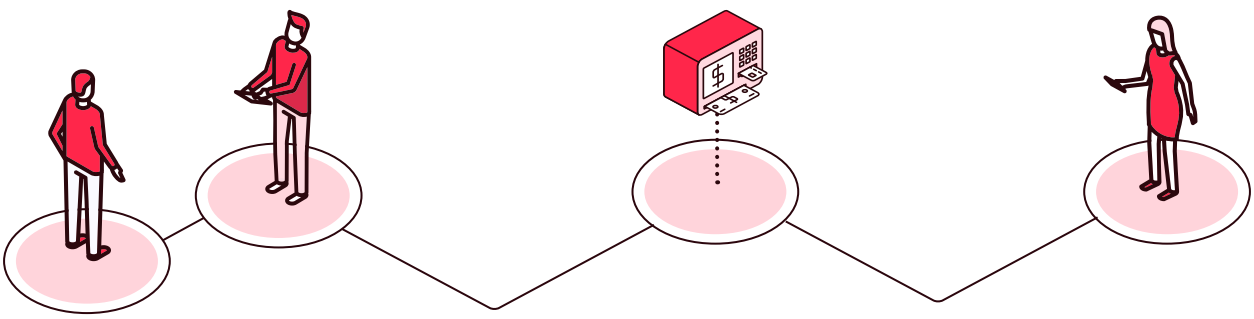
ACTIONS CAN BE PRIORITIZED ACCORDING TO THE NEEDS OF USERS AND THE DIFFICULTIES THEY HAVE IN ACCESSING SERVICES.



SOME KEY STRATEGIES

There is no single strategy for administrative simplification; however, some key steps can be highlighted that could guide the process:

- **Make an inventory of existing formalities:** Creating a "catalog" of formalities makes it possible to prioritize simplification actions around issues such as
  - the volume of procedures provided.
  - the requirements that users must meet
  - delivery times.
  - the link with economic activities.
- **Measure transactional costs:** This strategy can serve different purposes associated with administrative simplification at different scales:
  - Calculating the burden on citizens in monetary terms can help to make the case for investment in simplification actions, since fierce competition for fiscal resources is often decided by calculations of returns on investment.
  - A comprehensive measurement, based on administrative data to minimize calculation costs, can be an input to prioritize the procedures to be simplified.
  - More detailed measurement, for example through the standard costing model, can be used to identify priority areas for reform within a process, once it has been prioritized.
- **Establish the figure of the "service inspector":** This means having an official responsible for verifying that the established standards are complied with and with the power to impose sanctions on persons and/or entities that fail to comply.



USEFUL TOOLS

What is really important in any administrative simplification action is to place the citizen at the center of the service and make access as simple as possible. Any reform or restructuring of a process must take into account the experience of the citizen or the company performing the procedure and seek the coordinated use of digital, regulatory, and managerial instruments (including possible modifications in human resources) in the analysis and proposal for improvement of production and delivery processes.

One element that is proliferating and being used more and more to bring administrative simplification closer to citizens is chatbots. These digital solutions, which make use of natural language processing (NLP) techniques allow citizens to feel more comfortable interacting with the administration, as long as it is well designed and built. Keep in mind that, on many occasions, citizens are not aware of the options that the administration offers in a given situation. On many other occasions, citizens may also feel embarrassed about having to ask too basic questions to the public employees at the counters. And these two situations, together with the fact that on many occasions the web portals do not offer the information in the clearest possible way, can make the use of chatbots for a first approach of a citizen, in a specific situation, a good option. The citizen will be able to explain in natural language what his situation or problem is, allowing the chatbot to inform him of his options or possible procedures. Depending on the depth to which you want to go, the system can even offer the forms that are useful, suggest sections of the web that can help, or even provide information on how to do the procedure online or which offices to go to. If, in addition to the chatbot, a single portal is made available to citizens where they can find the catalog of procedures and the citizen folder with access to all files and services, regardless of the administration, it will be easier for citizens to access the administration.

It is worth insisting that elements such as the chatbot, single portal, and citizen folder, among others, are tools that undoubtedly help greatly to promote administrative simplification, but in no case should they be used to cover up the bureaucratization that in many cases is already entrenched. For this reason, it is essential that administrative simplification begins with the simplification of procedures and the elimination of administrative burdens. Moreover, this step is essential when it comes to bringing administrative services to the digital world because if these are not simplified and streamlined, there is a risk of building services in the digital world that do nothing more or less than automate chaos.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Vice minister of health
Sara

When Sara assumed her position as vice minister of health, her first objective was to streamline the process of affiliation to the public health system. The problem centered on complaints about the delay between completing the paperwork and being able to use the health services, as well as the long lines due to the crowds of citizens waiting in line to complete the process. She thought that a digital appointment system, through which citizens could reserve the date and time to go to the public office to carry out the procedure, would speed up the whole procedure, as it would avoid long lines of people at the counters.

After a few weeks of operation of the online appointment platform, Sara noticed that, although there were fewer people at the windows, the waiting times to be enrolled in the system had not changed significantly, and complaints about the service continued, now with complaints about appointments that were only scheduled for weeks later. Sara had not given much importance to the fact that in order to comply with the procedure, citizens had to bring several documents that had to be validated at the windows, take pictures, and fill out forms. All these procedures meant that people spent a lot of time looking for their papers and then during the service at the public offices. The number of people in the department was not the problem; rather it was the consequence of complex procedures and processes that had to be fulfilled. Sara realized that, had she conducted an analysis of the activities involved in the paperwork process, she could have made effective simplification interventions by addressing the causes of the delays in enrollment, through measures such as revising standards, digitalization, or reorganization of the service process.

Citizen
Camilo

Camilo is not used to doing business with the administration, and every time he is confronted with them, he thinks they are difficult to understand, they have many steps, they force him to go to different offices to get documents (sometimes from the same public entity), and everything takes a long time. He does not understand why some requirements have not been simplified, nor how the transaction is handled internally, which makes him more and more dissatisfied with the institutions. He discovers that there is a chatbot on a web page that provides useful information on the procedures he has to carry out, and at least he has an idea of what he has to do and where to go.

Entrepreneur
Ana

Ana is part of the pilot program to simplify customs procedures that her country has promoted with neighboring countries. Now, all foreign trade procedures and associated documentation can be done digitally, in advance, and a significant time saving has been achieved in border crossings. Ana is delighted, not only because her relationship with the public administration is easier, but also because thanks to these time savings, her company is more competitive in international markets and has more customers. Ana is eager for the pilot to become a general project for everyone and to be carried out with more countries, because she is sure that it will clearly benefit the country's competitiveness.

Mayor's advisor
Daniel

Daniel has just received public recognition for his work in simplifying procedures for businesses. He learned about the new regulations that allow simplification of these procedures, and his became one of the first municipalities in which opening a business does not require all the certificates and formalities that other administrations require. Risks are now classified, and depending on the results of this classification, blocking procedures are replaced by declarations of responsibility and ex-post control. On the other hand, the way was paved so that all procedures could be carried out through the internet. This has brought more investment to the municipality and has generated greater satisfaction among the businessmen who were already based there, so Daniel feels very proud of this recognition.

EXAMPLES

Click on each flag or icon to go deeper

Mexico
Simplification of Procedures and Services Program (SIMPLIFICA).

Portugal
Zero Licensing Program

European Union
Administrative Burden Reduction Program

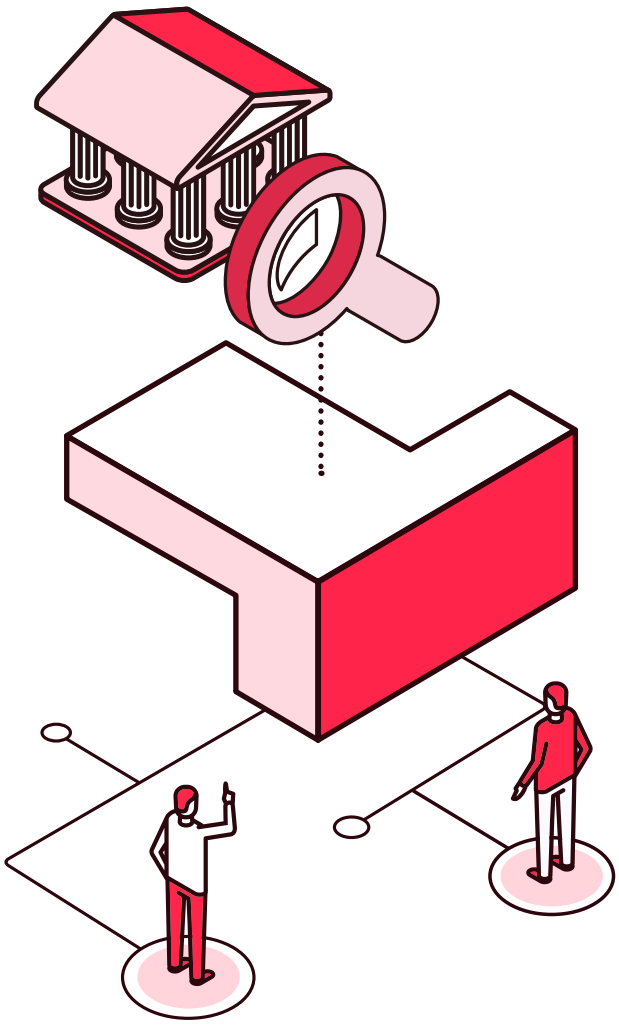
OECD
Standard Costing Model

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

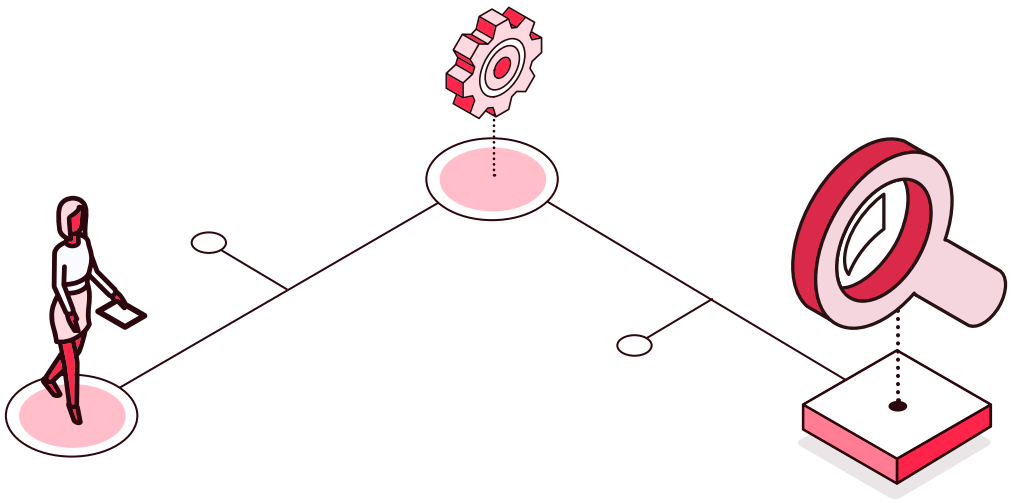
- Is there a catalog of procedures? If so:
  - Does it contain all the procedures provided by central government entities?
  - Does it contain all the procedures provided by subnational governments?
  - Does it define processes for the creation, modification, and elimination of procedures?

- Is there a technological tool for documenting procedures?
- For the absolute majority of central government procedures, are processes documented with descriptions and flowcharts showing all steps, actors, business rules, deadlines, *inputs, outputs,* etc.?
- For the absolute majority of subnational government procedures, are processes documented with a description and flowchart using BPMN or similar notation, including all steps, actors, business rules, deadlines, *inputs, outputs*, etc.?
- Are continuous improvement policies in place?
- Are multidisciplinary simplification teams in place (management, technology, human resources, regulatory)?
- Is there a management system that allows your institution to know the exact demand for procedures (volume provided)?
    - If so, do you use indicators to measure performance (such as delivery times, satisfaction, user costs, quality)?
- Are estimates of the unit cost of processing procedures (the cost to the public institution) made on a regular basis?
- Are estimates of the cost to users of accessing procedures made on a regular basis?
- Are process performance indicators used for agency management purposes (e.g., distribution of human resources among services)?
- Is there a figure responsible for compliance with service delivery standards (a service inspector or similar)?
    - If so, does this figure have sanctioning power?



2.2

Transparency and open government



Although there are numerous definitions from different angles and disciplines, it can be stated that an open government is one that promotes a fundamentally different relationship between the state and citizens, with the aim of building more legitimate and accountable institutions and greater effectiveness and efficiency in the provision of public services through the use of new technologies. Open government strategies consist of three fundamental pillars:

- transparency
- integrity
- collaboration and citizen participation

The notion of transparency is directly linked to the right of access to public information. It is classified into the following:

- **Active transparency:** Refers to information that governments publish or should proactively publish.
- **Passive transparency:** Refers to the information provided in response to requests for information submitted by citizens to different entities obliged to respond to them.
- **Focused transparency:** Refers to public information that is organized in such a way that it is socially useful for citizens of various social groups (companies, consumers) according to their interests, to facilitate their decision-making.[22] The laws that regulate open government policies and transparency in particular are usually those on access to public information, public integrity, or open data policies, and/or those that promote the participation of civil society in matters of public interest.

22. Fung, A., Graham, M. y Weil, D. (2007). *Full disclosure: The perils and promise of transparency.* Cambridge University Press.

THE NORMATIVE VERSUS MODERN CITIZENSHIP

Social and economic changes have generated a new, more informed, interconnected citizenry that demands higher-quality public services. At the same time, there has been a decline in citizen confidence in institutions, from political parties, justice, government, and public administration. Democratic systems of government must respond to all these demands and move toward a relational administration, reinforcing the legitimacy of public decisions and efficiency in the provision of public services and openness to citizens.

Therefore, it is necessary to promote the general interest by creating spaces where civil society can approach the administrations, learn about issues of interest to them, and participate in the decisions that may affect them, as a way of strengthening democratic systems. To achieve these objectives, more information and the expansion of channels for the participation of the citizenry as a whole are required.

In order to face this context, it is increasingly common to find regulations that regulate all public entities and develop principles of transparency and open government (including citizen participation and collaboration and accountability), with the aim of restoring citizens' trust in institutions. It is not uncommon to find that concepts such as transparency, public information, accountability, good governance, promotion of citizen participation, and interadministrative collaboration, among others, are included in the regulations as principles of the administrations or as citizens' rights.

ICTs open up the possibility for government to recover its lost space, improving both the way it relates to society (services, participation, transparency) and its internal decision-making processes. The generation of computerized records relating to all administrative actions (files, reports, regulations, registers, etc.) and the technologies that make it possible to organize, index, and catalog information are now also an essential tool for developing systems to provide all this information to citizens in an accurate, natural, and accessible way.

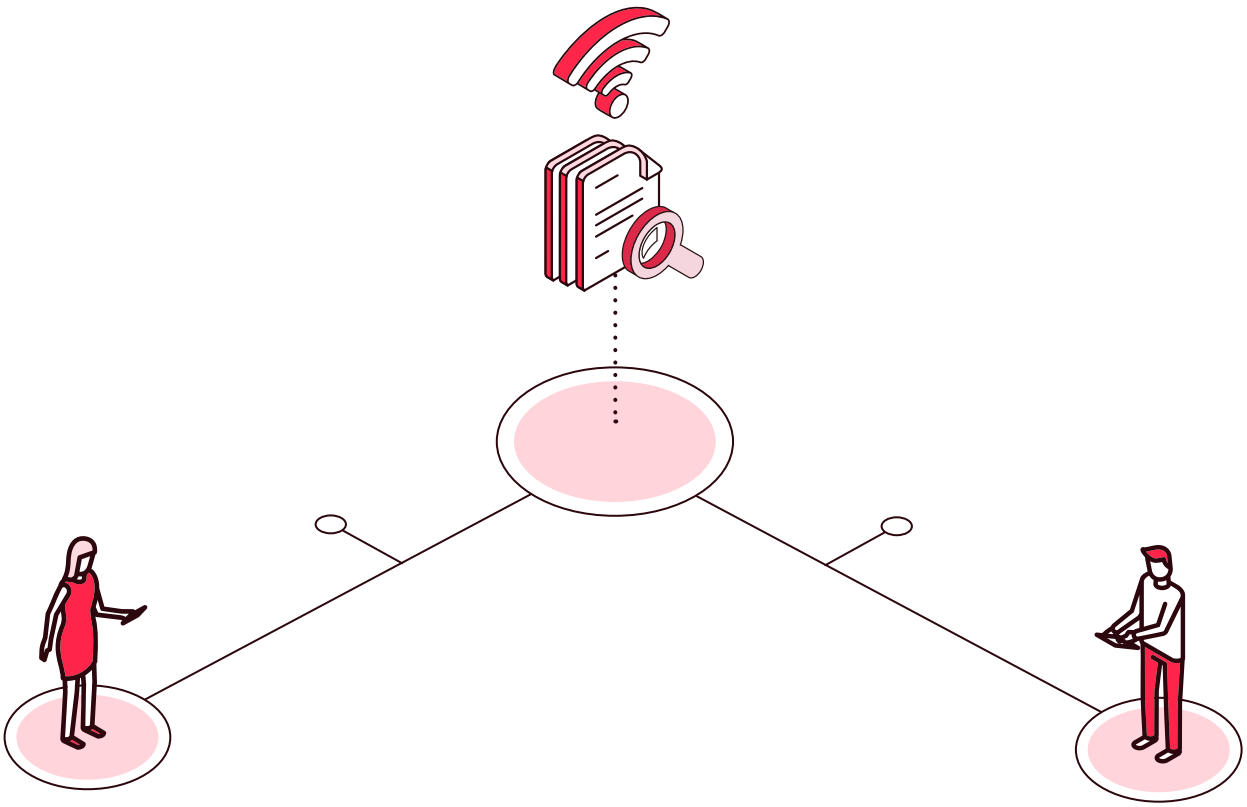
In addition, new technologies associated with the processing of huge volumes of data (such as big data, business intelligence, etc.) and the analysis of these with new approaches and perspectives entail the possibility of providing very relevant information to citizens, including indicators of the evolution of the levels of provision of public services, their social impact, or the results of the public policies adopted.

STEPS TO CREATE A NATIONAL TRANSPARENCY FRAMEWORK

- **Adoption of laws and regulations that respond to international standards and best practices:** Most Latin American and Caribbean countries have made progress in adopting laws on access to public information and have legislation to promote open government policies such as social participation and public integrity. These regulations should not be static but should be updated periodically in light of their results and new trends, with a view to allowing the use of technology and thus be more efficient and effective.

- **Institutional capacity to enforce regulations:** This requires agencies to implement and/or supervise specific public policies, with trained human resources in sufficient numbers and adequate infrastructure and digital resources.

- **Apply the regulations and evaluate the results obtained:** This will make it possible to diagnose and evaluate the public policy.



ACTIVE TRANSPARENCY

Access to information laws require the publication of certain relevant information in public portals; for example:

- budgetary and financial information.
- state assets.
- who makes up the staff of an institution, especially the management positions, their curriculum to reach that position, and how they are selected.
- procurement of public goods and services of all agencies.
- agendas and relations with companies and *lobbies.*
- the internal organization and competencies of public entities.

This information is usually published in different formats. Among them, the open data standard is currently the most promoted as a good practice, to facilitate its processing by automatic means and its reuse or distribution by third parties. Good practices also require that the data be updated periodically, that they be easy to access and in user-friendly formats, and that they employ visualizations and wording that is understandable to ordinary citizens.

Now, as mentioned, the rules of access to public information should allow citizens to exercise their right to request information that is not part of the catalog of active transparency information. The laws, in turn, must protect certain principles, such as the presumption in favor of the principle of publicity (with few exceptions), free of charge, informality, speed, among others. With few exceptions and limitations, in general, citizens should be able to access any information, file, or decision-making of the public administration (always respecting the rights of others, such as personal data protection).

It is usual for the regulation to establish a guarantor body to ensure that the provisions of the transparency law are complied with, in order to ensure effective compliance with this citizen's right. As in the case of data protection, this body must be sufficiently free from political or administrative pressures, so its relationship with the government or the corresponding public entity must be one of independence, since in general it is the body in charge of dealing with citizens' complaints and acting on their behalf, to ensure that the government or the institution complies with the transparency regulation.

CITIZEN PARTICIPATION

Transparency is also a precondition for greater citizen participation in matters of public interest, which affects the legitimacy of decisions and confidence in the state. Transparency is intended to create spaces that encourage legitimate debate and the direct involvement of citizens in political or administrative decision-making.

Increasingly, countries are regulating the creation of participatory budgets, opening public consultation periods with face-to-face and virtual channels, and implementing innovative design thinking methodologies so that citizens are part of the solution of public policy problems and can even collaborate in the design or adaptation of public services to their real needs. This increases the participation of citizens in public decisions that affect them, raising the standards of quality and effectiveness of public services, and, above all, improving the functioning of the social contract between institutions and citizens, as the latter become more involved in decisions.

MANY COUNTRIES HAVE ADOPTED MECHANISMS WHEREBY CITIZENS CAN KNOW, PRIOR TO THEIR APPROVAL, THE CONTENT OF REGULATIONS AND PARTICIPATE IN THEIR CONTENT AND DEFINITION.

Technological tools make citizen participation more viable by eliminating geographical and time barriers. This has been reflected in different ways:

- The creation of spaces for participation in portals, both permanent (participation portals, citizen proposal websites, etc.) and temporary (on specific campaigns, participatory budgets, public consultations, etc.), which have become a powerful instrument for channeling in an orderly manner the involvement of civil society, organized or individual, in public affairs of major interest.

- The use of social networks and other messaging systems has de facto established a new, very direct, immediate, and in many cases public channel for interaction between administrations and citizens.

- Direct intervention of citizens, either individually or through associations, in public affairs.

    - For example, if citizens can use an application on their cell phones to report streetlights that are not working or asphalt problems, as long as the problem is solved and the citizen

sees that his or her complaint has been addressed, relations between citizens and institutions can be restored, valuing the usefulness and public service offered by the latter and reinforcing the social contract that makes it possible for countries to function.

Therefore, an *open government* approach based on *transparency* in the management of public resources, an *open data* policy for its reuse, and *citizen participation and collaboration in* order to take part in public affairs and decision-making for better management imply a fundamental change in the relationship model between the administration and the citizen. With this approach, citizens have ceased to be mere recipients of government action and services provided by the administration, assuming a much more active role and playing a key role in the definition, implementation, and evaluation of public policies.

OPEN DATA

There is a growing awareness that data is a fundamental economic asset for a country. Large technology companies that do not have relevant physical assets are important in the stock market precisely because they have data.

Public institutions are often the agencies that accumulate the most data in a country, but in general and until recently these data were jealously guarded by each agency, in silos. There used to be no openness toward society, with data that could be processed automatically, which limited the potential use of this information, even though there were clear benefits for the producing organization. To overcome this inertia, a regulation is needed that frees the institutions from these constraints and forces them to make the data available.

Therefore, open data regulations should do the following:

- Oblige public entities to give effective access to the data they have, in order to improve transparency, and also to offer this information to both citizens and companies, in order to create added value.

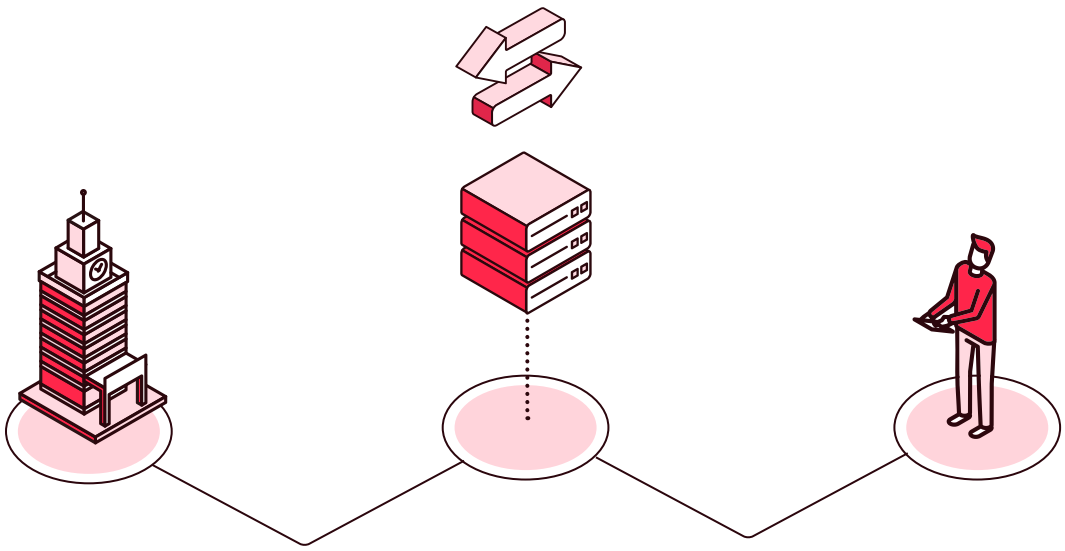
- Establish the conditions under which institutions have to make data available for consumption by other public entities as well as the private sector. It is important that this regulation is aligned with and respects the rules that exist in relation to the protection of personal data, but it is necessary to be assertive in the regulation of data openness, since the protection of personal data is often used as an impediment to the release of data. In order to make protection compatible with the opening of data, rules must be established that, by means of procedures for anonymizing, generating aggregated data, etc., allow the opening of originally personal data, without jeopardizing the protection of individuals' information.

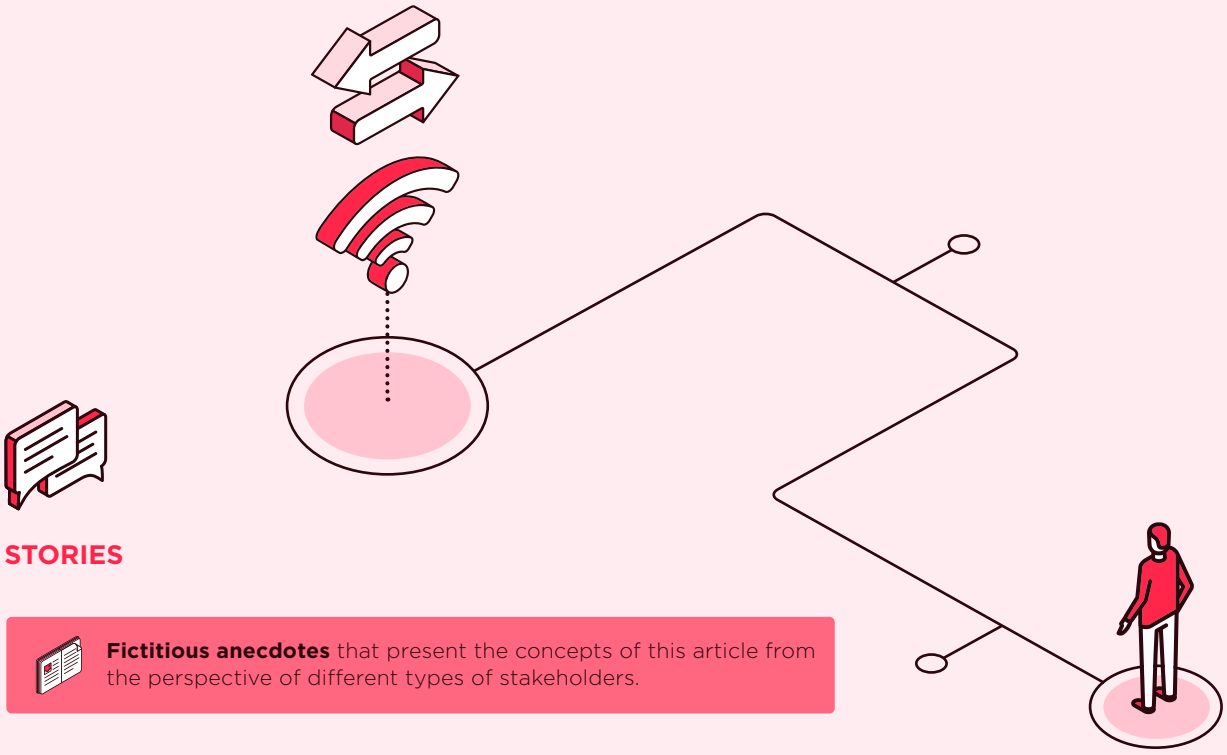
- Facilitate the reusability and automatable processing of the data; therefore, aspects such as the types of formats in which the data should be released, or provide the context meta-information associated with the data, so that automatic processing can be carried out, should also be considered.

- To regulate classifications and datasets by release, and to attempt guidelines and standardization among the different public sector entities, so that data from similar categories can be managed together and easily processed. Sometimes the challenge arises that data from the same health category, for example, are so different among the different institutions that provide them that they cannot be exploited jointly.

- Consider licensing and possibilities for data reuse. As in the case of intellectual property or software licenses, in the case of data it is necessary to establish under what conditions and under what framework both the initial and derived data can be used, reused, and exploited. For this reason, the regulatory framework in relation to licenses for the exploitation of personal data must be carefully considered.

- Control knowledge of and access to released data. There is no point in having released datasets if you cannot find them or know of their existence when you are interested. It is therefore necessary to regulate how datasets should be published on a country portal, so that they integrate information from different institutions (or even the private sector) with simple criteria for searching, accessing, downloading, and reuse, so that society can exploit the available data as efficiently as possible.





STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Entrepreneur

Ana

Ana has just seen on television that a regulation is being considered that directly affects her business. Thanks to the advice of a friend, she went to the website for citizen participation and regulatory development, and not only was she able to learn about the proposed reform and access its draft and the planned timetable, but also, based on her experience, she proposed a series of improvements to the articles, which she hopes will make the regulation more effective and useful. Ana is satisfied and feels more connected to the regulation and the government thanks to the possibility of participating in the issues that affect her.

Ana has just seen that information on tenders is published in open data format and is automatically actionable. This is especially interesting for her because, thanks to this information, she automatically finds out about any public tender she might be interested in. She used to miss opportunities because she could not have someone hired to read the official journals. With this information in open data format, every time there is something interesting, a notice automatically reaches her company's commercial department.

Citizen
Camilo

Camilo is a citizen who is very involved in the social activity of his neighborhood since he belongs to the neighborhood association and is closely linked to his family's lifelong neighborhood. Now he is worried because he has heard that the municipality is not going to do any work there and is focusing all its efforts on other areas, which is generating a deep social unrest. Thanks to his knowledge of the transparency portal, he has been able to access information on the municipality's works and has indeed verified that there are no works in progress in his neighborhood, something easy to see because all the information is georeferenced. Thanks to this portal, he realized that this is due to a delay in contracting, attributable to a company, and that not only are there several works planned, but also that a participatory budget is available for the neighbors themselves to propose the works they are most interested in. Camilo is happy to present all this information at the next neighbors' meeting and to change a feeling of anger for one of approaching the public administration, which will improve the life of his neighborhood.

Camilo is pleasantly surprised with his municipality. As a legally licensed cab driver, he belongs to the association of cab drivers who have an app that, through the use of open traffic data, helps him avoid cuts or traffic jams, saving him a lot of time (and thus allowing him to make a lot more money). This already existed in private mapping apps. What his city council has now published are the licenses for all events (sports, concerts, cultural), so Camilo can foresee, for example, where he should go to pick up customers at the exit of a concert. His clients are also delighted: they used to say that it was impossible to get a cab at the exit of large events.

Vice minister of health
Sara

Sara has a reputation for innovation, and open data is no exception. Having the peace of mind of its data protection policy, and ensuring the aggregation of open and anonymized data, she has decided to publish health data so that medical research has the possibility to advance and recognize patterns, as well as to improve the treatment of patients and diseases.

Mayor's advisor
Daniel

As an advisor to the mayor of a municipality, Daniel is clear that making the mayor's office information transparent and easily available to citizens can improve the effectiveness of public management. However, he is sometimes confronted with the mayor's office officials themselves, who are afraid of change processes and have become accustomed to working in a way that is closed to the public. Thanks to the regulation of transparency and good governance, it can change these practices, allowing it to make more and more information public, as well as to collect proposals and improvements that make its management more efficient day by day.

Daniel is proud of the award he is receiving from the business association. They have offered it to him because he has led the municipality's open data policy. Specifically, he reports in a georeferenced way on the licenses granted for businesses. Thus, everyone can see where the nearest stores, supermarkets, or hairdressers are. In addition, new firms are using this system to determine where there is a lack of services, which encourages the opening of establishments in these neighborhoods and improves the chances of survival of the companies.

EXAMPLES

Click on each flag or icon to go deeper

Chile
Citizen Participation Law N°. 20.500

Mexico
Budget transparency portal

Argentina
Principles of access to information

Chile
Virtual Congress

Paraguay
Transparency in public investment

South Korea
Legislation

Spain
Portal of transparency

Spain
Legislation

United States
Open Government Data Act

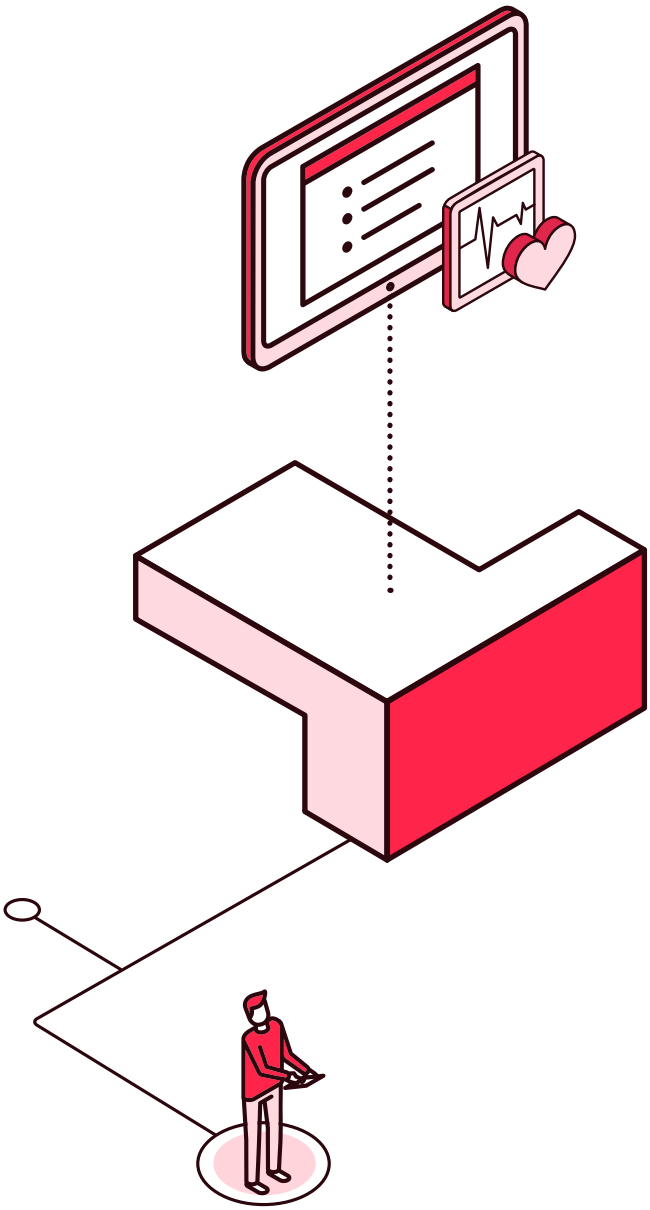
INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there regulations about the following?
  - Access to public information:
    - Are these regulations binding on subnational governments?
    - Is the obligation of the public administration to respond within a fixed period of time to a citizen consultation regulated?
  - Citizen participation:
    - Are these regulations binding on subnational governments?
    - Is the obligation of the public administration to respond within a fixed period of time to a citizen consultation regulated?
  - Open data:
    - Are these regulations binding on subnational governments?

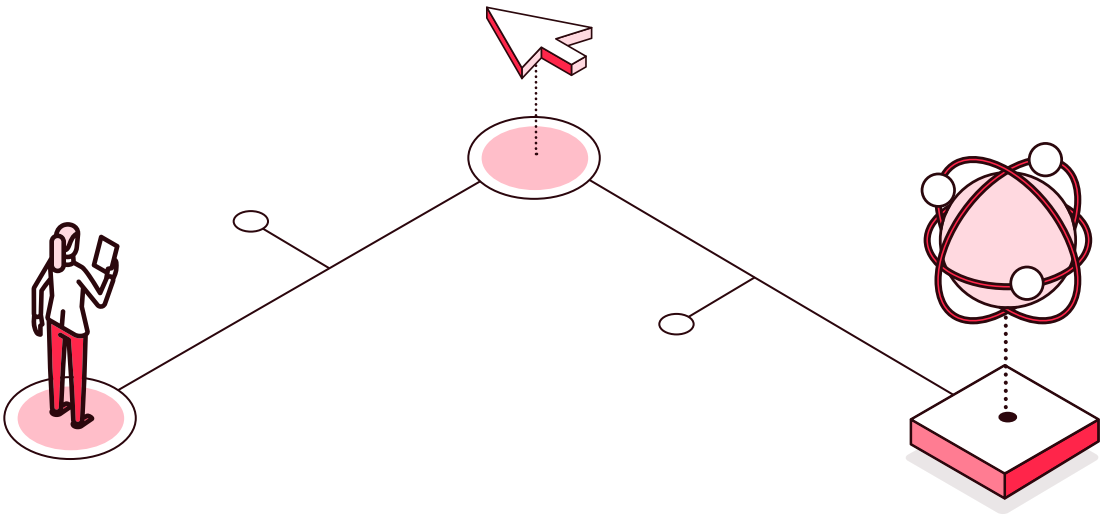
- Is the obligation of the public administration to respond within a fixed period of time to a citizen consultation regulated?

- Is there an agency with a legal mandate to enforce transparency and citizen participation legislation?
- Is there a transparency portal?
- Is the transparency portal among the top ten most visited government websites?
- Do citizens and the press routinely use it for requests for access to public information?
  - Are there any regulations regarding data openness? Do such regulations exist at the following levels:
    - Law?
    - Regulations?
    - Operational guide?
- Does legislation require the existence of a central open data portal?
- Is there an agency with a legal mandate to enforce open data legislation?
- Is statistical information on the implementation of open data legislation published?



2.3

Accessibility and usability



Digital transformation, more than a simple technological implementation, should be seen as a social reinvention and a cultural change that affects the procedures, uses, and customs of people and organizations, both public and private. In this sense, digital transformation is more an adaptation to the new times, necessary for social survival.

In such a scenario, one of the principles of good governance is that all citizens should enjoy the same rights and opportunities. This means that more and more regulations are being introduced to ensure that people with disabilities do not miss out on opportunities because of their condition. Accessibility regulations, which a few years ago acquired the seal of indispensable requirement at international level in all areas of public administration and in some private spheres, have become a technological priority and a new opportunity to bring citizens closer to information systems. But how can this be done?

USABILITY

Although accessibility is more associated with disability and the right to access services in the same way as other citizens, usability should be a priority for any information system. It is common for these systems to be complex and often require significant computer skills to be able to interact with them. In addition, public systems often overuse unfriendly language that makes it difficult or limits the completion of certain procedures.

All these barriers can be reduced, diminished, or eliminated thanks to a good usability that seeks to:

- create simple flows and processes to achieve efficiency.
- in a few steps, to achieve efficiency.

- with a close and understandable language to improve the usability of the language.

- or according to the standard models to which citizens are accustomed in the private sphere to achieve a satisfactory overall experience.

During the conceptualization of each system or the software production process, it is necessary to identify points of contact to work, for example with "cocreation" methodologies. In this way it would be possible to devise and conceptualize more usable solutions, the result of which will be part of the design for its subsequent construction.

In the case of accessibility, these needs are increased by having the dual objective that usability must be made for all citizens, regardless of their condition, place, or their disability. In this sense, it should be noted that accessibility, although it refers more strongly to people with visual, hearing or cognitive disabilities, has a much broader spectrum, since it also refers to being able to access an electronic transaction from a mobile device or, for example, to access certain information from a place with limited technological capabilities or resources.

If attention is focused on the day-to-day work of public administrations, it should be taken into account that information systems are usually created by IT personnel to meet the needs of an institution's functional manager. It is obvious that citizens may have neither administrative nor computer skills, creating a digital gap that in certain procedures becomes insurmountable. This generates a problem of understanding or relating to the system, either due to a lack of technical knowledge, a lack of understanding of administrative language, or both. Given the tendency of computer scientists to presuppose technical knowledge and skills that are not general, and the distance of administrative language from the usual language of citizens, regulation is often needed to ensure that information systems are understandable and usable.

In this order of ideas, the social and private mirror that surrounds us may be the key to understanding how the citizen's logic works when it comes to searching and making decisions in the digital sphere. It could be said that a procedure for applying for a benefit should be no different from the process followed to make an appointment at a beauty salon or buy any product online. This is where the usability of countries should be heading: toward stable, well-known, and generally internalized models.

ELECTRONIC PROCESSING

Similarly, the advantage of electronic processing must be addressed among citizens with disabilities, among the elderly, or in environments with low lighting, noise, or low bandwidth quality, among others. Accessibility, in this sense, must take into account a complex network of mechanisms that allow access to these procedures under a spectrum of very different conditions. Thus, a person with visual impairment should be able to access information in the same way as someone with mobility problems or someone in a rural area with limited network access.

FUNDAMENTAL RULES FOR CREATING INFORMATION SYSTEMS WITH GOOD ACCESSIBILITY AND USABILITY

- **The procedures should be like those of everyday life:** That is, search as in a blog, carry out procedures as in an e-commerce purchase, read as in a newspaper. The key is in all those processes that are done very often in environments that are not always public, but that have standardized processes and customs in the digital society.

- **Simplicity is the best way to orient yourself:** In large systems with a very high volume of information, you should try to structure the content as little as possible. This is the only way for citizens to find what they are looking for. Design also helps here, with simple color systems that allow visualization in all environments.

- **Usable transparency:** Citizens want to solve a problem; they do not know what or who is responsible for solving it. Therefore, we should avoid transferring the internal structure of a state to the processes to be carried out by the citizen.

- **Use of noninvasive technologies:** These help build trust and reduce overloads or unnecessary additional downloads. There are technologies, such as AJAX, JavaScript, and others that allow loading time to be reduced in certain situations.

- **Access from all types of devices:** Although the use of cell phones is already widespread and standardized, there is still a tendency to think that they are only used for certain operations, when the reality is quite the opposite. Citizens should be able to do the same things from their computers and from their cell phones; therefore, we must work on creating portals and applications for all screen sizes from the beginning and as a priority.

- **What is not seen is the most important part of a portal:** The correct use of tags and titles will allow, in cases where internet access is limited or the person has visual impairments, to see and read (or be read to) the information. This is one of the most important standards of the famous AA, but one that must never be forgotten to ensure that we reach 100 percent of citizens.

- **Usability and accessibility** should be part of the productive process of software construction, and experts should be incorporated in the initial stages, as is done, for example, with security issues, or change management, or software quality.

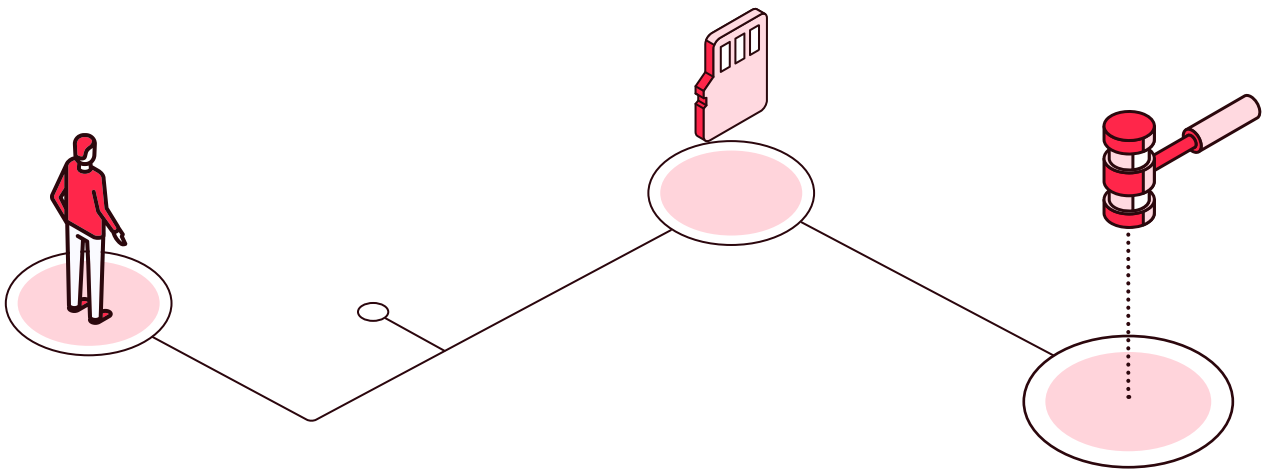
In conclusion, digital transformation, no longer as a reality but as a necessity in itself, needs certain levers that help the process to be carried out effectively, naturalized and in line with the current times. This transformation cannot take place without the needs, demands, desires, and limitations of citizens being met. Consequently, usability and accessibility must go hand in hand when addressing the digital transformation, as one without the other will not be able to keep up with the pace of change that countries are facing on a daily basis.

REGULATORY ADJUSTMENTS

It is necessary to work hard, and with consensus among the different states, on the creation of a regulatory framework that establishes the mandatory nature of certain standards or levels of accessibility for public or even private information systems. It is useful to create observatories or bodies to monitor compliance with accessibility regulations, since compliance is usually low when such bodies do not exist. The observatories can make use of tools that automatically or semiautomatically check the status of compliance with international accessibility standards in the country's different information systems.

On the other hand, the scope of regulation can be broadened to not only aim at making information systems accessible to users with disabilities, but also to ensure their user friendliness for both disabled and nondisabled users. Some useful steps in this regard are the following:

- Control the number of steps to be taken to reach certain information.
- Ensure clear and understandable language.
- Avoid technical IT features that impede the effective use of information systems.



SOME ACCESSIBILITY REFERENCES

Given that *accessibility* is directly related to the equal rights of citizens to have the same opportunities in the web or digital environment with respect to public services, it is absolutely necessary to prevent each agency from making its own interpretation. To this end, the technical criteria for application must be unified, and criteria and periodic reviews must be imposed in order to ensure compliance with the regulations on the subject. For this reason, accessibility is widely addressed at both the international and national levels, which has given rise to standards and norms that allow certification to be obtained.

In terms of international standards, the *Web Content Accessibility Guidelines (WCAG)* 2.1 of the *World Wide Web Consortium (W3C)* stand out. This is the latest version of the web content accessibility guidelines:

- **Principles:** These are the fundamentals of web accessibility:
  - perceptible
  - operable
  - understandable
  - robust
- **Guidelines:** Each principle has its own guidelines. The twelve guidelines provide the basic objectives to be achieved in order to create more effective content.

WCAG 2.1 (OR ITS PREDECESSORS) IS A MAJOR INTERNATIONAL EFFORT TO ESTABLISH AN ACCESSIBLE DESIGN STANDARD AND PROVIDE GUIDANCE ON WEB ACCESSIBILITY.

In terms of regulations, for example, in the European Union there is *Directive (EU) 2016/2102* on the accessibility of websites and mobile applications of public sector bodies, which establishes a set of principles and techniques to be respected when designing, building, maintaining, and updating websites and mobile applications to make them more accessible to users, particularly people with disabilities (aligned with the guidelines established in WCAG 2.1). This directive reveals the importance and transcendence of accessibility, coming from the European Commission itself. Thus, although

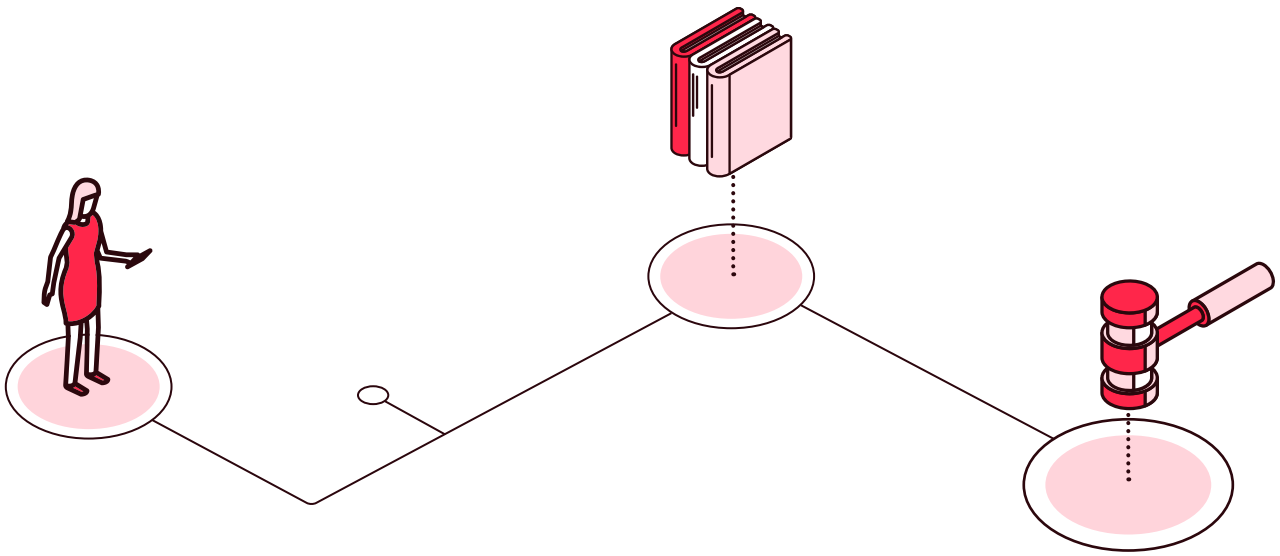
compliance and implementation is the responsibility of each country, guidelines are established, and compliance and verification requirements are imposed in the public sector.

In order to establish the technical applicability of the aforementioned directive, the commission has stipulated two implementing decisions:

- **Implementing Decision EU 2018/2048** on the harmonized standard applicable to websites and mobile applications to ensure accessibility requirements, establishing the European Standard EN 301 549 Accessibility for ICT products and services. This standard is intended to assist both developers and evaluators in accessibility.

- **Implementing Decision EU 2018/1524,** which establishes a methodology for monitoring accessibility requirements, a model accessibility statement and reporting guidelines for member states.

Once this stage of regulation and technical practicality has been reached, each EU country has transposed the directive according to its legislation, normally through the development of a royal decree (or higher-ranking regulation) that establishes the accessibility requirements indicated in *European Standard EN 301 549*. In order to verify and establish a level of compliance with the standard, Annex A lists all the requirements that must be met, equivalent to meeting all the level A and AA requirements of WCAG 2.1 plus a series of specific requirements for special cases.



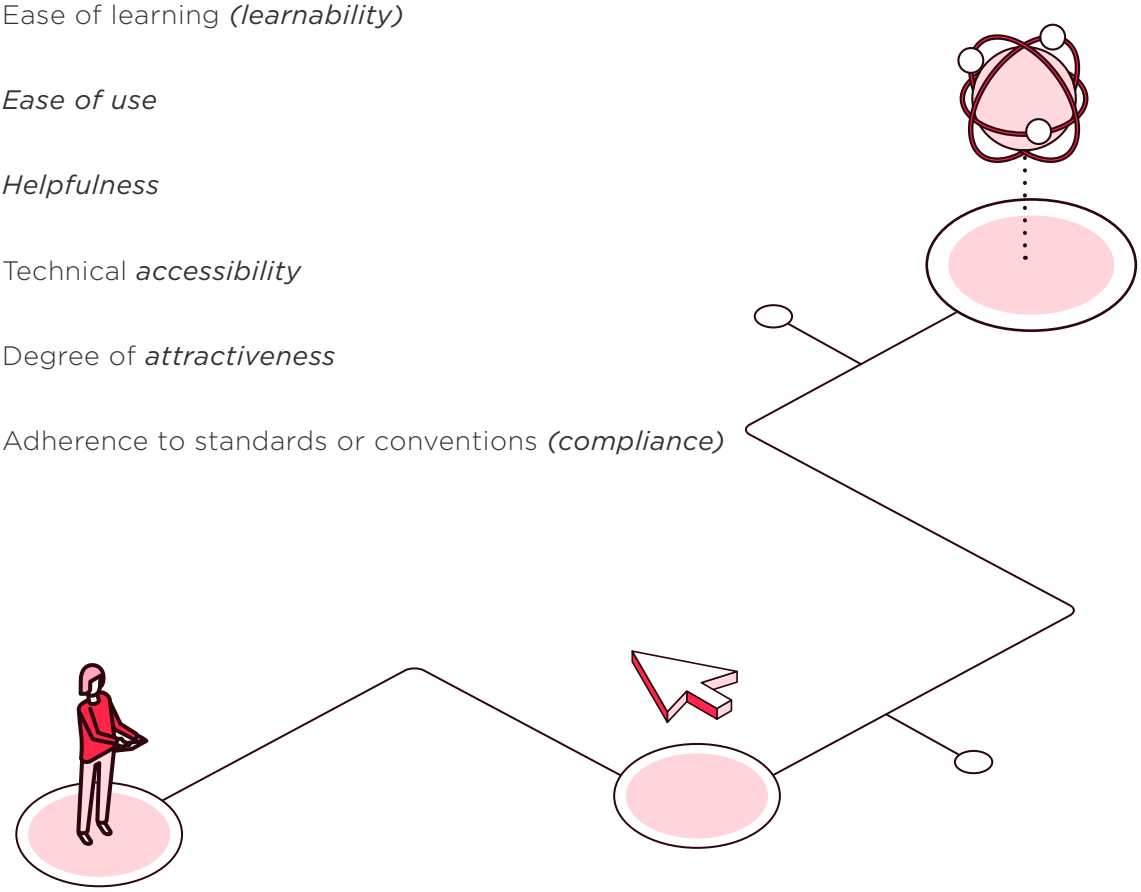
SOME USABILITY REFERENCES

Since usability does not have such direct implications on citizens' rights, there is not such a well-developed set of regulations regarding usability. However, there are different international norms or standards that establish, rather than requirements for implementation, mechanisms or methods for evaluating usability.

ISO 25000, known as SQuaRE *(Software Quality Requirement Evaluation)*, is a unification and revision of the *ISO/IEC 9126* (Software Product Quality) and *ISO/IEC 14598* (Software Product Evaluation) standards. Its main objective is to guide the development of software products with the specification and evaluation of quality requirements.

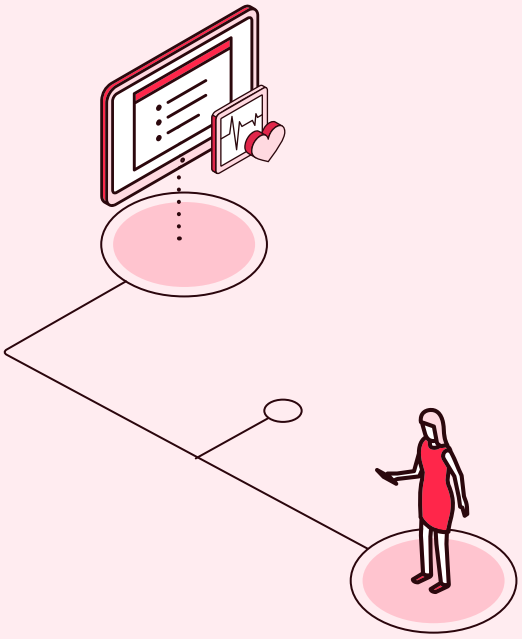
SQuaRE proposes that the usability of a software product can be decomposed into the following characteristics:

- Ease of understanding *(appropriateness, recognizability)*
- Ease of learning *(learnability)*
- *Ease of use*
- *Helpfulness*
- Technical *accessibility*
- Degree of *attractiveness*
- Adherence to standards or conventions *(compliance)*



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

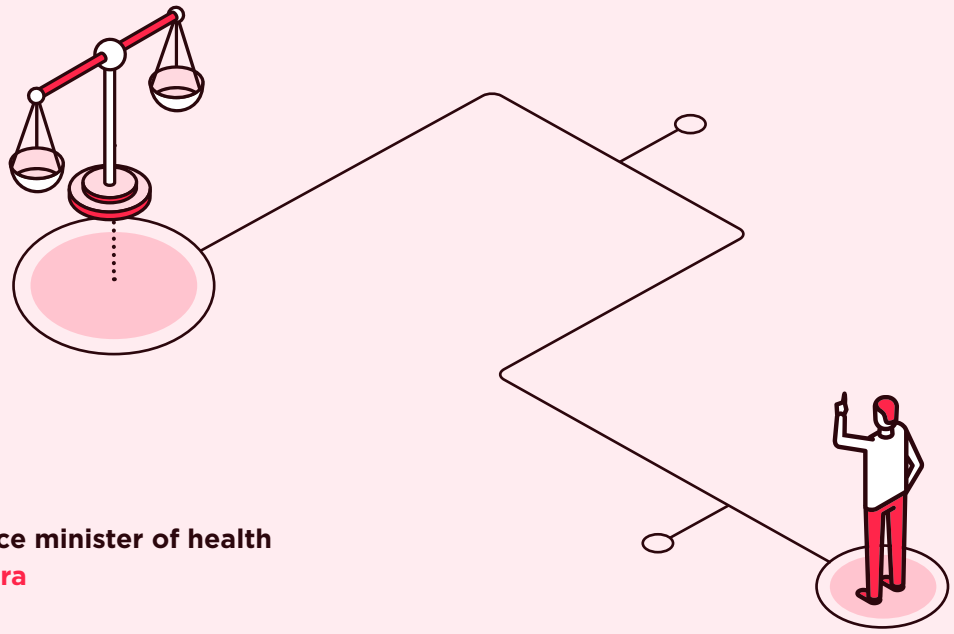


Citizen
Camilo

Every time he has to carry out a procedure with a public entity, Camilo tries to do it electronically, but many times he encounters complex systems that he does not understand and ends up going to the office of his municipality or the entity where he has to carry out the procedure. When he tries to do a procedure that he did last year in person, he realizes that the web page is now very simple and easy to navigate; in addition, he understands the texts, which until now had been written in a language that was really complicated to understand. Thanks to these improvements, he has been able to do the procedure from home, without having to go to any office.

Entrepreneur
Ana

Ana has an ever-growing process of hiring permanent staff to help in her company's tasks. She has a particularly interesting candidate with a strong visual impairment, but she is afraid that she will not be able to help in the procedures her company has to carry out with the public administration, which are mostly done through the internet. In the last interview, she tests to see how the candidate works in real time with the web pages and is pleasantly surprised to find that, since the pages are adapted for people with disabilities, she can carry out the formalities just like anyone else. Ana is happy not only because they have no problem hiring her and offering her a job, but also because she was the best candidate of all those who had applied.



Vice minister of health
Sara

Sara has received a complaint from her country's association of people with disabilities that her ministry's web pages are not adapted and therefore cannot be used by people with disabilities. He finds this particularly serious, not only in his ministry but in the government in general, so together with the Ministry of ICT, he promotes an accessibility policy for government pages, so that all of them meet international standards. He is also creating an observatory to ensure that citizens will never again be limited in their rights by something that has been technically resolved.

Mayor's advisor
Daniel

Daniel is concerned about the gap that exists in the case of some of his citizens, especially the educational and age gap, since in his municipality there are very old people and people with low educational levels. He wants the digital transformation to benefit all citizens equally and for no one to be disadvantaged. Therefore, in order not to leave out the citizens who need it most, he proposes to the mayor a plan to change the web pages and applications, making them simpler and more accessible, with a clear and natural language.

EXAMPLES

Click on each flag or icon to go deeper

Spain
Royal Decree on accessibility of websites and applications for mobile devices of the public sector.

Republic of Korea
Legislation

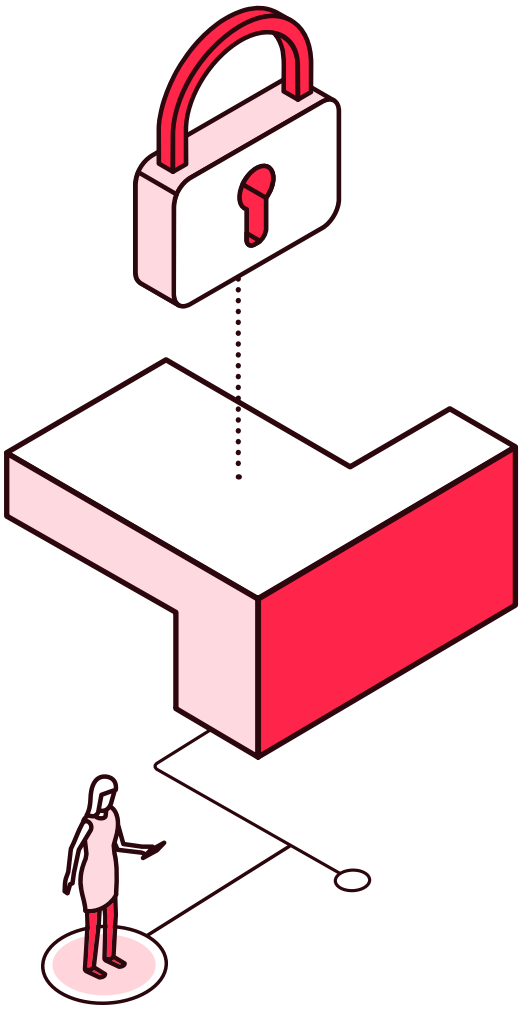
W3C Web Accesibility Initiative
Guidelines and other standards related to web accessibility

United Kingdom
Understanding accessibility requirements for public sector bodies

INDICATORS

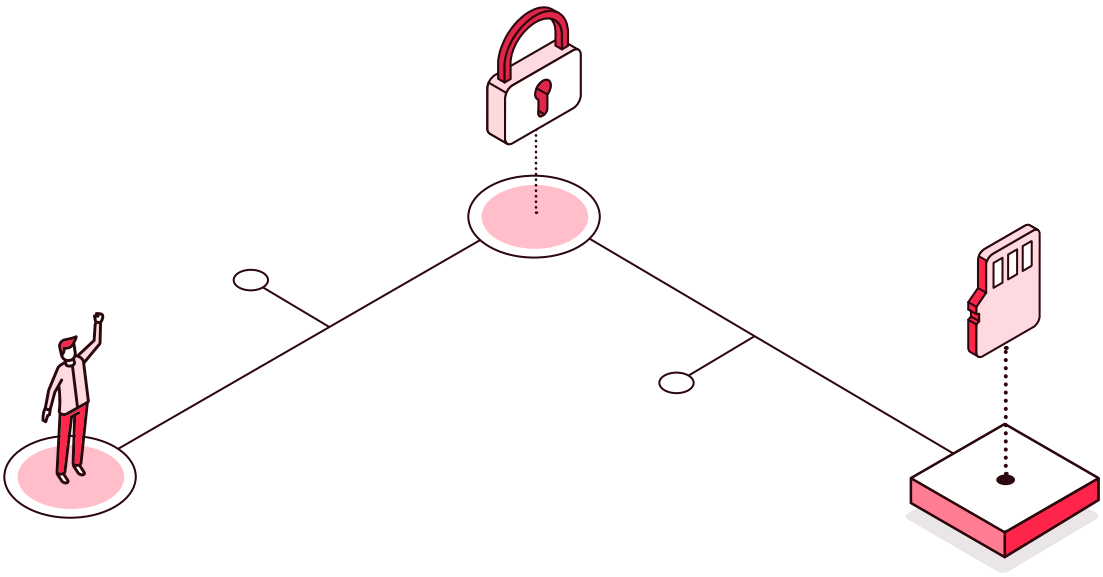
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there regulations associated with digital media accessibility? If so:
  - Does this regulation include usability criteria?
  - Do the regulations also include criteria of comprehensiveness and inclusion (i.e., not only technical accessibility)?
  - Is such accessibility standardized internationally?
- Is there an accessibility observatory?



2.4

Data protection



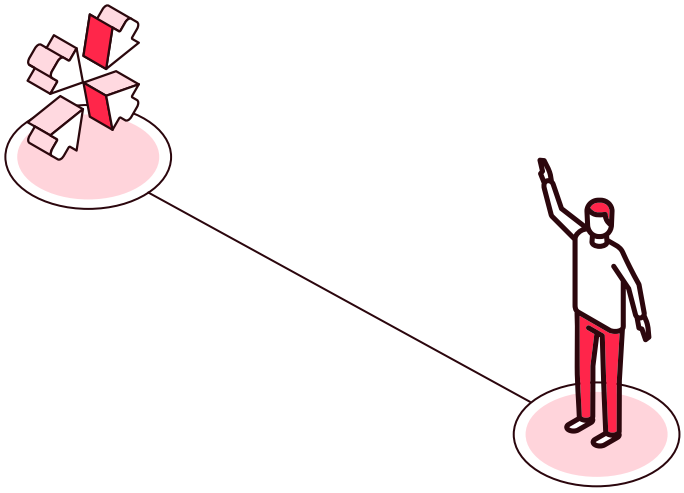
The development of the information society has led to the majority of personal data processing being carried out in the cyberspace. The advent of new technologies, in addition to important advantages for the citizen, has led to an increase in risks with respect to some of the most essential rights, such as the right to privacy or intimacy, which has triggered the need for rules that specifically regulate the processing of personal information of individuals.

THE CURRENT INFORMATION SCENARIO

Data has become a resource base for a country's growth, job creation, and social progress. Data analytics, in particular, facilitates the optimization of processes and decisions, as well as innovation and the prediction of future events, which can help to decongest many of the lengthy bureaucratic processes suffered by public administration.

This global trend has enormous potential in a number of fields:

- health
- environment
- food safety
- weather
- resource efficiency
- energy
- intelligent transportation systems
- smart cities



The data economy is characterized by an ecosystem in which different types of market players—such as manufacturers, researchers, and infrastructure providers—collaborate to ensure that data is accessible and usable for public administrations and other players. These administrations, in particular, play a key role in promoting the reuse of information and data, as intelligent information processing is increasingly required to enable agile and informed decision-making, allowing efficient management of public resources and better adaptation to the needs and demands of users. In this paradigm shift toward a "citizen-centered" administration, the reuse of information and data plays a role of capital importance as in no other previous technological evolution.

E-government is also bringing a country's procedures (administrative, economic, judicial, etc.) closer and closer to its citizens. However, this progress would be unthinkable without the development of systems and applications that make possible, in a good number of countries, the creation of the electronic file linked to a digital ecosystem that makes it possible to speak of native electronic information. This language is made possible by factors made possible by new technologies, such as

- integration with electronic signature systems.
- storage by means of electronic archives.
- the possibility of carrying out telematic notifications and communications.
- communication with other public administrations within or outside the country of origin of the information processing.

Therefore, the use of information services by these administrations, adapting public services to what society and the economy demand today, in a balanced way, is to speak of efficiency in public management and decision-making, based on evidence that allows achieving a responsible use of technology.

PROTECTING PEOPLE MEANS PROTECTING THEIR DATA

The use of the aforementioned new technologies and the need to promote the reuse of information must not lose sight of the protection and privacy of individuals. This implies always respecting the basic rights related not only to the protection of personal data, but also to intellectual or industrial property. Thus, the progress in terms of digital transformation of many public administrations regarding the opening of data to gain in terms of efficiency, time, and cost savings, etc., must in turn respond to an appropriate balance in the protection of these rights.

The digital transformation driven by data not only penetrates into a change of mentality when dealing with daily operations, but also in the social strata of any country, such as the economy, education, healthcare, justice, etc. This makes palpable the increase of larger volumes of data generated by machines or processes based on emerging technologies such as the Internet of Things (IoT).

It can be argued then that globalization and rapid technological developments have posed new challenges on this front, as the scale of personal data collection and sharing has increased significantly in recent years. Technology allows public authorities to use personal data on an unprecedented scale when carrying out their activities and processes, which makes it necessary for states to increasingly facilitate the free flow of personal data through transfer to third countries and within the framework of cooperation between different public authorities, ensuring a high level of protection of personal data.

However, the development of autonomous connected systems means that we are not in an era of change, but in the midst of the changing of an era. To take advantage of these opportunities, a careful assessment is therefore required to ensure a more robust and consistent framework for data protection, especially personal data, backed by strict enforcement, given the importance of building trust in a digital economy that is likely to develop in any country's internal market.

This regulatory framework ensures that the new challenges that arise in relation to data processing do not have a negative impact on the privacy and protection of individuals. In addition, it can be understood as a strategic aspect for a country in its international relations, since those nations that do not protect this asset with an adequate level will hinder public administrations, as well as their economic agents, in their international relations with third parties.

THE DEGREE OF PROTECTION GRANTED IN EACH COUNTRY WILL DEFINE THE LEVEL OF COMMITMENT ACQUIRED FOR THE PROTECTION OF PRIVACY AND THE PROTECTION OF REFERRALS WITH RESPECT TO THEIR INDIVIDUALS.

In summary, the protection of natural persons, in relation to the processing of personal data, is an important right that makes it necessary to establish a control system through mechanisms that prevent the improper manipulation of such information. This right is not absolute, but must be taken into account in accordance with its function in society and must be balanced with other fundamental rights, in accordance with the principle of proportionality.

RISKS OF MISUSE OF PERSONAL DATA

LEGISLATIVE MILESTONE

The Judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, of July 23, 2020, invalidated the EU-US Privacy Shield Decision on the grounds that US domestic law requirements, and in particular certain programs allowing public authorities in the US to access personal data transferred from the EU to the US for national security purposes, impose a burden on the US public authorities to access personal data transferred to the US for national security purposes. It was held that the requirements of US domestic law, and in particular certain programs that allow US public authorities to access personal data transferred from the EU to the US for national security purposes, impose limitations on the protection of personal data that are not circumscribed in a way that provides substantially equivalent guarantees to those required under European law. It was also pointed out that this legislation does not provide any judicial remedy against the US authorities for data subjects. This fact has led to the paralysis of countless businesses and relationships between European and American agents until international data transfers are readjusted to other mechanisms that guarantee security and compliance with the applicable regulations.

Individuals should have control over their own personal data, as they are the owners of such data. Furthermore, they should be in charge of deciding on their purpose and destination, in compliance with the regulations applicable in each country. To this end, it will be necessary to reinforce legal certainty and safeguards in the actions of economic operators, as well as to guarantee adequate processing in the actions of public administrations or third parties subject to data processing.

In this regard, it is worth mentioning the main risks that the misuse of personal data may entail for the rights and freedoms of citizens, with the consequent physical, material, or immaterial damages:

1. Problems of discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social damage.

2. Depriving citizens of their rights and freedoms or preventing them from exercising control over their personal data.

3. Disclosure of ethnic or racial origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or sex life, or criminal convictions and offenses or related security measures.

4. Evaluation of personal aspects, in particular the analysis or prediction of aspects related to work performance, economic situation, health, personal preferences,interests, reliability, behavior, current situation, or movements, in order to create or use personal profiles.

5. Processing of personal data of vulnerable persons, in particular children.

6. Processing involving a large amount of personal data and affecting a large number of data subjects.

In general, before undertaking a digital transformation process, it is essential to have a regulation that protects citizens from the interference, in their right to data protection, involved in the use and abuse of this information. However, the use of new technologies detracts a high impact for the individual according to the risks listed above; therefore, it is essential to:

- Create a regulatory framework to prevent the misuse of data, whether in the public or private sector.

- Guarantee the citizen's control over his own data, as well as the possibility of exercising certain rights that confirm this control, such as the rights of access, rectification, deletion, portability, limitation, and opposition.

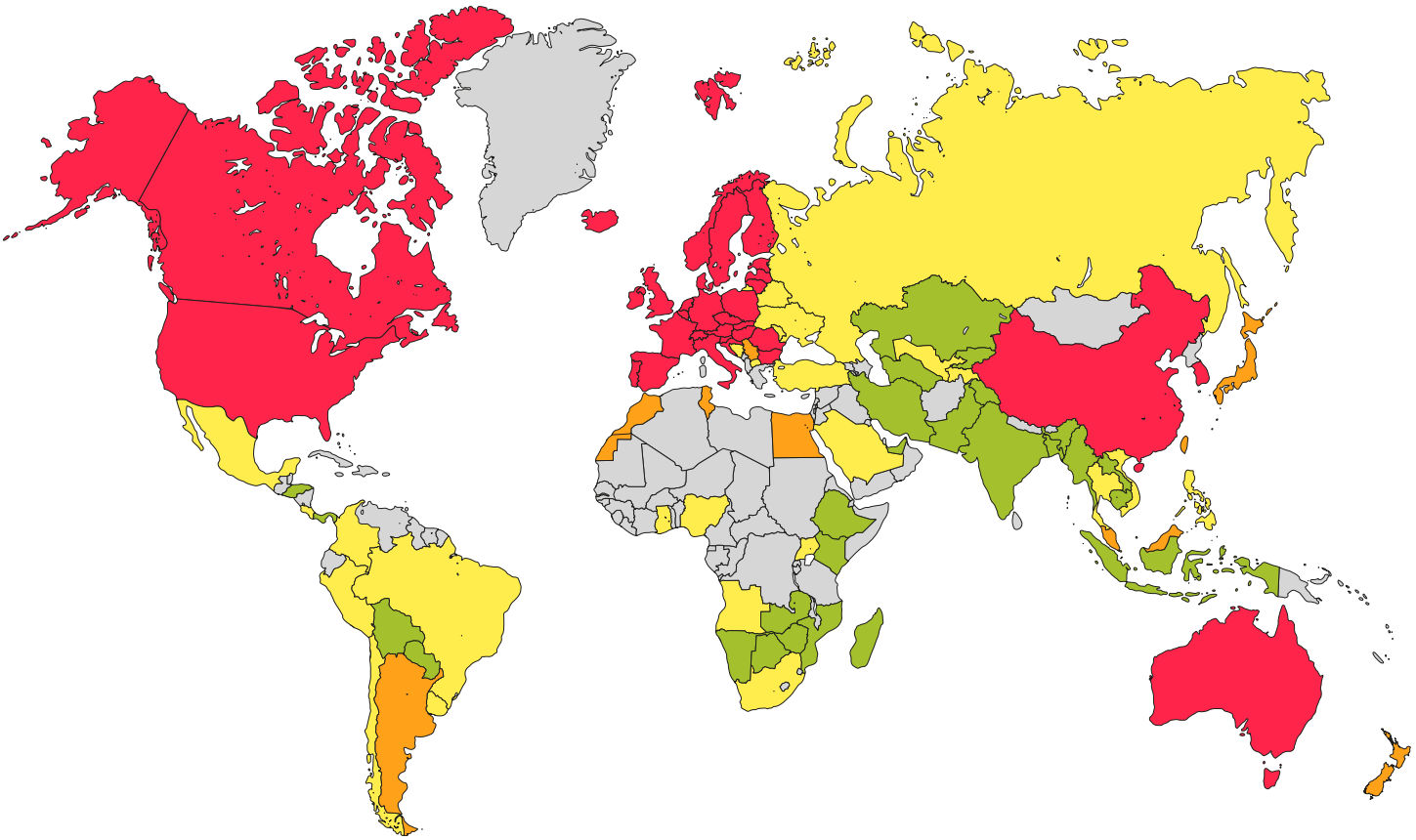
- Guarantee the possibility of filing a legal claim in case of violation of these rights.

- Prevent personal data from being subject to automated decisions.

DATA PROTECTION IN THE WORLD

As mentioned above, the importance of data protection in the digital environment is a relevant issue in the information society. Consequently, it is treated with special attention in the vast majority of countries and, therefore, there is some international standardization. The following image shows the level of protection afforded to data protection at the international level:

Illustration 1. Data protection laws around the world.



Regulation and enforcement

© 2021 DLA Piper

Heavy | Robust | Moderate | Limited

Among the national and international regulations on data protection, the European General Data Protection Regulation (GDPR), which affects all European countries equally, as well as third countries outside the European framework when they are subject to the processing of personal data from the countries of that continent, stands out in particular. This reference makes it necessary to reflect on the importance of proposing a regulation, by country, that is adapted to the principles established therein. For the countries of Latin America and the Caribbean, the Ibero-American Standards for the protection of personal data are a reference. Although several countries in the region have adopted personal data protection laws, the topics included in these laws vary, as well as the level of coincidence with the Ibero-American Standards. The portal "Datos personales y sus leyes," maintained by the IDB (2022), performs this comparative analysis among the twelve LAC countries that have personal data protection laws in force[23].

ASPECTS THAT SHOULD BE TAKEN INTO ACCOUNT IN ANY COUNTRY'S DATA PROTECTION REGULATIONS

1. The design of personal data protection in some legal systems revolves around the notion of "risk" to the rights and freedoms of individuals. The focus is not on threats to the organization, but on threats to the rights and freedoms of citizens. Therefore, the regulation requires a risk analysis to be carried out, both in the systems and applications developed by public administrations and by third parties, with the aim of establishing security and control measures to guarantee the rights and freedoms of individuals. The regulations must change in their traditional confection, in particular in the security measures for the protection of personal data, moving from a static model to a more dynamic one focused on the continuous management of the risks associated with the processing from its design. To this end, it is necessary to observe the legal framework in force in each country, applicable to both public administrations and the private sector.

2. The establishment of control and supervisory authorities for the correct application of legal provisions. It is essential to create a data protection unit or agency with executive, regulatory, inspection, and, most importantly, sanctioning capacities to effectively enforce personal data protection regulations. It is preferable for this unit to be independent and not dependent on the government, since it should have sufficient autonomy to control and, if necessary, be free to impose sanctions without worrying about power relations or dependence.

23. IDB, Personal Data and Its Laws, 2022, https://www.datasketch.co/bid/datos-personales-y-leyes/.

3. Establish accountability as the backbone of the protection system. The aim is to establish a principle requiring the implementation of appropriate technical and organizational measures to ensure and demonstrate that processing is compliant with the regulations. In practical terms, this principle requires organizations to analyze what data they process, for what purposes, and what kind of processing operations they carry out. Based on this knowledge, they must explicitly determine how they will implement the measures provided for in the GDPR, ensuring that these measures are adequate to comply with the GDPR and that they can demonstrate this to the public and to the supervisory authorities. In short, this principle requires a conscious, diligent, and proactive attitude on the part of organizations with regard to all the processing of personal data that they carry out.

4. The development of rules to ensure that all data processing needs to be supported by a basis that legitimizes it, be it consent, the contractual relationship, a legal obligation, the vital interests of the data subject or third parties, the public interest or exercise of public powers, or the legitimate interests of the entity processing the data. In this connection, it will be necessary to determine specific rules for the communication of data between organizations, whether public or private. It is also important to regulate that a data that has been transferred for a specific purpose by citizens should not be used for other purposes, which is known as the purpose limitation principle.

5. Specific rules to protect, in particular, sensitive personal data, determining what is understood as such. In other jurisdictions these data are health, biometric, sexual, political or religious orientation, or similar. The rules for the control of these data must be stricter, since when this information of citizens is known, the consequences of its abuse can be very significant.

6. Regulation of the rights of citizens to have access to data held by public administrations or third parties, in order to rectify them if they are incorrect or delete them, limit their processing, object to receiving commercial communications, forward the data to another entity, or refuse automated individual decisions. These rights must be able to be exercised effectively and free of charge by citizens, although they are not absolute but may be limited by certain related obligations, for example, within the framework of public administrations, which process data to safeguard: state security, defense and public safety, prevention, investigation and detection of criminal offenses, general public interest, judicial independence, and protection of the data subject or the rights and freedoms of others, among others.

7. Contemplate the regulation of the structure and digital governance in data protection, defining the roles and responsibilities of data managers in each institution, so that protection is effective and that those ultimately responsible are well defined if a problem arises with the management of personal data or in meeting the demands of citizens.

8. Establish adequate security conditions in information systems that manage personal data. This is especially important to avoid data security incidents, leaks, or unwanted uses. Ideally, this regulation should be aligned with the cybersecurity regulations of each country in order to achieve effective protection of personal data. The obligation to notify of data security breaches, publicly reporting statistics on the state of security with respect to data processing in the country, is also relevant for the knowledge of how a country and its agents are evolving with respect to data protection.

9. Finally, it should be easy for the citizen and the supervisory authorities to know how data is used by the public administrations of each country, or by third parties that process personal data. Control by the citizen necessarily involves providing information on the conditions of the processing operations that affect them as well as on the responses to the exercise of their rights. To this end, the information obligations (what data is stored, how long, how it is managed, how to exercise rights over this data, etc.) must be provided in a concise, transparent, intelligible, and easily accessible form, with clear and simple language. Similarly, if there are interoperability platforms within the framework of public administrations that exchange personal data among themselves or with third bodies, it is important for the citizen to know in a clear and simple manner what personal data of theirs is being exchanged, for example, in the processing of electronic files.

Finally, it is essential to put in place an increasingly reinforced system for the protection of data subjects' data in the face of the challenges and risks involved in the use of technology. Among the set of requirements to be imposed on data processing, the following should be highlighted:

- Comply with certain security levels (i.e., implement appropriate technical and organizational measures to prevent any unauthorized interference in data processing operations).

- Ensure the confidentiality, integrity, and availability of the personal information of data subjects in any process that may involve these assets.

STORIES

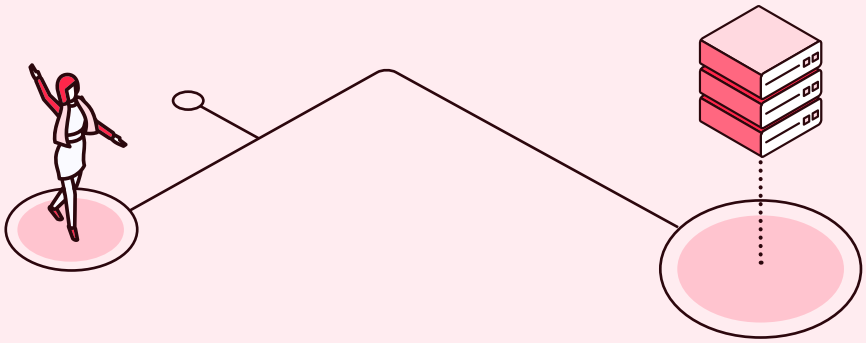
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Citizen
Camilo

Camilo is delighted with digitalization. He likes the fact that public institutions carry out procedures without asking the citizen for data, but he has the feeling that his information travels without his knowledge. He knows that interoperability in his country makes the government more efficient, but he feels that he has lost control of his data. He would like to know what data the state has, access it easily, and be able to easily rectify data that is not correct and assert his rights in court if he has suffered harm or damage as a result.

Entrepreneur
Ana

As a businesswoman, Ana has to comply with the data protection obligations imposed by law, and she is happy to do so. The problem she sees is that all this processing has to be done on paper, and that the information related to it is not available to the citizen. Ana understands that complying with the regulations is important, but she also does it for compliance culture, thus adding value to her client, but she needs this benefit to be known by the citizen. She has the feeling that the data protection law in her country is designed more as a formality in itself than to really protect the rights of citizens.



Vice minister of health
Sara

Sara knows that there is no data more sensitive than health data, so she is taking its protection very seriously. She was horrified when she learned that her IT staff had permissions to access patients' medical records. Similarly, she understands that there is not much control or traceability of who accesses what data, or why. She has therefore implemented a data protection strategy, appointing a data protection officer responsible for the task, and will be employing a privacy management system in his organization.

Mayor's advisor
Daniel

Daniel believes that he has data protection under control within the municipality. Among other things, any access to data in the information systems is logged (who accessed it, for what purpose, and when), and there are courses that warn officials of the penalties (which under the data protection law can lead to imprisonment) in the case of improper access to data. Now that he is satisfied with the situation, he is implementing a citizen information strategy so that citizens can easily access and know what data the municipality has about them, as well as exercise their data protection rights.

EXAMPLES

Click on each flag or icon to go deeper

Red Iberoamericana de Protección de datos

Standards for personal data protection for ibero-american states

Europe

Complete guide to GDPR compliance

Europe

European Data Protection Board

Spain

Spanish Data Protection Agency

Netherlands

Dutch Data Protection Agency

France

French Data Protection Agency

Latin America and the caribbean

Data protection and its laws

Republic of Korea

Data protection legislation

Canada

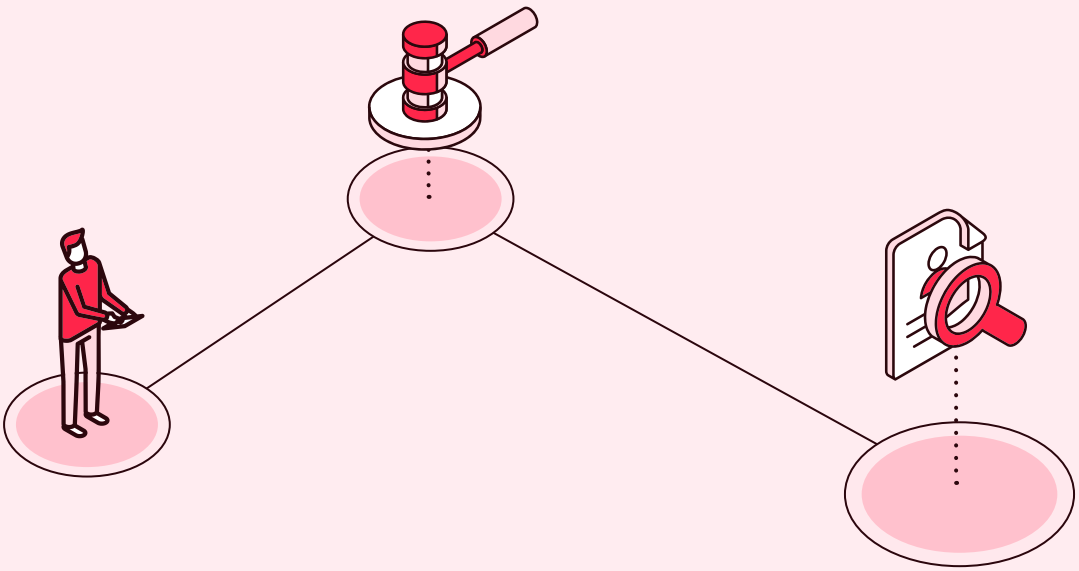
The Personal Information Protection and Electronic Documents Act (PIPEDA) - Office of the Privacy Commissioner of Canada

Argentina

Personal Data Protection Law 25,326

Brazil

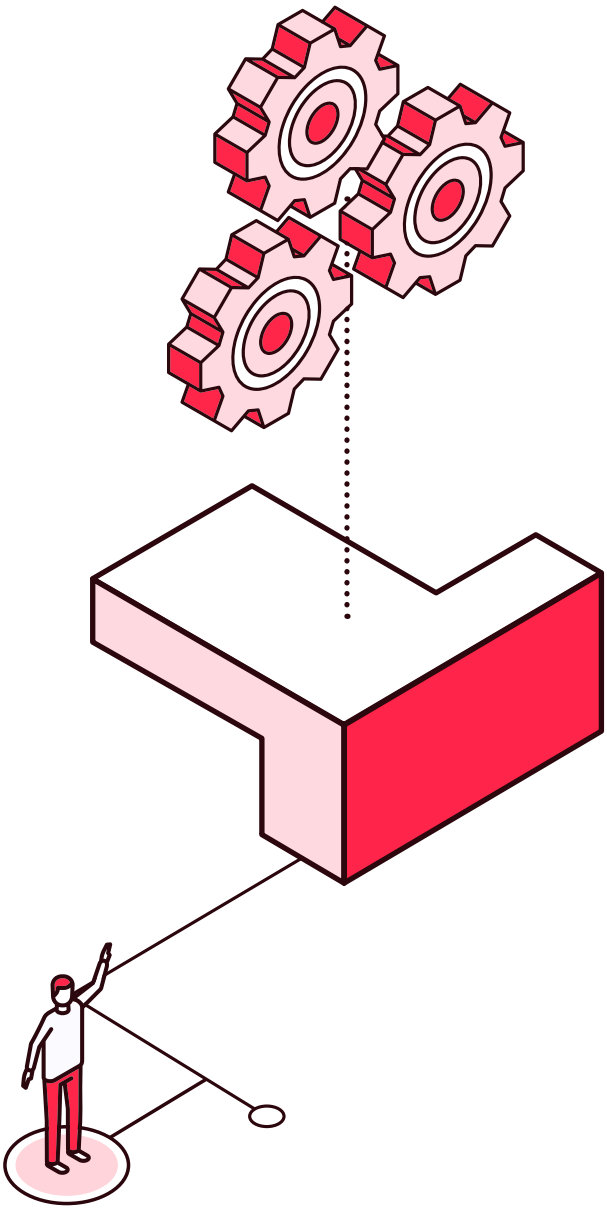
Personal Data Protection Law 13,709



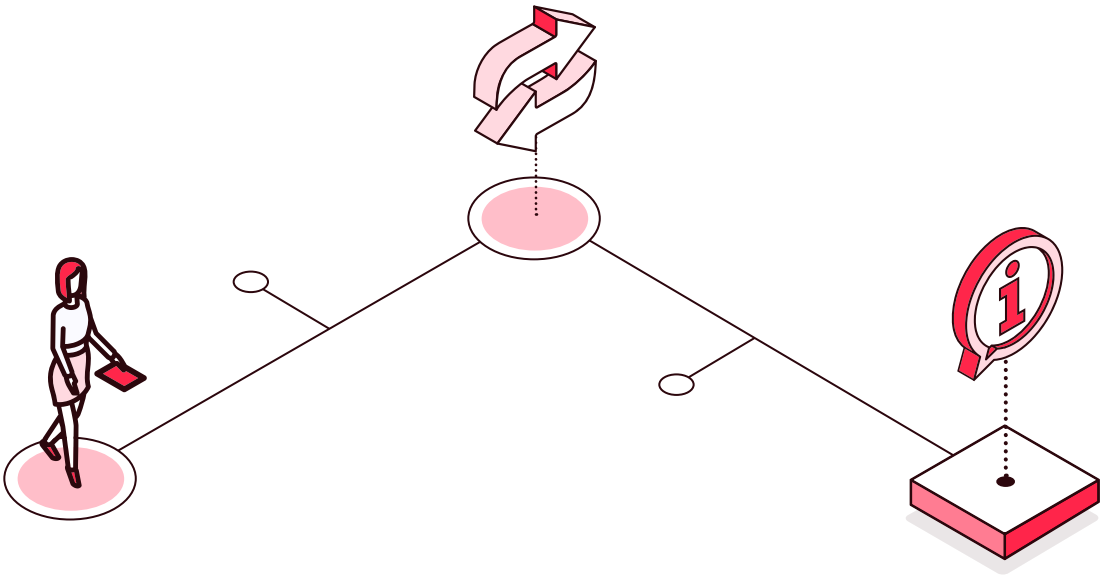
INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there data protection regulations?
- What rank is given to it in the legal system? Do these regulations exist at the following levels:
  - Law?
  - Regulations?
  - Operational guide?
- Is there an independent statutory data protection agency or unit with inspection and sanctioning powers?
- Is the legislation adapted to international (European) standards?
- Are there data protection agreements with other countries to enable transfers of personal data between countries?



2.5 Interoperability



In all areas in which there is a significant component of interrelationships, it is essential to have standards that set out the way in which the different actors involved should proceed in order to ensure that products and services are compatible and can be integrated. Therefore, a regulatory framework for interoperability regulates that the different information systems, from different sectors, or from the same sector but different entities, can exchange information and have compatible operating modes, among all of them, with the private sector and citizens, and with the surrounding countries.

AS A METAPHOR

Cell phones of different brands work in different countries and carriers because they are designed to comply with standards previously agreed upon by industry and governments. When an electrical appliance is plugged in, it is done with the same standardized plug. The way postal addresses are written in the country is standardized so that letters can reach their destination. All this is made possible by standards that are widely accepted

It is widely accepted, and this is reflected in prestigious frameworks such as the European Union's ISA2 (Interoperability Solutions for Public Administrations, Businesses and Citizens) or the EIF (European Interoperability Framework), that interoperability is not limited exclusively to the technological level, contrary to what is unfortunately very widespread. Interoperability must be established at four different levels:

- legal
- organizational
- semantic
- technological

Thus, the end of interoperability is none other than connections between applications, albeit in an automated manner. However, in order to achieve this goal, it is a sine qua non condition that interoperability rules have also been established at the other levels. Therefore, it would not be possible to interconnect two systems without having previously defined the semantic exchange models. Nor would it be possible without the existence of legislation to enable this to be done, or without the two ends of the exchange having agreed to do so.

INFORMATION INTEROPERABILITY

In general, the regulation is associated with the "one-time" principles and data interoperability systems. It should be noted that it is also necessary to regulate the operation of document interoperability, as well as the interoperability of complete electronic files, not only of data and certificates. This regulation can be contemplated within the interoperability section, or within the regulation related to the electronic file, dossier, and document.

Usually, the file, the electronic document, the information systems, and their operation are not standardized in the different countries. This means that each IT project develops its own file model, data, processing methods, etc., which generates a chaos in which not only can these files not be exchanged, but it is not even possible to process them outside the area in which they were created. In fact, there are many cases where simple exchanges of documents or unstructured information are referred to as interoperability. Although, strictly speaking, end A sending a document to end B, and B doing something with it, such as leaving it in a tray, may be called interoperability, this is clearly neither in the spirit of interoperability nor efficient.

Interoperability becomes an extremely powerful element when information is exchanged in a structured way, based on rules established by semantic schemas that describe the information. In such a way, through data nodes and metadata, information systems can be able to process information automatically and, therefore, exponentially increase their efficiency, and bring the capabilities of interoperability to their maximum.

Therefore, a set of rules is needed to standardize technology projects (from the structure of data and metadata to the rules and systems for exchanging them), in the same way that industrial projects are standardized. It should be noted that a precondition for technological standardization is the standardization of the administrative procedure.

HIERARCHIES OF STANDARDS FOR INTEROPERABILITY

Ideally, the regulation will have a legal or equivalent rank, allowing the definition of the basic concepts to establish the general operating framework, without going into technical details of implementation, but only indicating the general provisions. It should be binding and reach all institutions, companies, and citizens.

However, it is advisable not to freeze at a high regulatory level something that will undergo changes as technology and the development of the country's digital transformation progress. Thus, the law should have an abstract character, with a medium-term maintenance vocation, without the need to change, and should provide flexibility to the country's interoperability system. For this reason, it will surely be necessary to have second-level regulations or equivalents to further detail some aspects while maintaining regulatory formality.

Even so, due to the specific nature of the subject matter, its rapid modification due to technological advances and the technical detail required, it is common for both the law and the regulations to provide technical instructions to detail the implementation aspects that will ensure that there really is interoperability between systems. In fact, once interoperability between systems is implemented, the semantic schemes defined, such as the document or electronic file, for example, will undergo continuous changes that will require numerous modifications and adaptations to new needs. Such is the case of the incorporation of a new group into the interoperability ecosystem, which may result in a metadata adopting new values, or the evolution of part of the structure of a schema due to better technical reflections. This makes this normative technical level much more agile when it comes to adopting new versions.

However, it is important to bear in mind that version updates of technical standards must be done in an orderly manner and based on preestablished rules, usually through an interoperability committee. This committee is usually made up of representatives of the stakeholders that make up the interoperability ecosystem and must decide on changes to each standard according to a set of rules, thus ensuring effective version control.

Some building blocks of effective regulation of a national interoperability system include the following:

- Master tables (national data classification agreements, general or sectoral, to enable interoperability).
- Common elements of information systems (e.g., identification and digital signature).
- What is an electronic file and an electronic document.
- How to exchange an electronic document.
- The definitions of the information systems interfaces that allow information to enter and leave them.

IN SOME CASES, THE EXISTENCE OF INTEROPERABILITY STANDARDS PRECEDES THE EXISTENCE OF OTHER STANDARDS AND TOOLS. IN OTHER CASES, IT IS SUBSEQUENT. WHAT IS VERY IMPORTANT IS THAT IT IS COORDINATED AND COHERENT WITH SOME AREAS OF SPECIAL RELATION.

Consider as an example a country's data strategy: interoperability has to facilitate synergies with data policies, so that relationships with automated processing and competitiveness of the country can be exploited (remember that interoperability systems can also facilitate services to the private sector, not only to institutions). Likewise, it must be aligned with semantics and standardized data policy, or open data.

Given the importance of maintaining the privacy of citizens' data, there must be cross-referencing between interoperability, regulation, and the personal data protection strategy. Similarly, in order to facilitate transparency and increase citizen control, it is useful for citizens to be able to see, know, and control, through the citizen folder, the exchanges of citizen data that take place.

The regulation should be established prior to—or in coordination with—the data interoperability platform, as well as interoperability systems for electronic documents and records, if any. Ideally, interoperability should cover these aspects (electronic file and document), so it should also be aligned with the electronic documents and records policy and its associated tools.

IN ADDITION TO HAVING THE TECHNICALLY APPROPRIATE REGULATIONS IN PLACE, IT IS ESSENTIAL THAT THESE REGULATIONS ARE ALIGNED WITH GOVERNANCE SCHEMES AND IMPLEMENTATION CAPABILITIES TO ENSURE THAT THEY CAN BE EFFECTIVELY ENFORCED.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Vice minister of health
Sara

Sara arrived at the Ministry of Health with the idea to stop working on paper and start working digitally. She does not know how to start because in her country there is no common service model on which she can base herself, which defines in a standard way the electronic document, how to sign it, how to save the information, etc. There is a lack of these common guidelines. Sara thinks it is important not only to have a regulation on data interoperability, but also common document and file models, signature compatibility, common metadata, and master tables.

Citizen
Camilo

Camilo has to renew his permit at his municipality every year so that his work as a driver is registered and legal. Just like last year, he goes prepared and brings his set of papers, as well as the tax declaration and the certification that proves he has no criminal record, but when he goes to the office to do the paperwork, he is pleasantly surprised that he does not have to hand them in; the official tells him that, thanks to interoperability, he already consults them at the competent body and includes them in his paperwork. He is happy to know that next year he will not have to obtain and bring all these documents, and that it will be much easier to renew the permit.

Entrepreneur
Ana

Ana leads a large company and is happy that in her country she does not have to deal with the various public institutions on paper. However, she sees room for improvement. The relationship with each of them is different: some operate through a website, others have automated web services, and a third group offers microservices (light web services that allow fast exchanges between machines). He does not understand how they cannot come to an agreement to relate in a single way, through a system that allows them to save costs and function as a single point for companies that, like his, have to relate to multiple public entities. If there were a regulation that contemplated interoperability, not only among public entities, but also between them and the private sector, a company like Ana's could see a significant increase in its competitiveness.

EXAMPLES

Click on each flag or icon to go deeper.

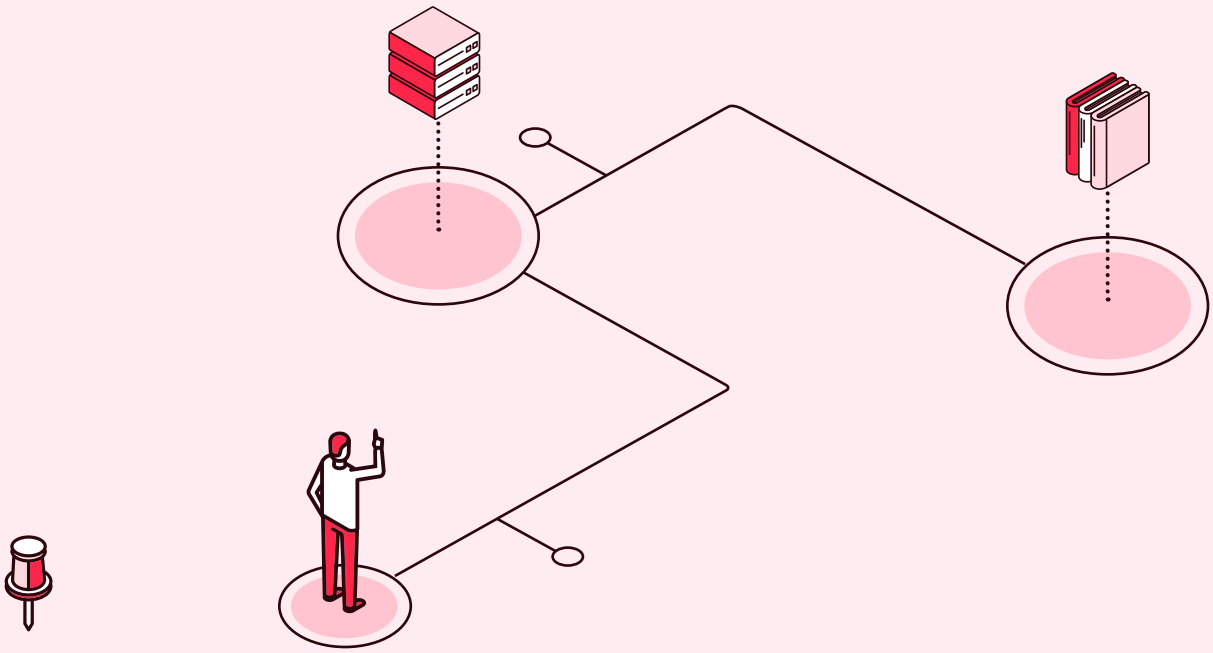
Spain
Technical regulations on interoperability.

Spain
Regulation of interoperability (Law 39/2015, of October 1).

European Commission
European Interoperability Framework

Spain
Regulation of the National Interoperability Scheme (Royal Decree 4/2010, of January 8)

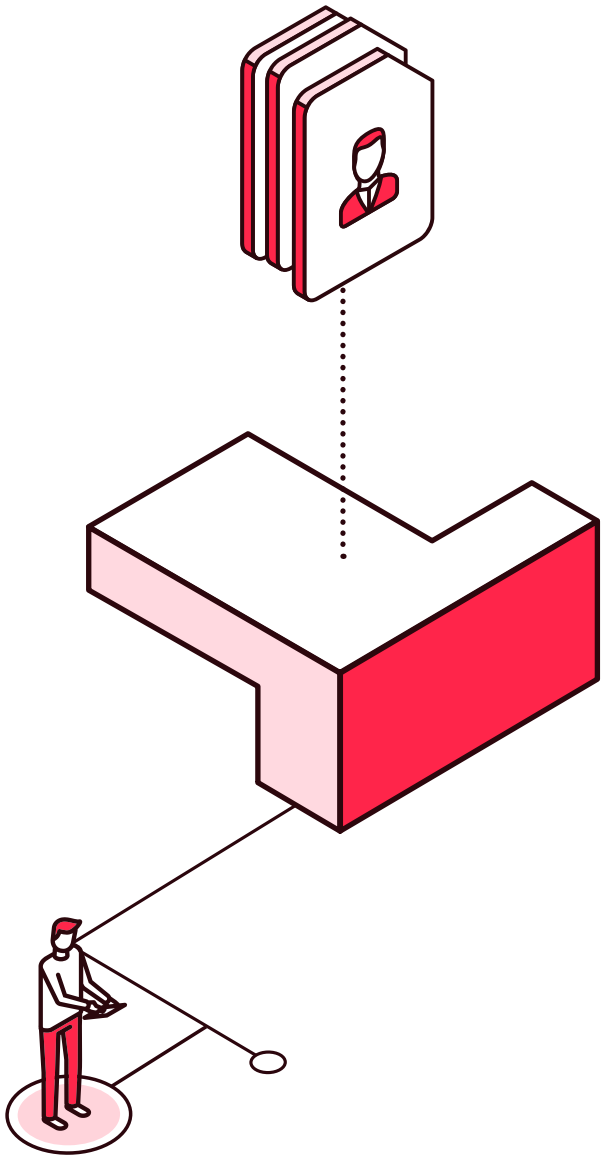
Estonia
Interoperability services



INDICATORS

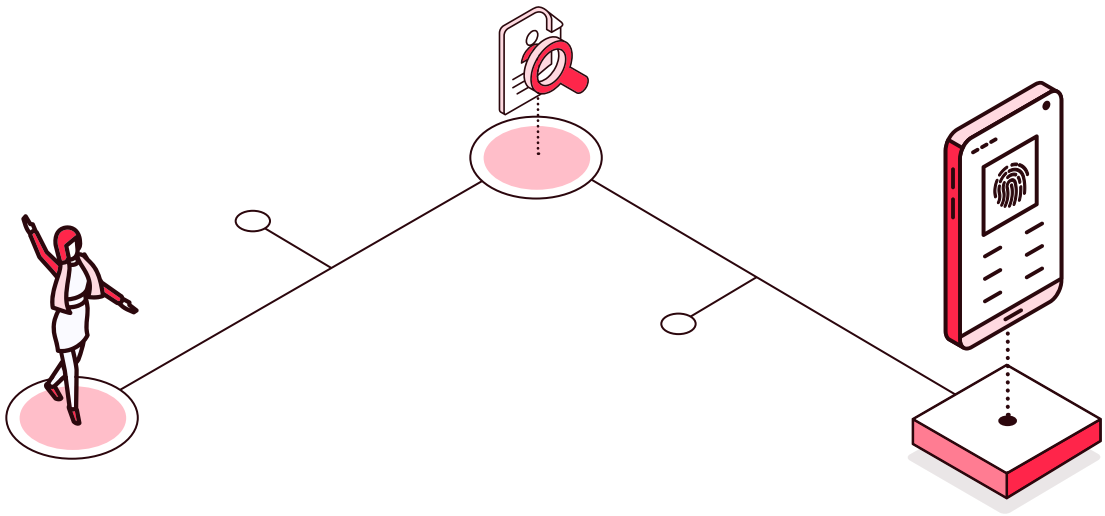
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Does interoperability legislation exist? If so:
  - It is mandatory for the following:
    - Central government executive branch entities?
    - The entire central government, including the judicial and executive branches?
    - State/departmental governments?
    - Municipal governments?
- Does it contemplate the participation of private companies in the national interoperability scheme?
- Does it contain dependent technical regulations that address dimensions such as semantics and technique?



2.6

Digital identity



Identification, in legal terms, can be defined as the accreditation of the personality of the intervener. Digital identification is essential in the development and promotion of any country wishing to implement the so-called e-government: practically nothing of administrative relevance can be done in the digital sphere without being fully identified. For this reason, it is essential for any country to have a regulatory framework associated with identity.

In some cases it will be possible to move forward with some digital services in individual sectors, regulated by the agencies in charge, but this generates the risk of incompatibility between institutions in the event of needing to exchange information. Given its basic nature, since identification is the basis on which all electronic processing is legally based, it must—and usually is—the first regulation that provides legal certainty to the system.

The regulatory context must establish—and, if necessary, evolve to cover—digital identification, in parallel and separately from the regulations on electronic signatures. It should be borne in mind that, in fact, identification and, in association with it, authentication are the elements that provide proof of the applicant for a procedure, and on many occasions it would not even be necessary to collect an electronic signature to consider a request for a procedure completed. It is important to emphasize that the quality and trust of a digital identity is closely aligned with the quality of the civil and identity records that feed it, so the legislation (and operation) of the civil registry and identity agencies is also relevant.

For example, an electronic banking system, when making a transfer, records the different levels of multifactor authentication required, but without requiring an electronic signature or considering that it has been used, not even on the basis of a relaxed definition of signature, such as the so-called "noncryptographic signature." This consideration implies in a certain way a change of paradigm, because public administrations have historically had an organizational system oriented to the document (on paper) and its signature, while in the financial sector it has evolved to the concept of transaction.

Thus, in the administrative sector, paper processing and the assessment of requirements for initiating a procedure have been considered an essential part of the administrative procedure, shifting the burden of justifying the legitimacy of the procedure to the citizen and requiring the provision of supporting documents. In a transactional banking environment, legitimacy is derived from the customer status management process, from a preprocessing procedure, and from an automatic assessment of the requirements context that makes it possible to offer some transactions or others in the user interface.

LEGAL RELATIONS, ESPECIALLY WITH PUBLIC ADMINISTRATION, DEPEND ON IDENTIFICATION. IT IS THEREFORE ESSENTIAL TO HAVE A LEGAL SYSTEM THAT ALLOWS THE DEVELOPMENT OF IDENTITY TO ENSURE THE PROTECTION OF CITIZENS (EXCLUSIVE RIGHT OF USE).

The impact of digital identity is directly related to its use, so all of the above must be compatible with a simple use of the identity (not requiring specialized technical knowledge or particular software, with the possibility of using the cell phone). At the same time, it is necessary to have security levels in accordance with the processing to be carried out, so that legal support is necessary to contemplate all these aspects of a complex problem. There must be a balance between the necessary security measures required by a process and the electronic tools that support it. In general, increasing security means increasing the cost and complexity of use, so the regulation must be aware of this and not demand, as is very common, many more requirements from the digital medium than from the physical one.

Information technologies and their use evolve very rapidly, unlike regulatory processes. Therefore, it is proposed to do the following:

- Have a high-level regulation, indicating in an abstract manner the basic principles of identity, with the rank of law and general application. This should include, as a minimum:
  - the relationship between foundational identity, civil registry identity, and digital identity.
  - the use and types of digital identity, and its use in all procedures and in all public institutions.

- the possibility of having different "confidence levels" or "security levels".
- the enabling of the corresponding regulatory development, but without the rank of law.

› Have an identity regulation detailing the principles of the law, but without going into technical specifications. This is important, given that in general the specific technical part tends to change relatively frequently, so flexibility is required to be able to adapt to these changes.

› Have web pages, information systems, instructions, technical guides, or similar elements that contain the technical details, interoperability, etc.

› Pay attention to the type of technical solution implemented for identity authentication, as it may be associated with high costs that ordinary citizens or small and medium-sized enterprises (SMEs) or micro and small enterprises (MSMEs) cannot afford, resulting in a solution that could not be adopted by the majority. This is especially important when addressing the digital transformation of a country.

CROSS-BORDER DIGITAL IDENTITY

At the international level, it should be noted that the development of digital identity management regulations has usually had a first phase with the definition of state standards that evolved citizens' identity documents to contain digital certificates usable in authentication environments (encoding of the key usage field as an electronic signature). Subsequently, many states developed regulations to create authentication systems that were simpler for citizens to use but sensitive to the need for mechanisms that could be used in contexts with different requirements for "assurance levels" of identity.

In turn, the European Union has published EU Regulation 910/2014 (EIDAS), in which Articles 6 to 12 regulate the requirements for mutual recognition of identification systems, so that identification systems notified by one country must be accepted by all other countries for use in the procedures available to these nations' own citizens. To develop these articles, the European Commission published several standards with indications for countries, which can be considered as a model for the development of regional standards in other continents.

Identification is necessary for any electronic service (both for citizens and for internal users—for example, civil servants). Of special relevance, logically, are the technological systems that provide services for the effective implementation of electronic identification. It is essential that these services be shared and, if possible, general and unique for all procedures and all institutions; otherwise, interoperability will suffer significantly. To this end, even if a country's lead institution directs the regulatory framework, it should be the sectoral institutions that participate in the coordination groups with public entities, as well as with the private sector and the international arena, since, given the impact of this regulation on all stakeholders and sectors, the decisions to be taken should be as consensual as possible, through effective governance.

It is worth mentioning at this point, due to the recent boom in initiatives related to the self sovereign identity, which are based on blockchain technologies. It is important to note that, although it is an interesting technology, today it is still incipient and immature and would not be ready to be implemented by government entities on a massive scale, although its use in the long term is not ruled out once the technology has more mature standards, and large projects are implemented in different sectors.

In any case, it is important to note that, although the name itself is misleading in Spanish-speaking countries, this philosophy of identity does not in any way intend that the technology should provide users with identities on its own. In fact, this situation could lead to a perversion of the technology, depriving states of the provision of citizens' identities, something that could not happen in any case. For this reason, it would be much more interesting to translate the term "self sovereign identity" as "self-management of attributes associated with identity." In this case, it would be much clearer that when someone has a digital identity (official, granted by a state), it could be used in a blockchain-based ecosystem to associate attributes to it, such as titles, diplomas, licenses, and contracts. In any case, as it becomes clear, this is an initiative that should be constantly evaluated in order to assess the technology market in the medium to long term.

NONVERIFIABLE METHODS

A different issue is the "digital identities" that can be obtained over the internet but are based on nonverifiable methods of the natural person to whom it is granted, such as email provider accounts or online shopping services. These "identities" refer to a user account that may or may not have an associated and verified payment method, but in no case have they verified the real identity of the person holding it. In this sense, it is important to point out that this type of unofficial "identities" recognized by the state cannot be used by citizens for their relations with the public administration, since the level of trustworthiness behind them is too low, or practically null.

In fact, and related to the above, it is important that states review the practices by which some digital services are provided to citizens by unverified means, something that, unfortunately, is a fairly widespread practice. For example, it is common, in many places, for citizens to receive official notifications in private email accounts of internet providers. This, however, neither ensures that the destination mailbox belongs to who it claims to be, nor does it usually guarantee the security that state administrative procedures require, and furthermore it does not incorporate any mechanism for verified acknowledgement of receipt and nonrepudiation.

For all the reasons explained here, it is important that the states work decisively in the generation of regulations that cover the creation, issuance, and use of digital identities recognized by it and that, therefore, are usable in relations with public administrations.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Mayor's advisor
Daniel

Daniel wants to promote the use of digital government tools in the small municipality he works for, and he thinks it is a very good idea to replicate the way in which transfers can be identified and signed on the electronic banking website he uses. However, he has serious doubts about whether or not he can implement something similar to do business with the municipal agency.

Vice minister of health
Sara

Sara wants to promote digital transformation in her ministry, but she is afraid to use her electronic identification and signature in such a sensitive area as health services because she does not know how electronic identification relates to the person, and she is very concerned about one individual accessing the very sensitive health data of another. Since in her country identity is managed by the civil registry, she consults there and also the Ministry of ICT, and they inform her about the regulations, as well as about the information system that ensures and gives legal validity to electronic identity and signature. Thanks to this, Ana knows that she can drive the digital transformation in her field without any problems.

EXAMPLES

Click on each flag or icon to go deeper

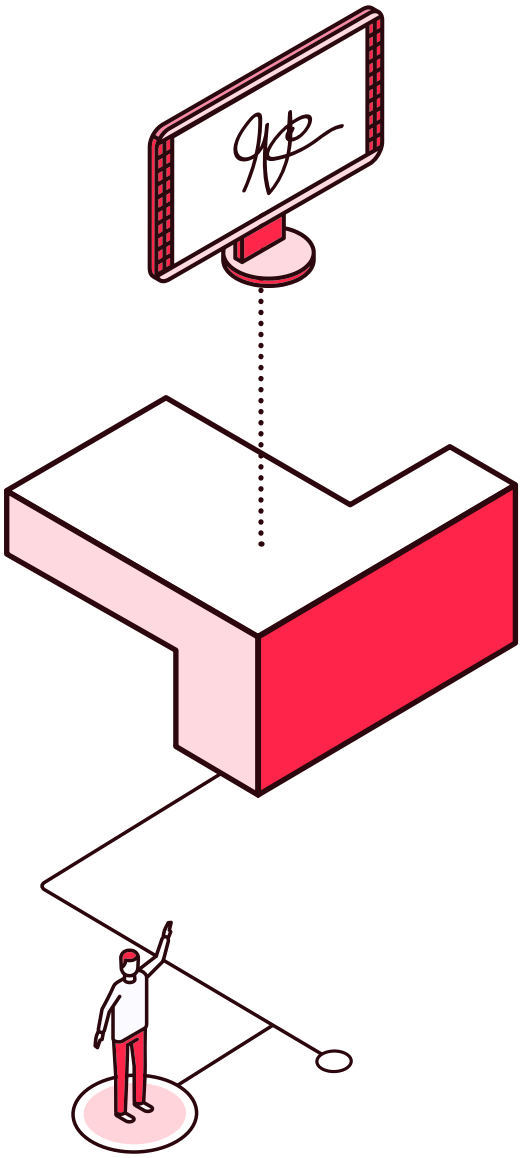
European Union
Regulation 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions.

Uruguay
Digital Identification Policy

INDICATORS

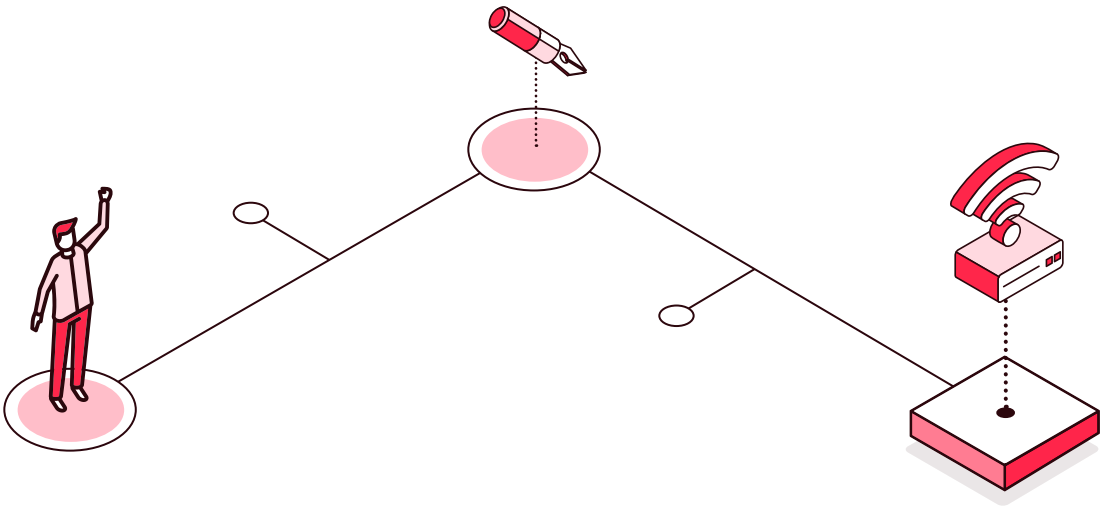
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there legislation that establishes the legal validity of digital identity? If so, do they contemplate the following?
  - Identity based on cryptographic systems?
  - Identity based on noncryptographic systems?
  - Identity based on mobile systems?
  - Cross-border uses?



2.7

Digital signature



The electronic signature is defined as the set of data that, associated with an electronic document, unequivocally identifies the signatory and gives legal validity to the signed document, guaranteeing that it has not been manipulated or altered after signing. Digital identification and the possibility of creating and verifying electronic signatures and seals are essential in the development of electronic administration. In some cases it will be possible to move forward with some digital services in individual sectors, regulated by the agencies in charge themselves, but this generates the risk of future incompatibilities between institutions in the event of needing to exchange information. For this reason, the lead institution must generate the framework for collaboration with the aim of creating or unifying the regulations that support the electronic signature of documents.

Nowadays, it is unthinkable that any type of relationship in a digital context between citizens and administrations, between administrations themselves, and even between countries should not make use of the digital or electronic document, which has among its components the so-called electronic signature. Legal relations, especially with the public administration, depend to a large extent on electronic documents and therefore on the signature.

In a digital and global scenario, all parties must understand each other. Thus, the need for constant interoperability leads us to consider compatibility and full legal security as minimum requirements in any transaction. At the same time, the great variety of institutions, service providers, tools, etc. in the market makes it necessary to consider that—both to converge systems already developed and to build new systems—there must be a basic standard that regulates the common aspects to be followed in the field of electronic signatures.

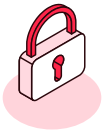
MAIN REGULATORY ASPECTS

The signing of documents is an action that involves all types of actors in all circumstances, which results in the previously mentioned factor of compatibility or standardization, but also in the simple use of a complex concept from the technical point of view. The regulations on digital signatures must establish the legal validity of a signature in digital format and the conditions for it to be accepted with the same legality as a signature in physical format (holographic signature).

Information technologies and their use evolve very quickly, unlike regulatory processes. It is therefore proposed to have a global regulation that is able to respond to the abovementioned aspects:

Have a high-level regulation

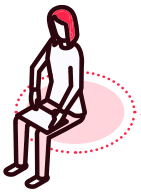
Have web pages and information systems Instructions, technical guides



Establish a system for the use of cryptographic keys

Have an electronic signature regulation

Pay attention to the type of technical solution implemented for the firm



Have a high-level regulation

- That indicates in an abstract manner the basic principles of electronic signatures, with the rank of law and general application. This should include, as a minimum, the following:

  - The regulated use of the digital signature in the country and granting the equivalent validity to the handwritten signature, backed by a certifying authority.

- The types of signature, and their use in all procedures and in all public institutions.
- The possibility of having different "confidence levels" or "security levels."
- Enabling the corresponding regulatory development, but without the rank of law.
- Respecting the principle of technological neutrality as a pillar.
- Rewarding globality as a regulatory premise. Bringing several countries and even continents into a common framework is not an easy task, but better results are expected to be achieved in the future. This need responds to the current global situation, where there is a growing and constant internationalization of companies and of the relationship between clients and suppliers, between administrations, etc.
- Encouraging interoperability. Trusted lists, which in the European case are an infrastructure especially driven by standards such as EU Regulation 910/2014 (EIDAS), are key in this regard. A trusted list allows each state to indicate the certification service providers that have passed the audits required to provide trusted services. A list of these trusted lists at the regional level supports mutual recognition. This aspect is especially important when talking about a country's digital transformation. It is worth nothing that electronic signature types and policies are very varied; it is also difficult to find an objective criterion that would indicate that one type of signature is better than another. For example, in certificate-based electronic signatures, and just to name the ones internationally standardized by the European Telecommunications Standards Institute (ETSI), there is a choice between PAdES, CAdES and XAdES, each of which offers dozens of variants. When it comes to a digitization project, one type can be chosen. However, when there is a nationwide digital transformation, with tens of thousands of procedures, thousands of institutions, and millions of citizens and companies, it is not possible to give everyone the freedom to choose the digital signature they like best because it incurs the risk of lack of interoperability, and its mitigation is always costly (since everyone has to adapt to all standards and variants). For this reason, the lead institution must be in charge of generating and governing the collaboration framework with the aim of creating or unifying the regulations that support the signing of electronic documents.
- Because of its importance and impact, it is essential to pay special attention to—or enabling the regulation of—the electronic document and file, which should always be signed and is the basic element of interchange between administrations. In this line of thought, the so-called automated processing should be taken into account. In certificate-based models, this can be achieved thanks to international standardization, but even so, the different information fields must be standardized so that transactions can be processed automatically by a machine.

- Reflecting the principle of regulatory balance by responding to real cases of use. Generally speaking, regulation is usually more demanding for the electronic medium than for paper. For example, when it comes to bringing paper documents to an institution, in many cases it is enough to go to an office and hand them in, and in other cases, especially if there are predefined models, it is not even necessary to identify oneself. However, when similar projects are embodied in the electronic world, many regulations require everything to be submitted with an advanced electronic signature based on certificates, so the difference in criteria between the physical and digital case is surprising. Therefore, regulation is necessary, but we must be aware that the value of a very secure system that is not used at all is zero. Therefore, it is important to facilitate the electronic signature, with full legal guarantee, avoiding making the system too complex, so that it ends up not being used.

- Carefully differentiating the services and levels of signature and associated security. Electronic signatures should be promoted with full legal security, but at the same time always seeking a balance. Always implementing the highest level of security increases the cost and complexity of use, which need not be the norm for all services.

Have an electronic signature regulation

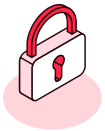
› Detailing the principles of the law, but without going into technical specifications. This is important given that the specific technical part tends to change relatively frequently, so flexibility is required to be able to adapt to these changes.

Have web pages and information systems Instructions, technical guides

› Or similar elements that contain the technical details of interoperability, to facilitate automated processing—for example, signature policies, exact application technologies, metadata configuration, or types of algorithms to be used.

Pay attention to the type of technical solution implemented for the firm

› As it may be associated with high costs that ordinary citizens or SMEs or MSMEs cannot afford, and therefore would not be adopted by most of them.



Establish a system for the use of cryptographic keys

- In recent years, the so-called cloud signature has gained special relevance as a modality for the use of cryptographic keys used to sign electronically, which are managed in a centrally managed hardware security module (HSM). This mechanism can work as follows:

  - The user installs a driver on his personal computer that remotely accesses the keys in the HSM but performs the identification and signature functions on his own computer, as if it were a chip card.

  - The documents are uploaded to the server, and the electronic signature is made on the server with the corresponding keys among those managed by the HSM.

- In both cases a Signature Activation Module (SAM) checks the user's authentication to give him access to his key. The requirements for this type of system are included in the technical standard ETSI TS 119 431-1[24] : Electronic signatures and infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.

- Sometimes the signature in the cloud is complemented with a remote registration system by videoconferencing or video identification, so that the generation of keys and obtaining the certificate are also managed remotely. This type of system is essential in contexts where mobility is restricted, for example due to a pandemic.

- In the context of the ETSI standards body, a standard has been developed that aims to harmonize remote identification requirements for the issuance of qualified certificates: ETSI TS 119 461[25] (Policy and security requirements for trust service components providing identity proofing of trust service subjects). At the time of writing, the standard was in draft form.

24. https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.01.01_60/ts_11943101v010101p.pdf
25. https://docbox.etsi.org/esi/Open/Latest_Drafts/Draft%20ETSI-TS-119-461-v0.0.5.pdf

INTEGRITY AND ATTRIBUTABILITY

All the procedures carried out with the administration are based on documents that are required to have two attributes:

- **Integrity:** When the electronic signature is made, a mathematical function is performed between a value obtained by applying a summary function to the document and a private key associated with the signatory's certificate (element containing the public key that allows the signature to be verified, calculating this summary value both from the signature and from the document).

- **Attributability:** This is obtained because the certificate, in addition to the public key, includes other data that allow the signer to be identified.

THE SIGNATURE IS A LEGAL BASIS FOR ELECTRONIC PROCESSING AND IS NECESSARY TO GIVE LEGAL VALIDITY TO DOCUMENTS AND TRANSACTIONS CARRIED OUT IN THE ELECTRONIC ENVIRONMENT.

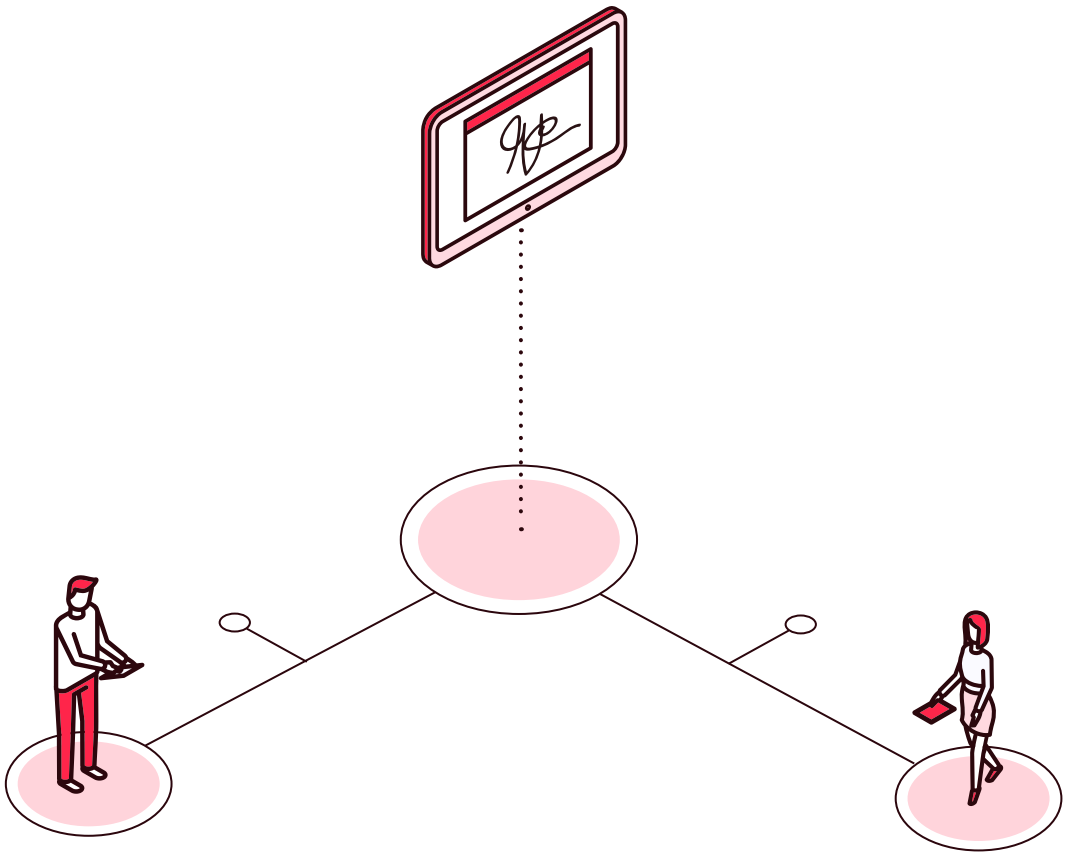
CROSS-CUTTING RECOGNITION

Logically, a particularly important aspect is the technological systems that provide services for the effective implementation of the signature policy. It is essential that these services be shared and, if possible, general and unique for all procedures and all institutions; otherwise, interoperability will suffer significantly. To this end, relations with the coordination groups with public entities, as well as with the private sector and the international sphere, are essential, since, given the impact of this regulation on all actors and sectors, the decisions to be taken should be as consensual as possible through effective governance.

As a result of the above, the lead institution must bring the sectoral institutions into agreement and set the common strategy of a country at the regulatory level. To this end, it is essential to create governing bodies such as technical committees, where problems can be shared and managed in a constructive spirit, while maintaining technological neutrality for the administration.

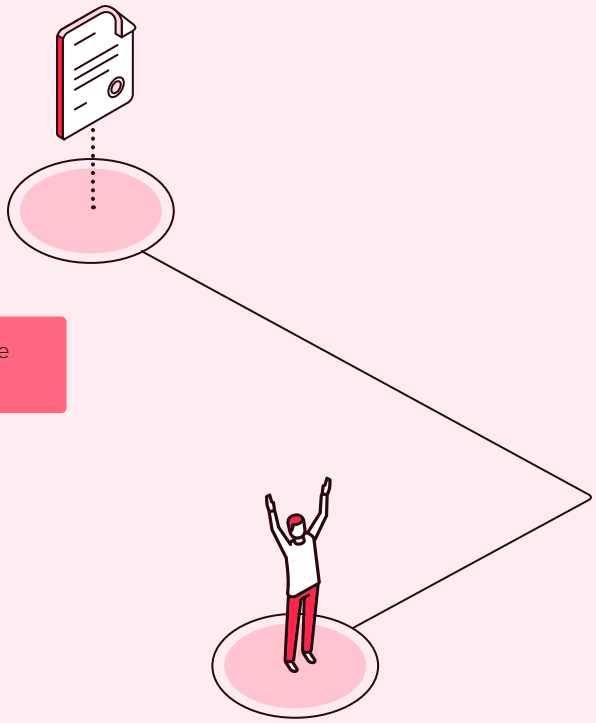
At the international level, it is important to have mechanisms for mutual recognition of electronic signatures. In this way it will be possible to open up a world of possibilities for the interoperability of administrative documents between agencies in different countries, or for a citizen to send a document originating in country X to an administration in country Y. To solve these problems, there must be entities or organizations that, in a centralized manner, standardize formats and semantic and technical elements, and create directories of trusted digital signature issuers.

› *Example:* The Latin American and Caribbean e-Government network (GEALC network) has launched an initiative called "Cross-border digital signature." As its name suggests, it is aimed at recognizing and exchanging electronic signatures in the countries of the region, beyond their borders.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.



Entrepreneur
Ana

Ana has to present a signed document to a public entity to carry out a procedure. She has doubts as to whether she can use the electronic signature she already has because she wonders if it is legally valid for this particular procedure. She is afraid that if it is not, she may have problems in the approval of this procedure, which is key for her business.

Citizen
Camilo

Camilo goes to apply, as he does every year, for his daughter's education allowance. At the office, the official not only assists him with his request, but also informs him about the new digital signature and identity system, which he finds very easy to use. He gives him a leaflet with information about it, whose regulation gives Camilo confidence and leads him to register in the system at that very moment. Thanks to this, not only will he be able to check the status of the subsidy he has just requested from his cell phone, but he will also be able to process it next year without having to go anywhere.

EXAMPLES

Click on each flag or icon to go deeper

European Union

Regulation (EU) n. ° 910/2014 of the European Parliament and of the Council of 23 July 2014. It establishes the principle that the legal effects of an electronic signature should not be denied merely because it is an electronic signature or because it does not meet all the requirements of a qualified electronic signature.

Spain

Law 39/2015, of October 1, on the Common Administrative Procedure of the Public Administrations. Articles 9, 10, and 11 are highlighted, in which the electronic signature systems admitted for administrative procedures are recognized and established. This law also regulates noncryptographic electronic signatures based on cl@ve.

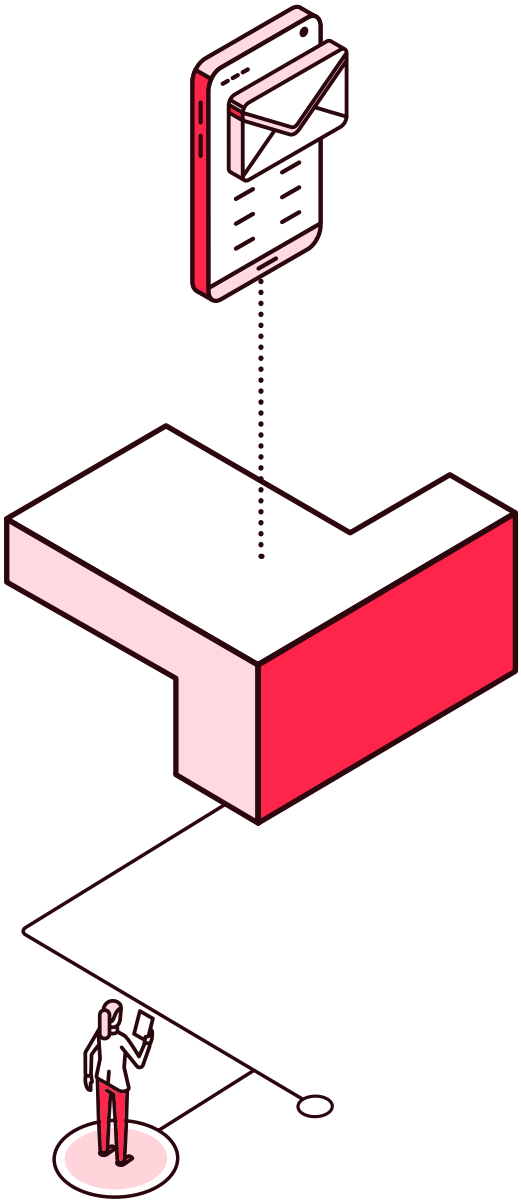
Uruguay

Law No. 18,600 of September 21, 2009. It recognizes "the admissibility, validity and legal effectiveness of electronic documents and electronic signatures" and describes the characteristics of the National Electronic Certification Infrastructure.

INDICATORS

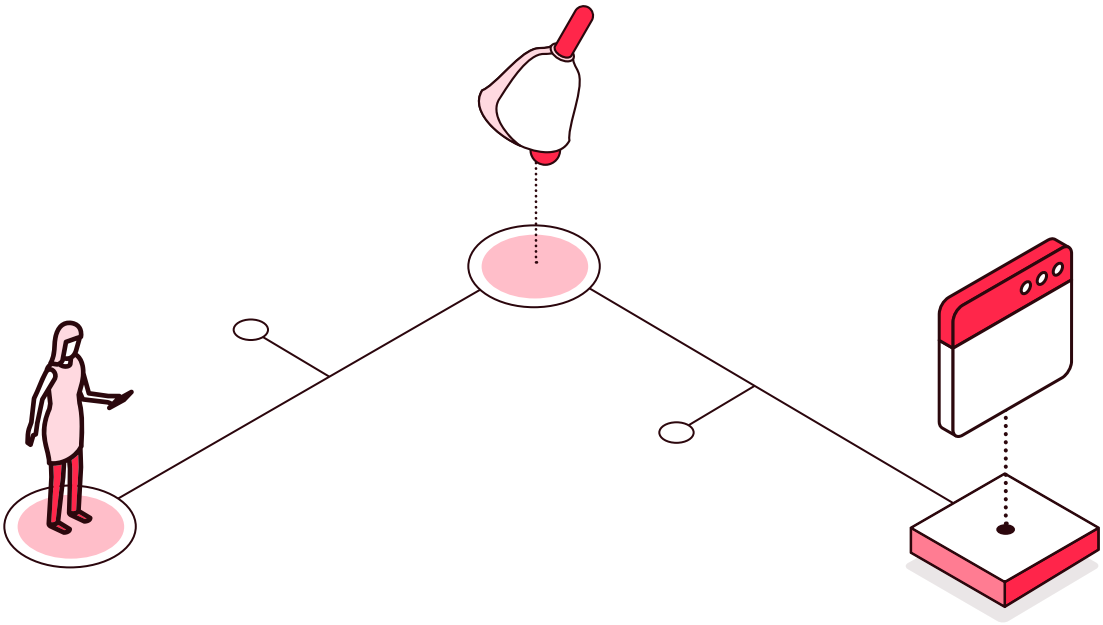
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there legislation establishing the legal validity of digital signatures? If so, do they contemplate:
  - The signature based on cryptographic systems?
  - The signature based on noncryptographic systems?
  - The firm based on mobile systems?
  - Cross-border uses?



2.8

Electronic notifications



Technological advances are reaching public administrations, and with it, the inevitable modernization of their management systems. In recent years, public bodies have opted for telematic communication, progressively replacing paper notifications and acknowledgement of receipt with electronic notifications. The latter are closely linked to the process of administrative simplification, as well as to greater effectiveness and efficiency.

The development of applications and systems aimed at any citizen (individual or third party public bodies) that allow aspects such as notifications to be taken to the electronic world, providing the possibility of receiving notices and documents that the public administrations wish to send them, is nothing more than further evidence of the unstoppable process of digital transformation that we are witnessing in a global world. This process encompasses purely technological actions, but it must go hand in hand with appropriate regulations that promote the creation, unification, simplification and/or elimination of channels, processes, or procedures created by the public administration. In this way it will be possible to improve government communications and procedures and, ultimately, public services.

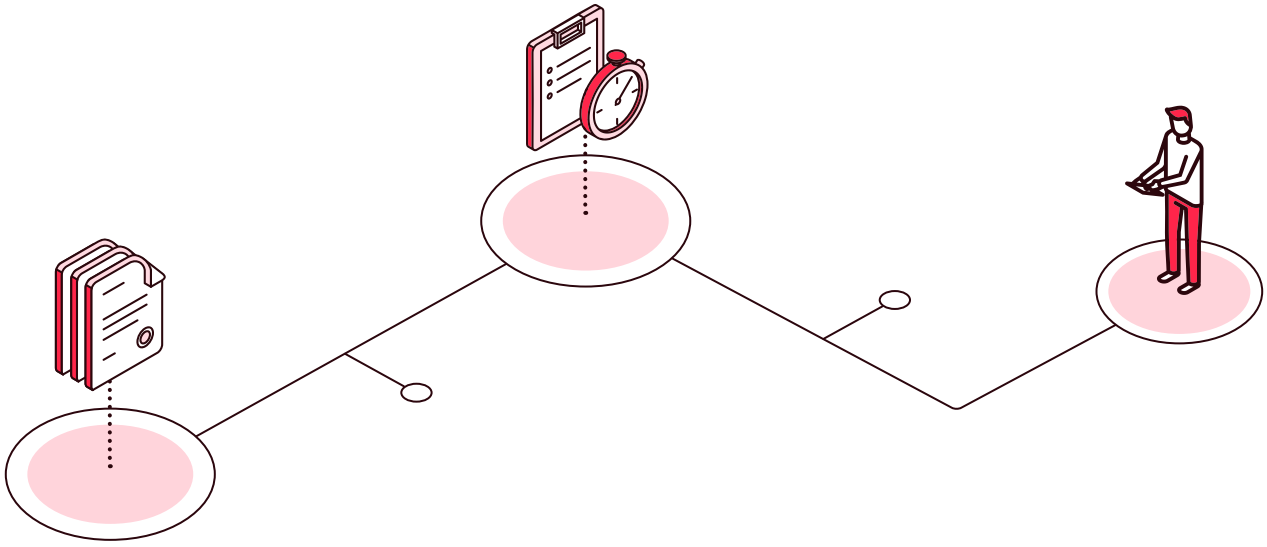
MAIN ADVANTAGES OF ALWAYS THINKING OF THE CITIZEN AS THE CENTER OF TRANSFORMATION

- Time savings, thanks to the immediacy of digital media by connecting more easily, avoiding waits, delays, etc.
- Cost savings for the public administration itself, reflected in lower expenses for
  - in-office printing;
  - sending of postal notifications;
  - time between sending and receiving the notification, coupled with the guarantee of the security of this simplified registration of notifications.

LEGAL VALIDITY

However, these undoubted advantages cannot leave aside the importance of an adequate regulation that supports, for example,

- the legal effects of these notifications.
- the form of access.
- the computation of deadlines.
- the effects of a possible rejection.



Otherwise, true electronic access of citizens to the administration could not be effective.

Although notifications are preferably made by electronic means, in order to be legally valid, they must comply with a series of requirements and guarantees that must be legally established. In this sense, it is of vital importance that the notifications are made and that there is a record that this has been done. They are presumed to be valid as long as there is evidence of their sending or making available, of their receipt or access by the interested party or his representative, of their dates and times, of their full content, and of the reliable identity of the sender and the addressee. Otherwise, the defense of the rights and legitimate interests of the individual may be affected.

LEGISLATION THAT GUARANTEES AND PROVIDES LEGAL CERTAINTY WILL RESULT IN GREATER AND BETTER USE OF ELECTRONIC MEANS OF NOTIFICATION.

A NECESSARY ELECTRONIC RELATIONSHIP

Many countries have introduced important innovations in their legislation regulating the relations of interested parties with the administration through electronic means. Thus, while individuals can still choose the means of relating with the administration (whether electronic or not), the obligation to relate by electronic means is already imposed on subjects, such as the following:

- companies and natural or legal persons
- entities without legal personality
- those who exercise professions of compulsory membership, including notaries and registrars
- the representatives of those obliged to relate by electronic means
- public employees for the actions they carry out with the different public administrations due to their condition as such

For these parties, notifications will be made exclusively by electronic means at the virtual headquarters, virtual office, electronic office, or similar office of the acting administration or agency to which they must have access.

However, paper notifications are still maintained in cases such as the following:

- Those sent by mail with acknowledgment of receipt for nonobligated parties.
- The spontaneous appearance of the interested party or his representative at the administrative body or office where the notification is delivered directly by a public employee.
- When the act to be notified is accompanied by an element that cannot be converted into electronic format.
- Those containing means of payment in favor of the obligors.

HOW TO GO FURTHER?

The administrations of some countries have tried to boost their regulatory standards for electronic notifications in the following aspects:

- Increasingly expanding the number of subjects obliged to interact electronically with the administration. To this end, they have established the obligation to electronically practice the notifications for certain procedures, as well as for some individuals served by the administration, due to their economic or technical capacity, professional dedication, or other reasons that prove that they have access and availability of the necessary electronic means to do so.
- Regardless of the notification channel, the user may also provide an email address or cell phone number for the receipt of notices. The regulations should clarify that these notices do not constitute a fully valid notification. Otherwise, the regulations themselves will regulate that it will be important to regularly check the mailbox or SMS, as well as to keep it updated in case of any modification, so that it will be possible to check if there is any notification notice, since the notification will be understood to be practiced at the moment in which the access to its content in the electronic headquarters, virtual office, or similar office of the administration takes place.
- In the case that the administered party has chosen the electronic means of notification, or this being mandatory, and the notification remains in the notification platform without being opened, it will be understood to be rejected when the period indicated in the rule has elapsed since the notification was made available without access to its content.

OTHER CONSIDERATIONS SPECIFIC TO NOTIFICATIONS THAT SHOULD NOT BE OVERLOOKED

- **The administrations** must adopt the measures they consider necessary for the protection of the personal data contained in the resolutions and administrative acts when these are addressed to more than one interested party.

- **Regulation of unsuccessful notific**ation: When the interested parties in a proceeding are unknown, the place of notification is unknown, or when notification has been attempted, it has not been possible, notification will be made by means of an announcement published in the official newspaper or gazette of the country or any other means that allows its publication for legal purposes. However, other complementary forms of notification through the remaining means of dissemination may be expressly determined, which shall not exclude the obligation to publish the corresponding notice in the official gazette of the country.

- If the competent body considers that the notification by means of announcements or the publication of an act harms legitimate rights or interests, it shall limit itself to publishing in the corresponding newspaper or official gazette a brief indication of the content of the act and the place where the interested parties may appear, within the term established, to be informed of the full content of the aforementioned act and to record such knowledge.

SECURITY MEASURES IN THE PRACTICE OF NOTIFICATIONS

There must always be guarantees associated with the notification. The public electronic notification service must be supported by a computer support system, which allows the verification and registration of the addressee and the object, as well as the date and time of availability of electronic notifications in the public electronic notification service, for all legal purposes. Therefore, it will be characterized by the following:

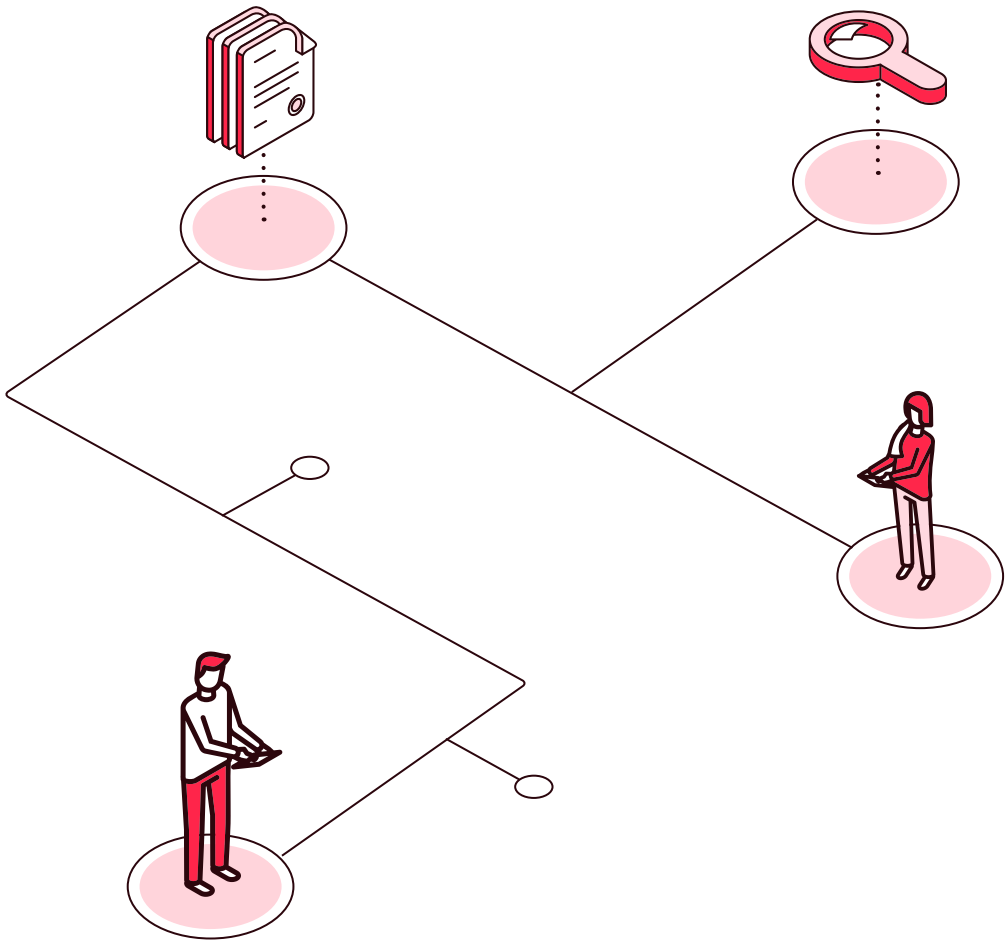
- **Traceability:** The notification system must record the time and date at which the notification was issued by the administration.

- **Logging:** The system shall be able to record the date and time at which the content was accessed by the user.

- **Conservation:** It will be necessary to establish an expiration period, so that after a determined and sufficient period of time these notifications are no longer accessible, in order to avoid accumulating huge amounts of obsolete documentation.

It is also important that the rule regulates the means of identification that allow access to the content of the notification. For this purpose, an electronic means of identification should be adopted, either issued by the administration or by another body, which may be in the name of the natural person as well as in the name of the company, natural person, or legal entity that it represents. Likewise, it is necessary to regulate the period of time available to the administration to issue a notification, which should be short after the administrative resolution has been issued, in order to take advantage of the immediacy of these technologies.

Finally, it would be desirable for the legislation to address the possibility of having a single point of access to all notifications. This would prevent interested parties, whether natural or legal persons, from having to access the different electronic mailboxes made available by multiple platforms and portals of the different services in a country. It would also support public services that do not currently provide electronic notifications. It would therefore be advisable to create a single system so that the public service of electronic notifications is provided by a single public entity.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Vice minister of health
Sara

When Sara took office as vice minister of health, her first objective was to reduce the expenditure incurred by the ministry. The problem centered on the amount of paper mailings and communications issued by the agency, which accounted for 30 percent of the entity's expenditures. In addition, there were complaints about the delay between having done the paperwork and getting a response from the health services, as well as the long queues due to the crowding of citizens to carry out any paperwork. Thus, Ana thought that implementing an electronic notification system for health services would mean a reduction in the cost of printing and sending postal notifications, a shorter time between sending and receiving the notification, and a no-less-important guarantee of the security of this simplified registry of notifications.

Citizen
Camilo

Camilo is not used to doing business with the administration, and every time he faces them he loses too much time traveling, waiting in long lines, and having to go repeatedly because he does not have all the documentation. He does not understand how it is not modernized so that he can carry out these procedures without leaving home, being able to receive the notifications in his email or to a portal where he can go to consult his notifications with the different administrations.

Entrepreneur

Ana

Ana is delighted with the step that the administration has taken when communicating with her company: now it is easier to carry out the procedure, and she is always aware of the progress. There is no longer any risk of losing paper; now she has everything centralized in her management software, controlled and stored in an integrated way.

EXAMPLES

Click on each flag or icon to go deeper

European Union

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems in the Union.

Spain

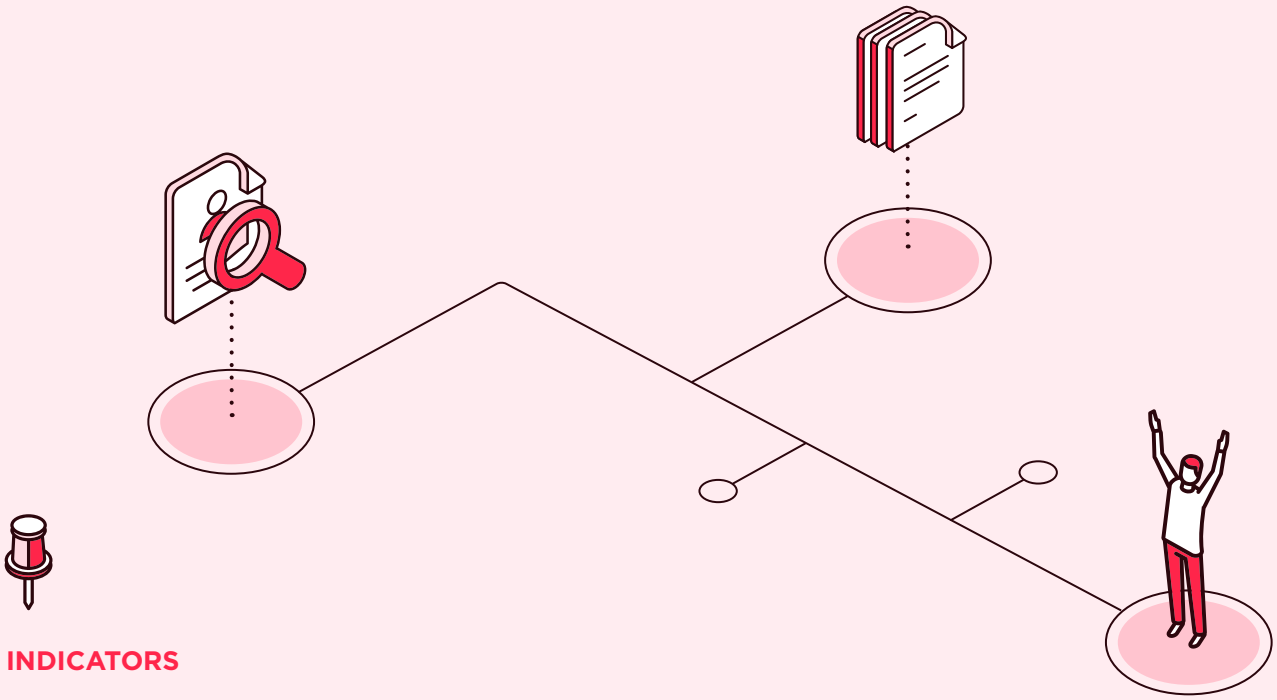
Law 39/2015, of October 1, 2015, on the Common Administrative Procedure of Public Administrations. Chapter II: Effectiveness of acts.

European Union

General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council.

Portugal

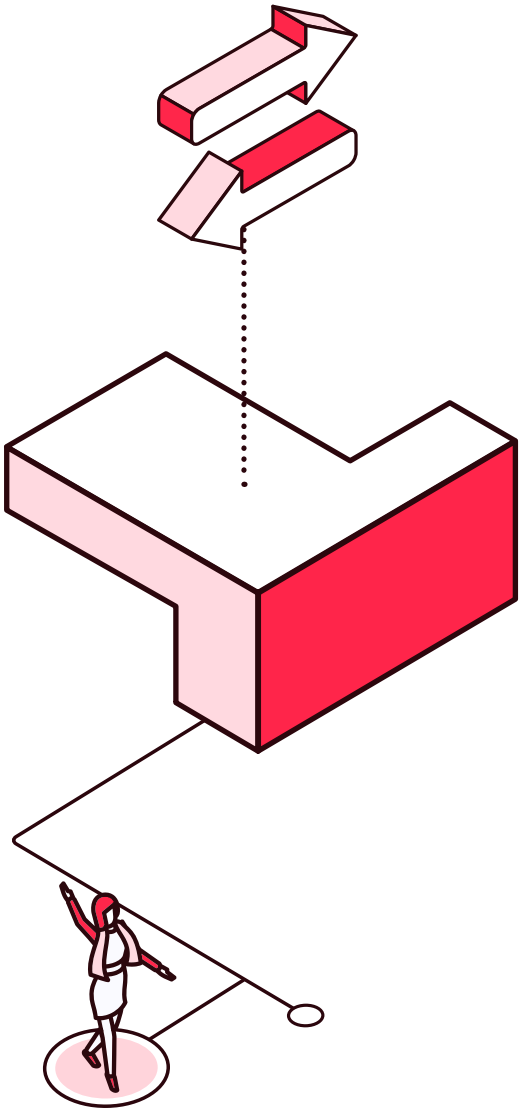
DL. 93/2017, of August 1, which regulates the public service of electronic notifications



INDICATORS

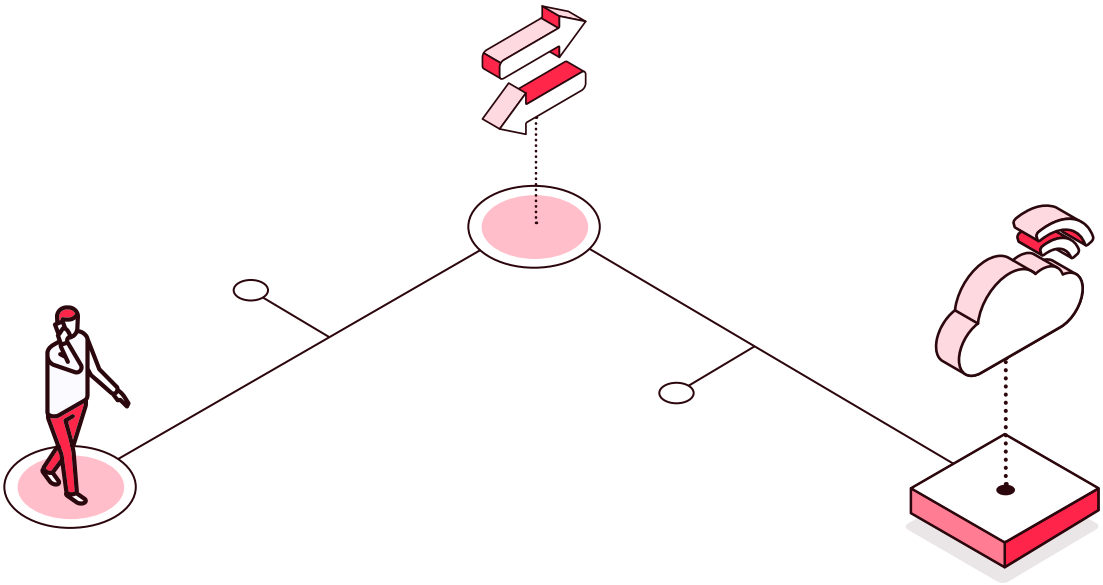
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there specific regulations governing the effectiveness of administrative acts?, If so:
  - Is there any reference within this regulation to electronic notifications and their effects?
- Is there a technological tool that allows the sending of electronic notifications?, If so:
  - Is there a regulation governing the means of digital identification, the use of electronic certificates, signature, etc.?
- Is there any system for accessing administrative documentation or notifications through the internet by users external to the administration, such as citizens or companies, and by other administrations in the country, if any?
- Is there traceability of this access for purposes of counting time frames, etc.?



2.9

Digital input and output register



In order to bring the administration closer to the citizen and thus make e-administration effective, the different public administrations have created and regulated internet portals. These electronic access points allow access via the internet to information from the public administration, a public body, an office or a public entity, and, where appropriate, to electronic processing.

From a regulatory point of view, access to electronic processing will be a secure site differentiated from the general information section, which will include all actions, procedures, and services that require authentication of the public administration or of citizens and companies by electronic means and that allow the completion of procedures exclusively by electronic or telematic means (i.e., through the internet) without having to go in person to an office. The standard, approved by the states, will determine the identification of these means of access clearly with denominations such as “electronic headquarters,” “virtual headquarters,” “virtual office,” “electronic office,” or similar,, as appropriate.

As in physical offices, in this virtual office it is essential to have a registry. The normative regulation of this is essential to provide legal certainty to citizens and companies when dealing with the administration, and should include aspects such as

- the form of access to the registry.
- time availability.
- the effects of the presentation.
- how the entries will be made, etc.

In general, registration or recording, based on the existing regulations in force in a good number of countries, is the action of noting and accounting in chronological order for a certain order of things. It is also understood as the book or support in which it is recorded, the place in which it is recorded, and the entry or annotation that is made.

OBJECTIVES OF THE REGISTRY SYSTEM

According to the current normative regulation, a registration system should

- attest to the dates of entry and exit of any document received or issued in a given organ or administrative unit.
- continue, from the registration number, all the steps of an application or request.
- know if the deadline has been met or not in a procedure.

REGISTRATION TYPES

Traditionally, there have been two types of registration in registry offices:

- **Incoming:** When the citizen submits requests, writings, and communications addressed to the public administrations.
- **Outgoing:** When the administration registers the documents that it sends to the citizen to private entities or to the administration itself.

SOME KEY ASPECTS FOR THE PROPER FUNCTIONING OF THE REGISTRY

Currently, the most advanced countries have included in their specific registration regulations key aspects such as

- receipt and dispatch of applications, writings, and communications.
- issuance of receipts or acknowledgments of filing.
- the annotation of entry or exit entries.
- the forwarding of requests, letters, and communications to the persons, bodies, or units to which they are addressed.
- the issuance of stamped copies of original documents.
- the realization of collations and attestations.

THE EVOLUTION OF THE REGISTRY

The registry offices receive numerous documents, information, and requests in different formats that must be classified and registered. In turn, a control stamp is included with this information to distribute it and deliver it to each recipient, who can accept, reject, or transfer the record received.

Traditionally, and as stated in the legislation regulating the operation of paper, the administrative bodies kept a general registry in physical format (the registry book), in which the corresponding entry was made for any document or communication submitted on paper or received in any administrative unit. Likewise, an annotation was made of any official paper documents or communications sent to other agencies or individuals.

Subsequently, the rules began to introduce the possibility of computerizing the operation of the registry. In this way, a computerized and correlative entry or exit record number was assigned, as well as the date, which had to coincide with the printed stamp that had been used when the documentation was received. This work, however, was still very manual, since it was recorded *a posteriori*, and there was a risk of losing some of the information or even the documentation provided.

It is here where digitization takes on special importance, understood as the process by which the traditional has to be converted into digital. Thus, digitizing the registry consists of converting this analog (manual) process into a digital registry, a cornerstone when regulating this matter in many countries.

A DIGITAL REGISTRY, AND THIS IS HOW IT SHOULD BE REGULATED, COMBINES THE ENTRY AND EXIT OF DIGITAL DOCUMENTS OR DOCUMENTS THAT, DESPITE ENTERING OR LEAVING ON PAPER, ARE DIGITIZED (I.E., THE ADMINISTRATION ALWAYS KEEPS AN ORIGINAL OR COPY IN ELECTRONIC FORMAT).

THE DUAL REGULATORY PATHWAY

It should be noted that digitization goes beyond scanning, since the digitized image incorporates its own metadata that must be defined in a technical regulation and that give value to the document, such as the electronic seal, the date and time, the value and type of document, etc. This addition is one of the first steps to achieve true electronic processing, allowing procedures to be processed digitally from the beginning.

Therefore, the rule regulating the registry must include the dual track:

- The registry offices attend in person and allow interested parties, if they so wish or if they lack electronic means, to submit their applications on paper, which will be converted to electronic format by means of digitalization processes. This allows the return of the originals to the interested party, without prejudice to those cases in which the custody of the documents submitted by the administration is mandatory or the submission of objects or documents on a specific support not susceptible to digitalization is mandatory.

- At the same time, it enables within the web portals a digital electronic registry open 24-7 that will allow the submission of applications, writings, and all kinds of communications by citizens and companies to an administration.

Thus, an increasing number of countries have effectively regulated and implemented digital public administration registries—in particular, a general electronic registry that is interoperable with other administrations or, where appropriate, that makes it possible to join the registry of the national central administration, whether at the state or federal level.

In any case, the rule must establish that this registry will be unique, regardless of whether the physical or virtual office is used. It will be a general electronic or digital registry, in which the corresponding entry will be made for any document submitted to or received by any administrative body, public agency, office, or entity linked or dependent on them. The output of official documents addressed to other administrative bodies or individuals may also be recorded there.

THE GENERAL ELECTRONIC OR DIGITAL REGISTRY OF EACH ADMINISTRATION MUST ALSO COMPLY WITH THE GUARANTEES AND SECURITY MEASURES PROVIDED FOR IN CYBERSECURITY AND PERSONAL DATA PROTECTION LEGISLATION.

WHAT TO SPECIFY IN A REGULATION FOR THE CREATION OF ELECTRONIC RECORDS?

- The body, office or unit responsible for the management of the registry.
- Official date and time.
- Days declared as nonworking days.
- The updated list of procedures that can be initiated in the registry. This should be constantly updated according to the capacity of the administration, trying, as far as possible, to simplify the formalities and thus include an increasing number of them.
- The entries or registers shall always be recorded in the order in which the documents are received or issued, and shall indicate the date of the day on which they are produced. Once the registration process has been completed, the documents shall be forwarded without delay to their addressees and to the corresponding administrative units from the registry where they were received.
- The characteristics and content of the electronic or digital registry. In this regard, it should be ensured that each entry records the following:
  - one number
  - an epigraph or expressive description of its nature
  - the date and time of your presentation
  - identification of the interested party
  - the sending administrative body, if applicable
  - the person or administrative body to which it is sent
  - a reference to the content of the document being registered, if applicable.

- The issuance of receipts accrediting the presentation automatically. These will consist of an authenticated copy of the document in question, including the date and time of presentation and the registration entry number, as well as a receipt accrediting other documents that, if applicable, accompany it and guarantee integrity and nonrepudiation.

ADVANTAGES THAT TECHNOLOGY BRINGS TO A REGISTRY

- Digitized management of the registry.
- Exploitation of information.
- Interoperability of registry offices with different systems.
- Savings in costs and cubic space in offices.
- Reduced risk of documentation loss.
- Saving of time of the personnel that manages documentation.

LEGAL REQUIREMENTS FOR DIGITIZATION

Prior to the implementation and regulation of the digital registry, all regulations must be evaluated and adapted to electronic administration, thus providing full legal validity to the entries. In particular, it is advisable to consider the following:

1. The right to interact electronically with the administration—that is, the right to
    - get information.
    - consult and make allegations.
    - formulate requests.
    - manifest consent.
    - establish claims.
    - make payments.
    - perform transactions.
    - oppose administrative resolutions and acts, among others.

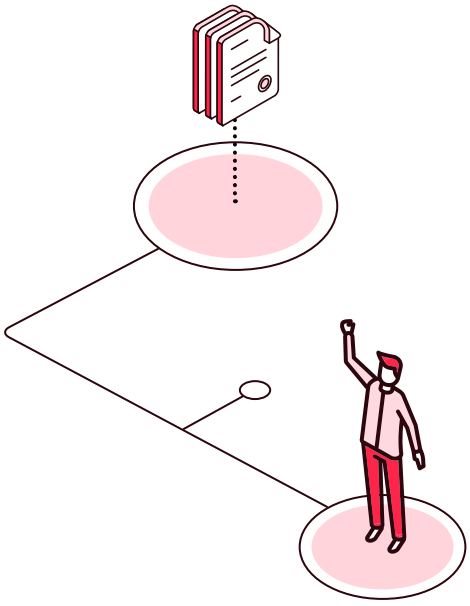
2. Obligations to certain groups, such as companies, to use electronic means to interact with the administration or to submit certain documents within certain procedures. This requirement could also be addressed to groups of individuals who, due to their capacity, whether economic, technical, professional dedication or other reasons, can demonstrate that they have access, knowledge, and availability of the necessary electronic means.

3. Preferably and to the extent possible, opt for the automation of the check-in and check-out process, complying with the interoperability requirements by means of the following:

- customized forms.
- data exploitation.
- digital seal or secure verification code on the digitized document.
- proof of registration.
- control of information by means of distribution, transfer, or rejection criteria.

4. Adequate regulations on identification, authentication, and electronic signature. Although it is proposed to allow the appropriate use of electronic means for the purposes pursued by the administration, these should not place an excessive burden on the person administered. For this reason, the use of commonly used technologies should be preferred, and in particular, identification will generally suffice. Thus, the electronic signature is intended for such limited uses as to

- formulate requests.
- submit responsible declarations or communications.
- file appeals.
- desist from actions.
- waive rights.

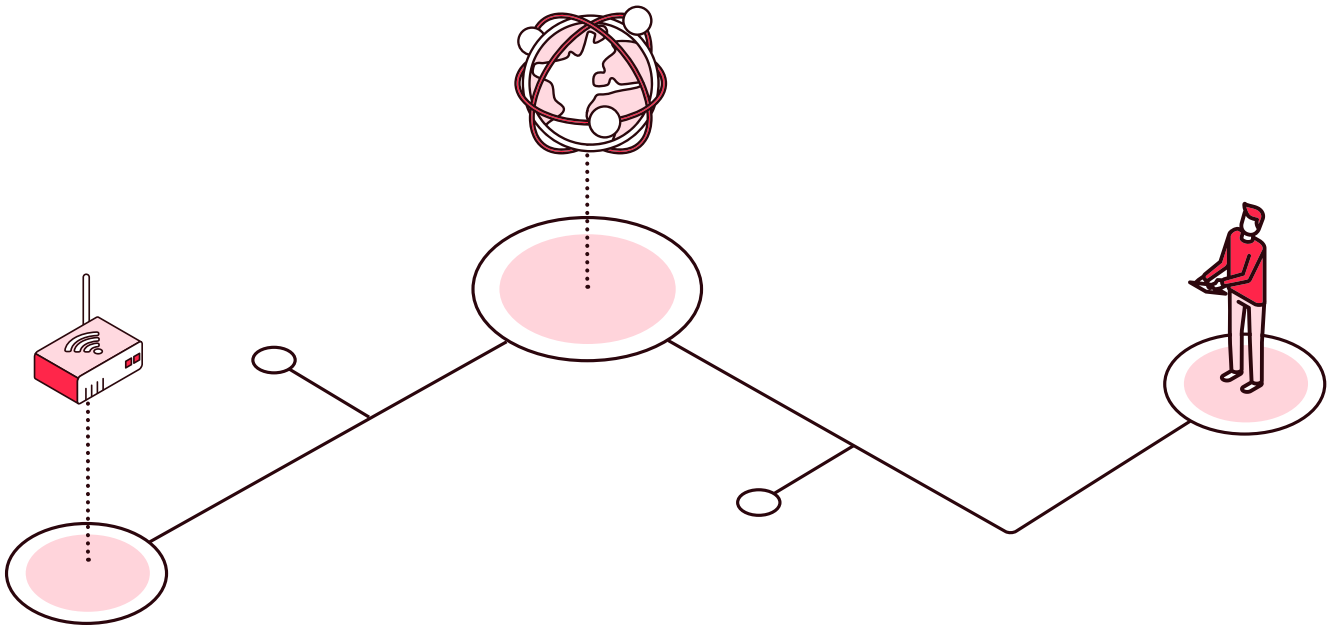


5. In the area of representation, it is recommended that an electronic central registry of authorizations be set up and regulated, in which all authorizations granted to act before the administration are recorded, and which can be freely consulted by all administrations. This would include new means of accrediting representation in the exclusive sphere of public administrations, such as the possibility of granting power of attorney in person or electronically by means of a virtual appearance, or simply with the accreditation of registration in the electronic registry of authorizations of the administration.

6. Review the archiving regulations of public administrations and opt to centralize in a single archive the documents and electronic files corresponding to completed procedures. Similarly, it would be appropriate to require that these files be kept in a format that guarantees the authenticity, integrity, and preservation of the document.

7. To have regulations that cover the issuance of certified copies by public employees, as well as a registry or other equivalent system that makes it possible to record who are the officials authorized to perform this task. This ensures that the copies have been properly issued. In addition, if each administration so decides to organize it, public employees dedicated to assisting interested parties in the use of electronic means may also be listed there jointly, without there being any impediment to the same employee having both functions or only one of them.

8. A technical regulation that includes the standardization and establishment, in a unique, global, and complete manner, of the data model for the exchange of entries between registry entities regardless of the system of registry of origin or destination, and of the exchange technology.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Vice minister of health
Sara

Sara arrived at the Ministry of Health thinking that, like the rest of her life, it would have been digitally transformed by now. However, far from that, there is still no regulation that defines in a standard way the electronic document, how to sign, how to store the information, etc. Sara thinks it is important not only to have a regulation on electronic registries, but also to standardize data models for the exchange of entries between registry entities regardless of the system of origin or destination registry, and of the exchange technology.

Citizen
Camilo

Camilo is not used to doing business with the administration, and every time he has to deal with them he loses too much time traveling and waiting in long lines. He also has to carry a lot of original documentation with him at all times, with the risk of losing or damaging it. He does not understand why a digital system has not already been implemented to be able to provide, submit, or process his documents and requests to the administration.

Entrepreneur

Ana

Ana, a successful entrepreneur, is happy that in her country she does not have to use paper to deal with the different public institutions but, as with everything, there is room for improvement. The relationship with each of them is different: some allow registration on their platform, others on the central platform and some have not yet implemented it and the registration is on paper. He does not understand how they do not reach a consensus to centralize the information in a single registry and the possibility that all the registries are interoperable.

EXAMPLES

Click on each flag or icon to go deeper

Spain

Law 39/2015, of October 1, on the Common Administrative Procedure for Public Administrations, through which the General Electronic Registry for the General State Administration is regulated.

Spain

Law 40/2015 of October 1, 2015, on the Legal Regime of the Public Sector, by means of which the regulation on the performance and functioning of the public sector by electronic means is approved.

European Union

Commission Delegated Regulation (EU) 2018/815 of 17 December 2018 supplementing Directive 2004/109/EC of the European Parliament and of the Council as regards regulatory technical standards concerning the specification of a single electronic reporting format.

European Union

Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 on establishing a single digital gateway for access to information, procedures and helpdesk and troubleshooting services.

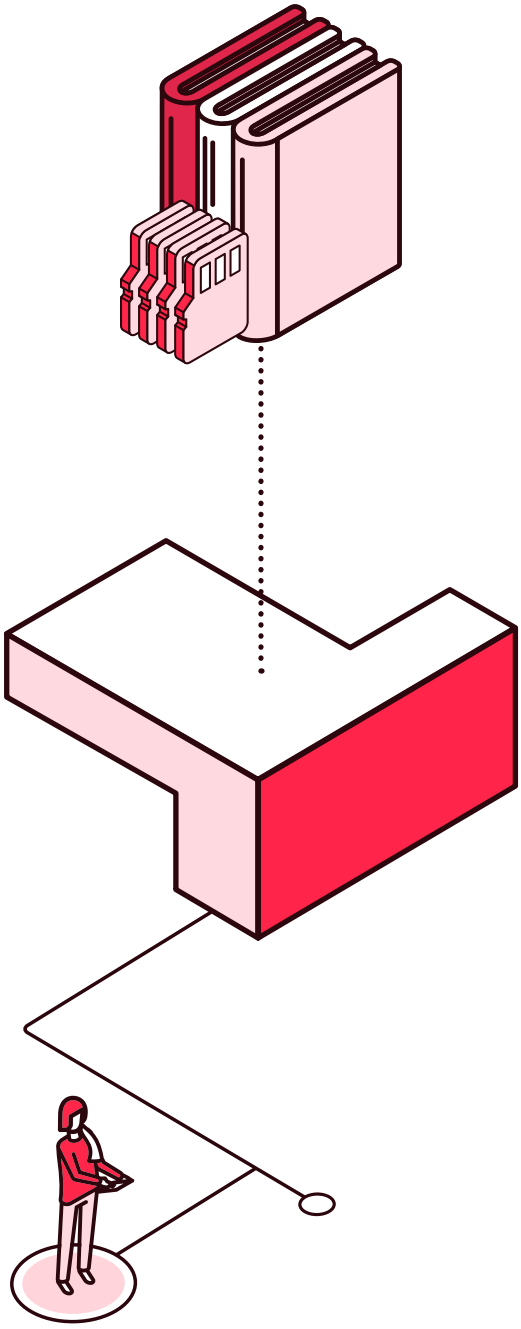
European Union

Regulation (EU) 2016/1191 of the European Parliament and of the Council of 6 July 2016 facilitating the free movement of citizens by simplifying the requirements for the submission of certain public documents in the European Union.

INDICATORS

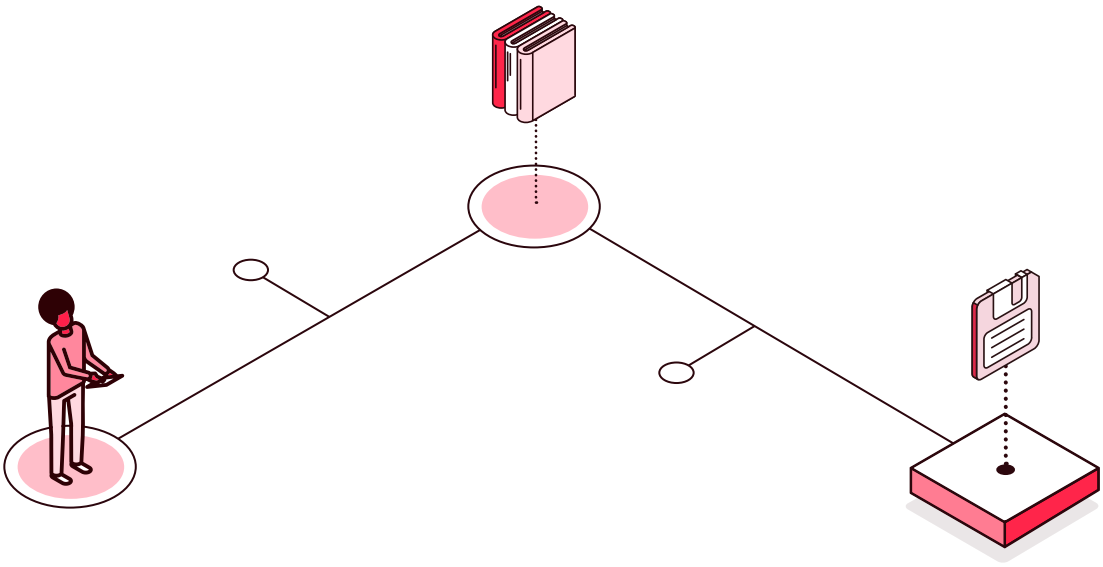
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there specific regulations governing administrative records?
- Is there any reference to an electronic or digital registry in these regulations?
- Are there any regulations that allow or provide for the digitization of paper input and output records?
- Is there a standard that enables a system for the exchange and/or consultation of records by the administrations?
- Are there any rules governing the right of access to archives and records?
- Is there any system for accessing administrative documentation through the internet by users external to the administration, such as citizens or companies? And by other administrations in the country, if any?
- Is there a regulation governing digital means of identification, the use of electronic certificates, signature, etc.?
- Do you have systems for logbook management, logbook user and permissions management, data catalog management, log number generation, internal and external referral generation, and receipt and stamp generation?
- Is there traceability in the records?



2.10

National digital archive



One of the most noteworthy characteristics of e-administration is that it is a more open and accessible administration, since it is available 24-7-365 and from anywhere. However, the objective to be achieved should not be limited to the use of new technologies, but should be to offer citizens a higher quality and more proximity administration. To this end, it is essential for the administration to be more transparent and to have a good regulatory base on which to rely.

Thus, the administration should not only seek to facilitate the electronic processing of administrative procedures, but should go further by simplifying the latter and publishing electronically and *motu proprio* information of interest to citizens. In addition, it must facilitate access to public information, understood as the contents or documents, whatever their format or support, held by any administration or public office and which have been prepared or acquired in the exercise of its functions. This information shall be provided in an agile and simple manner, and to this end, the use of new technologies is essential.

THE REGULATORY RECOGNITION OF THE RIGHTS THAT PEOPLE ENJOY IN THEIR RELATIONSHIP WITH THE ADMINISTRATION AND THE GUARANTEE THAT THIS LINK IS ELECTRONIC IMPROVES THE PERCEPTION OF PUBLIC SERVICE AND HIGHLIGHTS THAT THE CENTRAL AXIS OF THE ADMINISTRATION IS THE CITIZENRY. A CITIZENRY THAT DEMANDS A DIGITAL ADMINISTRATION.

The right of access to public information is an essential pillar for the citizen to perceive the administration as transparent and of quality. This right is embodied in the access to public records and files, so its regulation is of vital importance.

WHAT IS AN ARCHIVE?

In general and based on existing regulations, an archive can be defined as a place where various types of documents are stored, but also as the documents that are kept in these spaces.

A more complete definition is that archives are organic sets of documents or the collection of several of them, compiled by individuals or legal entities, public or private, in the exercise of their activities, preserved and organized in a certain way and at the service of their use for research, culture, consultation, and public information and administrative management. Likewise, archives are understood to be all those institutions where documents are gathered, preserved, and disseminated for the aforementioned purposes.

KEY ASPECTS TO REGULATE THE OPERATION OF THE ARCHIVE

- **Collect the documentation** (i.e., the archivist processes the entry of the documents into the archive).
- **Preserve documentation,** which follows two principles:
  - Security of facilities, backups and accesses, as well as custodial security.
  - Order, understood in its broadest sense as organization, classification, and arrangement by known criteria.
- **Serving documentation,** which consists of providing the information contained in the archives. This service may be offered to
  - the producing agency;
  - a specialized direct consultant (researcher);
  - the general public.

These functions should be performed regardless of whether the archive is paper or electronic, and should be provided for in the legislation.

WHAT TO FILE?

One of the main tasks that needs to be carried out before documents enter the archive is to decide what should be retained, and to this end it is essential that the legislation clarifies how this decision is made and which body should make it. It is also necessary to indicate when the documents will enter the archive.

The regulations generally state that not all documents in administrative offices should be filed. Thus, there are two types of documentation:

- Supporting informative documentation, which is not part of the archive.
- The documentation that is part of the archive (i.e., those documents that are produced in the course of the administrative unit's activity and that in any case will access the archive when the procedure has been completed).

AN ELECTRONIC DOCUMENT IS MORE THAN AN IMAGE

One of the first actions in the transformation of archives was their digitization. This is already contemplated in the regulations of several countries due to the numerous advantages in terms of access by citizens, particularly in terms of speed, simplicity, and agility. It also highlights the possibility of creating copies or working with documents more securely and efficiently without losing or damaging the original documents.

However, the digitization process should not only be limited to capturing the image of the documents contained in the archives. To be able to think of true electronic documents, it is necessary to assign metadata to them. However, the administrations of many countries have even gone a step further and have moved on to the production of public administrative documents, establishing in their legislation the characteristics that these documents must have in order to be considered valid. They should:

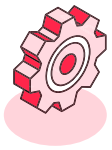
- be issued by the bodies of the public administrations in writing and through electronic means, unless their nature requires another more appropriate form of expression and record;
- have identification data that allow their individualization, without prejudice to their possible incorporation into an electronic file;
- incorporate the date of issuance;

- incorporate minimum metadata;
- incorporate electronic signature or signatures, or the electronic seal of the issuing body;
- contain information of any nature stored in an electronic medium.

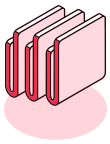
These documents by themselves constitute administrative information, and their production by bodies and offices is massive, but most documents become relevant when they are part of an administrative record—in this case, of an electronic administrative record.

The latter must also be regulated in specific provisions for each country, since the bulk of public archives are administrative records. It is therefore vitally important to have an electronic administrative archive with a regulatory basis that allows for the proper archiving of electronic administrative documents and records. This must respect the life cycle of the documents, particularly in the so-called "conservation and selection" phase for, as appropriate, archiving or destruction.

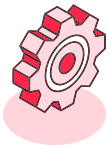
TYPES OF ADMINISTRATIVE RECORDS



Management archive



Central or general file

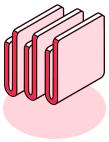


Management archive

- This is where the documentation is kept while it is still being processed or is of very frequent use, and it has to provide service to the producing administration and to the citizens. Therefore, its organization is part of the work of the administrative unit or office itself. In this case, the administrative file is in its opening and processing or even formal closing phases, but has not moved on to the conservation and selection phase. Some key aspects for this file are the following:
  - To have a document and file management software program that facilitates the daily work of public employees by uploading the documentation generated by the office. The design

of this program should be based on adequate regulations, both in terms of definitions and technical aspects, detailing the metadata of documents and files and the document management policy, among other aspects.

- This file should be accessible to citizens and/or companies in a controlled manner from the electronic headquarters, virtual office, or similar office. In this way, it would be possible that interested parties consult the processing status of the procedures in which they are involved, as well as the documents submitted by the citizens and/or companies and issued by the administration. This access is of vital importance in the comparison of copies of electronic or digitized documents, both in paper and electronic format, as it will allow the authenticity of the copy to be checked by accessing the public website of the electronic files of the issuing public body or agency. Likewise, for the comparison of paper copies, this check will be made by entering an electronically generated code or through another verification system that allows access to the file.



Central or general file

› Here are kept the documents of proceedings already completed in which there is a final resolution. The regulations in this case must establish the following:

- That all administrations have a single archive of electronic documents corresponding to all completed procedures. However, in this regard, it should be noted that the creation of this single electronic archive will be compatible with the various archival systems and networks in place, and in particular with the continuity of national, central, and/or federal historical archives. The administrations may therefore choose to create a single electronic archive themselves that is interoperable (at least in consultation) with those of the other administrations, or to adopt the same solution as the central, national, or federal administration.

- That all documents used in administrative proceedings are stored electronically, except when this is not possible.

- The format for preserving electronic documents, with a view to guaranteeing their authenticity, integrity, and preservation, as well as their consultation regardless of the time elapsed since their issuance. However, the possibility of transferring the data to other formats and supports that guarantee access from different applications and over time can be contemplated, which is already included in the technical regulations developed by

the most advanced countries in this field. Therefore, electronic documents must be kept in electronic media, either in the same format from which the document originated or in any other format that ensures the identity, integrity, and longevity of the information needed to reproduce it.

- The way to eliminate electronic documents, although authorized with the provisions indicated in the legislation itself.

- The media or supports in which documents are stored must have cybersecurity measures that guarantee the authenticity, confidentiality, integrity, availability, traceability, and conservation of the stored documents. In particular, they must ensure the identification of users and access control, as well as compliance with the guarantees provided for in data protection legislation, and also the recovery and long-term preservation of electronic documents produced by public administrations that so require, in accordance with the specifications adopted on the life cycle of the services and systems used.

All the aforementioned characteristics of the electronic archive are fundamental and essential for its proper functioning. Therefore, prior to the implementation of such an archive, it will be necessary to evaluate the regulations governing the archive, if they exist, and adapt them to the objectives and characteristics mentioned above in order to provide its electronic support with an adequate regulatory framework.

ASPECTS TO BE TAKEN INTO ACCOUNT WHEN LEGISLATING ELECTRONIC ARCHIVING

- Legally recognize the right of citizens to access public information in an agile, rapid, and transparent manner. This can only be limited for reasons provided for in legislation such as national security, foreign relations, or data protection.

- It also recognizes the right of citizens to interact electronically with the administration. In this way, the right of access in digital form to exercise several other rights—for example, to do the following:

  - obtain public information

  - consult and make allegations

  - formulate requests

  - manifest consent

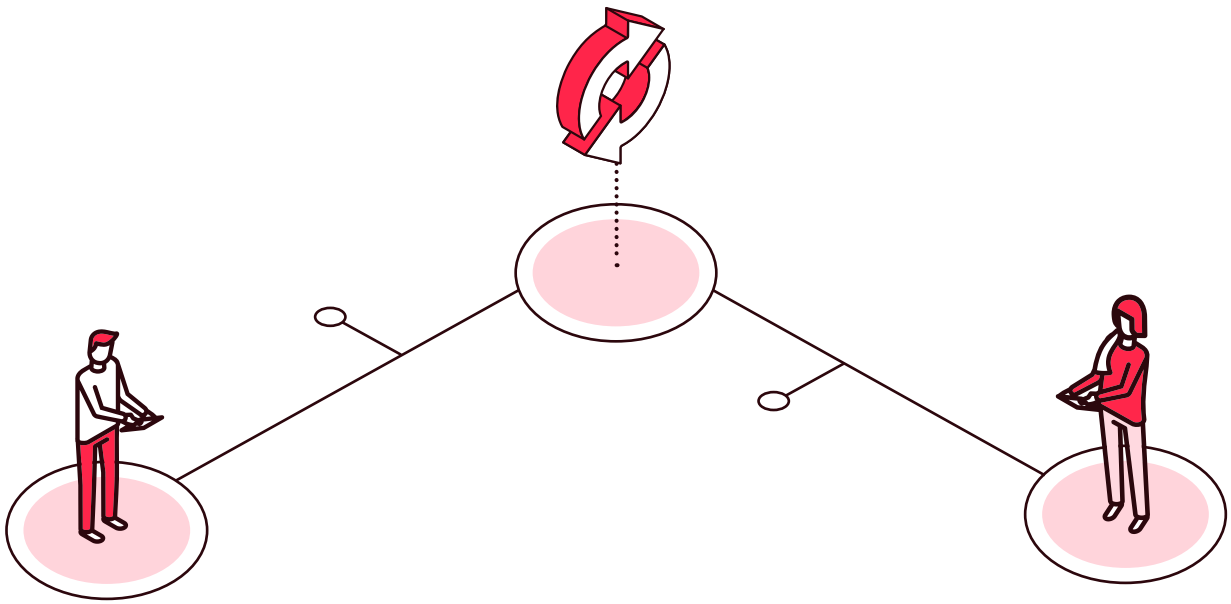
- establish claims
- make payments
- perform transactions
- oppose administrative resolutions and acts, among others

- It should also be recognized that the interested parties have the right not to provide documents that are already in the possession of the administration with which they are going to interact or that have been prepared by any other administration, unless the interested party objects, thus reducing the number of documents to be provided in the files and to be digitalized, if applicable.

- It is essential to have an adequate electronic document management policy that contains the guidelines defined by the administration for the creation and management of authentic, reliable, and available public documents throughout the life cycle of these media. It is important that this policy be based on best practices and consolidated national and international standards.

- A common archiving policy is needed to enable administrations to ensure the long-term preservation of electronic documentation within an appropriate legal framework.

- Automate, as far as possible, the process of electronic archiving of documents once the procedure has been completed. In any case, the authenticity, integrity, and preservation of the documents must be guaranteed.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Vice minister of health
Sara

Sara arrived at the Ministry of Health thinking that she would have a defined file as it happens on paper, but this is not the case. The public employees tell her that they have lost citizens' data that they had on paper due to a flood and that they were not digitized. Sara is going to digitize the most recent paper files and create an electronic document management policy.

Citizen
Camilo

Camilo wants to apply for a scholarship, and to do so he has to provide a large amount of documentation that he has to request well in advance. He does not understand how he cannot access this documentation digitally so that he can provide it or simply tell the administration that they already have this information.

Entrepreneur
Ana

Ana is happy that in her country she is allowed to access digitized information from the national historical archives, but she does not understand why the same is not true for the documents that her company has submitted to the city council in recent years. Every time she wants to access such information, she has to go to the office in person.

EXAMPLES

Click on each flag or icon to go deeper

Europe
European Archives Portal

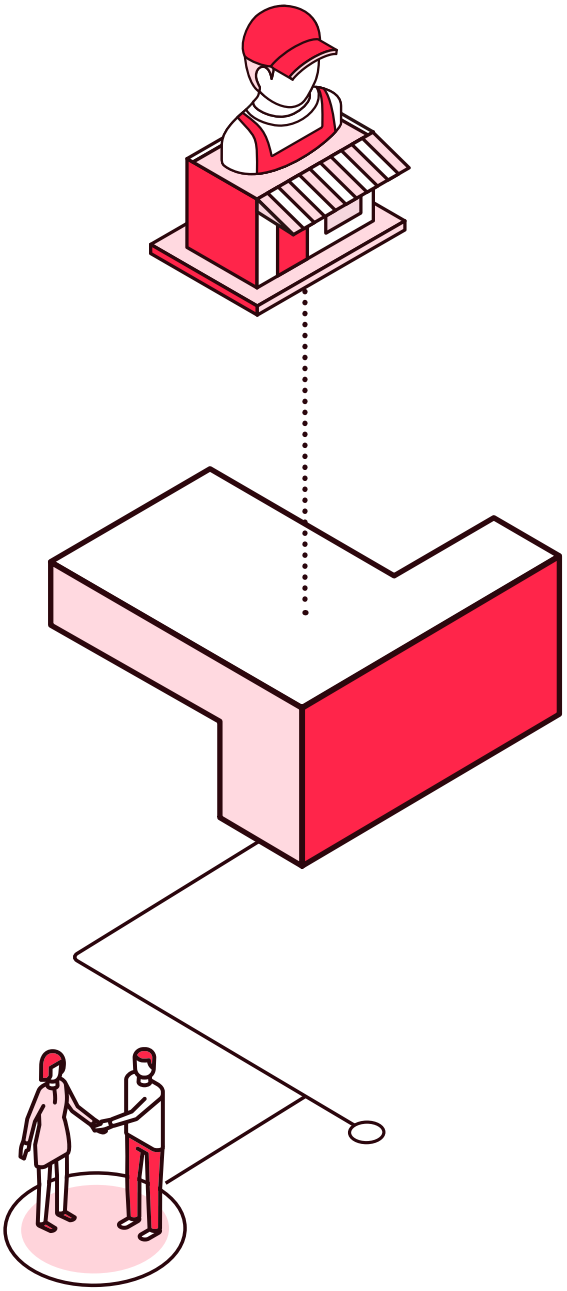
Spain
e-Archiving Strategy and Electronic Document Management Polic

Internacionals
Norms (standards) and best practices on document management, document retention, and other procedures.

INDICATORS

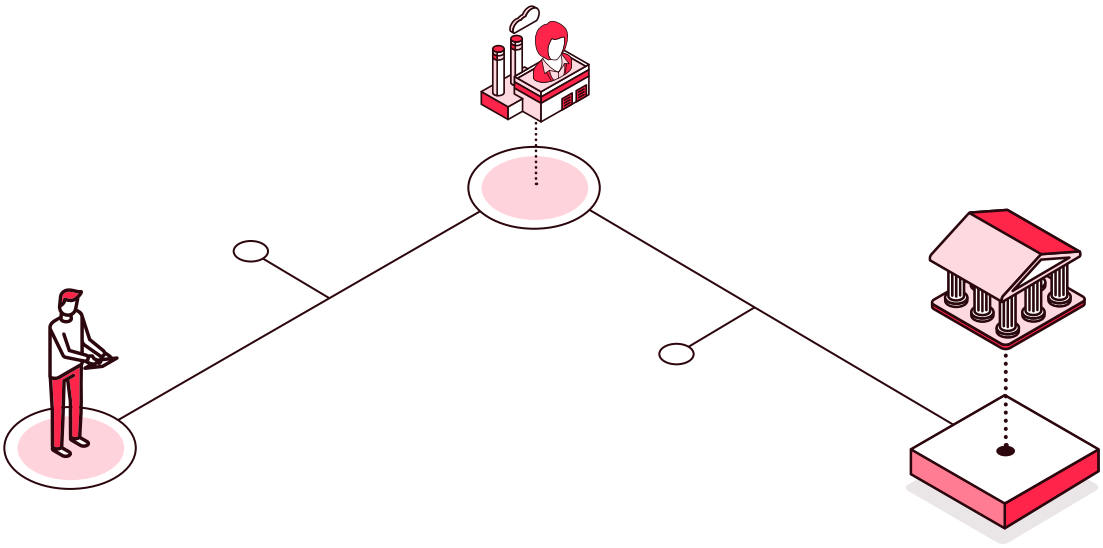
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there any rules governing the right of access to archives and records?
- Are there any rules governing the archiving of administrative documents?
- Is there any reference in these regulations to an electronic or digital file?
- Is there any regulation that allows or contemplates the digitization of administrative records?
- Is there a document and/or electronic records management policy?
- Is there an archival management system for electronic documents?
- Is there any possibility of digital access to the archives by citizens and/or companies?
- Is there an interadministrative information exchange system?



2.11

Administrative directories



Among the important challenges involved in a country's digital transformation, one of the most complex is interoperability (i.e., the ability of public administrations to work together efficiently). The first step in this regard is the definition of a common language (i.e., a reference framework in which the main guidelines for exchanging information between different agencies are established). In this context, administrative directories play a key role.

Administrative directories are catalogs of information relating to fundamental and reference elements necessary for the operations of public bodies. In the same way that a company has its master data (customers, products, suppliers, etc.), public administrations require their own master data to identify and organize administrative management and production (organizations, citizens, companies, etc.).

Administrative directories provide a univocal and common relation of the most important information elements in public operations, and their importance lies in the fact that they allow the administration to

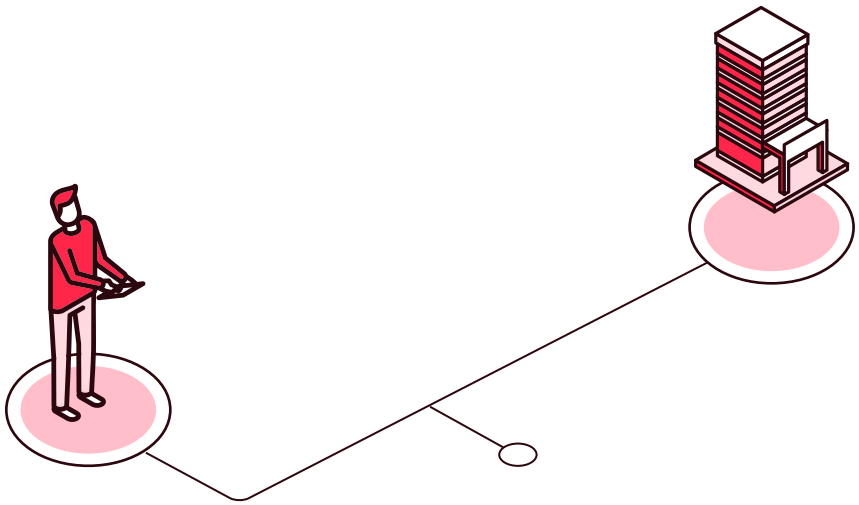
- adequately and automatically configure the information systems that manage procedures or services in their different phases or approaches: information dissemination, telematic submission of applications, file processing, archiving and document management;
- provide information to citizens;
- interoperate with other administrations.

WHAT IS INCLUDED IN AN ADMINISTRATIVE DIRECTORY?

Without intending to be exhaustive, some of the most common administrative directories include the following information:

- the relationship between public agencies, public institutions, and governmental companies
- the administrative units that comprise it
- offices, buildings, physical infrastructure, and other public spaces
- administrative procedures, formalities, and public services in general
- administrative rules and legislation
- administrative directories related to citizenship: directory of citizens, companies, taxpayers, etc.
- authorizations and administrative representations
- list of contractors
- collegiate bodies

Depending on the specific competencies of each country, the directories may also include relevant information on the territory, such as toponymies, maps, urban references, cartography, roads, transport infrastructures, geographic areas, etc.



MAIN ADVANTAGES OF ADMINISTRATIVE DIRECTORIES

- They establish a *common frame of reference* that enables interoperability between different agencies. If a file is sent with agency code XYZ1234 and process code ACB9876, any entity can automatically and unequivocally interpret the subject and origin of the matter.

- They allow the *automation of information processing.* Computer systems require codes to be able to interpret data and documents. This makes it possible to adequately and automatically configure the information systems that manage procedures, formalities, and services.

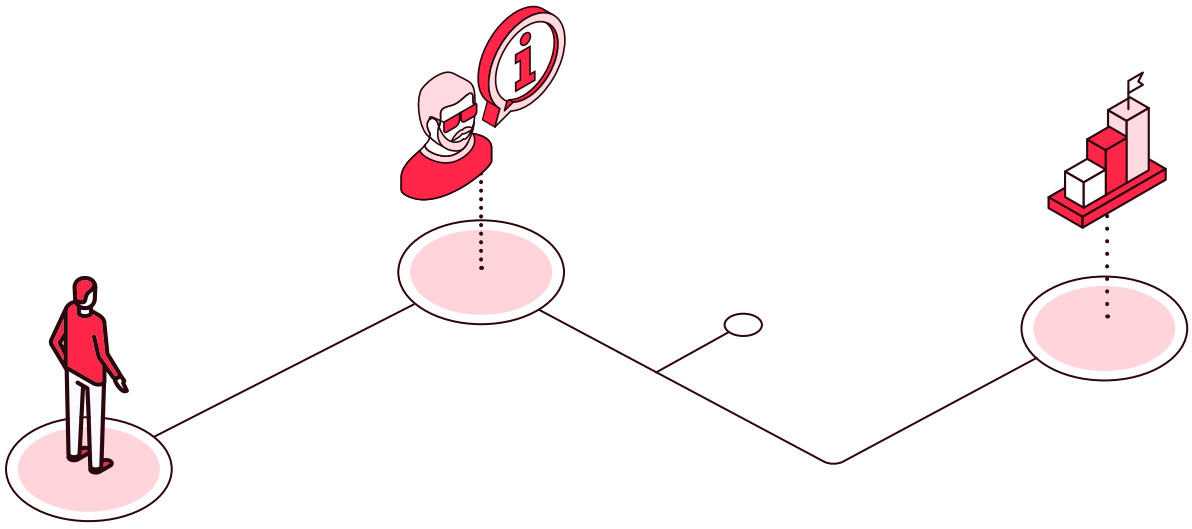
- *They consolidate information from different* sources and establish operating rules to keep it up to date.

- They allow for *maintaining historical information* and traceability.

- They *strengthen citizen services* by facilitating the dissemination of fundamental information to better interpret the administrative activity of citizens.

- They *reduce costs* by unifying information management criteria and reducing data conversions between different schemas, formats, and standards.

- They facilitate the *reuse of information* from public administrations and transparency.



MAIN ELEMENTS TO BE CONSIDERED IN THE REGULATION OF ADMINISTRATIVE DIRECTORIES

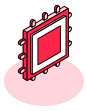
For a truly efficient management of these instruments, it is not enough to define and create them, but it is necessary to establish the criteria for their use and specify how these information catalogs are to be shared, so that they can constitute a single, common working framework. Hence the need for legislation.

To this end, it is advisable to establish these directories and the obligatory nature of their use by means of a regulation of higher rank (such as a law or decree), which will provide them with legitimacy and promotion, while it is more convenient to develop their structure and operation in a regulation of a more instrumental nature, such as a technical regulation, which can be modified over the course of the year and which can be complemented with user guides or application instructions.

The main elements to be taken into account when developing regulations for administrative directories are:

Identify the ownership of the board of directors

The governance model of the board itself



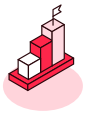
Directory information architecture

Mandatory provision of information or its use

Technical management tools and instruments

Information provision model

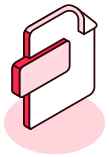
Information consumption model



Evolution of directory information

Regime of privacy, confidentiality, and protection of personal data

Other aspects of directory management



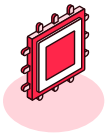
Identify the ownership of the board of directors

That is, determine who is responsible for its management. In this regard, there are two frequent cases:

- One in which the information is centralized and depends on a single institution.
  - *Example:* All companies in a country may be listed in an official register, in which case the ownership of the business directory could be vested in the competent body.
- One in which there is no single source, and the directory must become an aggregator of information.
  - *Example:* Lists of offices or physical locations of public administrations, where each of them must report their own. In this case, it is necessary to delegate to a body in charge of their management.

The governance model of the board itself

That is, who modifies the policies and practices of use and how. Roles and responsibilities for management should be identified. Who is in charge of managing the IT system, providing support, reviewing quality (avoiding information obsolescence), providing information, etc.



Directory information architecture

Includes the attributes, data, or metadata to be managed. In this section it is advisable to be very detailed, specifying for each attribute information such as the type of data, its length, its obligatory nature, and its possible values when it is a closed taxonomy (for example, defining the priority levels of a service, these could be “high,” “medium,” and “low”).

- *Example:* If a list of all offices, buildings, and physical infrastructures of public administrations is developed, it will be necessary to include information such as address, geolocation, purpose, ownership, service hours, and whether or not they serve the public.

Mandatory provision of information or its use

If any, as well as the conditions or cases in which it is permitted.

Technical management tools and instruments

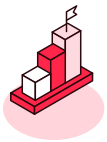
Such as computerized management systems or integration services.

Information provision model

That is, what are the sources of information in the directory and how is the data provided (through what protocols, with what processes, frequency, etc.)? Is it information generated by a single agency (e.g., if there is an official business register at the national level) or does it originate from several different ones (administrative procedures)? Is it possible to feed the directory automatically, or should it be a manual register?

Information consumption model

Which involves identifying the permitted use of the information, as well as the protocols, procedures, and technologies (centralized computer systems or through integration by the information consumers' systems) to obtain it, security conditions, etc.



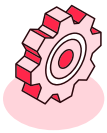
Evolution of directory information

This is one of the most complex issues to manage.

- *Example:* If you have a Ministry of Commerce, Industry, and Tourism and an organizational change causes it to split into two different ministries, how do you change all the references? Should the original one be deactivated and two new ones created? Or should one of the two keep the coding of the previous one?

Regime of privacy, confidentiality, and protection of personal data

As well as conditions of disclosure and transparency, if any.



Other aspects of directory management

Which may include security model, auditing of directory usage, or quality controls, among others.

GUIDELINES FOR USE

On the other hand, it is also advisable to establish technical and technological guidelines and standards to facilitate the use of the directories and the exchange of information based on them. In general, these guidelines include topics such as the following:

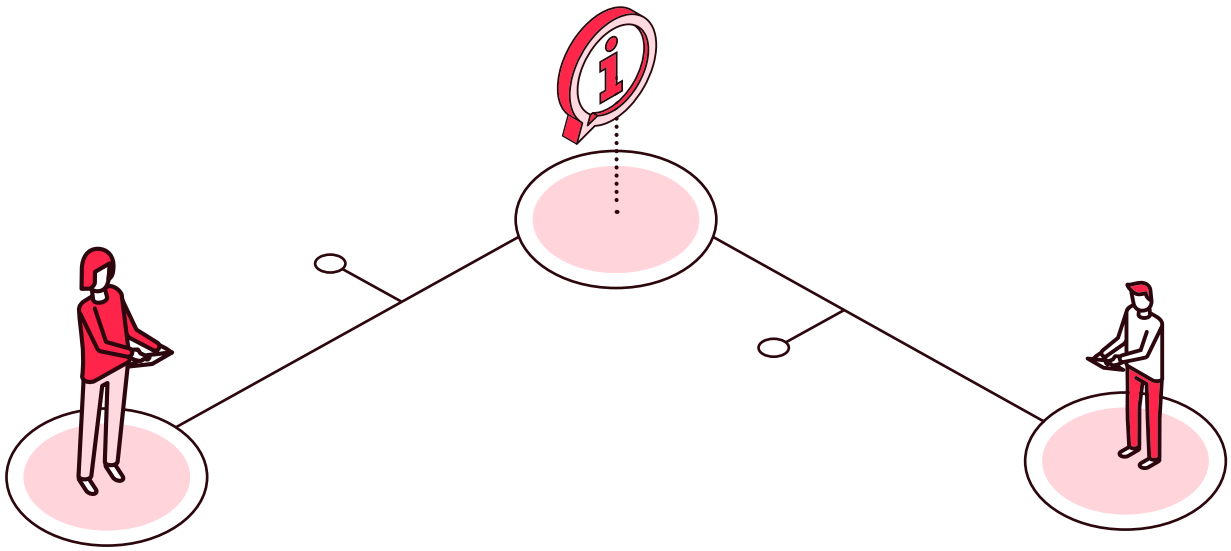
- **security measures required,** including methods of identification and authentication of users or connections, need for encryption of information, credential exchanges, etc.
- **communication requirements,** such as connection through limited access networks.
- **information exchange protocols,** specifying messaging, sequences, services, technology, etc.
- **exceptions and errors handled,** as well as their coding and meaning.
- **information exchange schemas,** including xml schemas or implementation examples.
- **standards, ontologies,** vocabularies or other common specifications used.

IT IS ALSO NECESSARY TO TAKE INTO CONSIDERATION THE RELATIONSHIP THAT MAY EXIST BETWEEN ADMINISTRATIVE DIRECTORIES AND OTHER INSTRUMENTS THAT CATALOG INFORMATION, SUCH AS STANDARDS AND TAXONOMIES (POSTAL CODES, COUNTRY CODES, MUNICIPALITY CODES, ETC.).

Specific legislation on administrative directories is desirable because of the need for unique, clear, and detailed interoperability protocols that eliminate possible uncertainties as to whether or not to adopt one standard or coding system over another.

The great challenge in this whole process is to properly identify the main administrative directories required by a country's digital transformation and to establish the interadministrative commitments and technical consensus that will make it possible to have quality, relevant, real-time, and user-friendly records. The idea is for these tools to become a useful and practical information asset when exchanging information between two administrations that operate independently.

Administrative directories are the fundamental pillars on which a complete interoperability framework is built and, therefore, the backbone of the true transformation of a country's administrative model. Otherwise, we will see a huge effort that will result in the automation of a set of isolated institutions, and not the comprehensive digital transformation demanded by citizens as a whole.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Mayor's advisor
Daniel

Daniel wants to modernize the processing of urban reform permits. He knows that the main problem is the time spent reviewing the region's urban plans, which are received on paper and checked manually, but he has asked the regional body to pass on the information digitally. However, he has found that his technicians tell him that the systems are incompatible because the municipality has its own system of urban planning references and they cannot establish equivalences between one set of references and another.

EXAMPLES

Click on each flag or icon to go deeper

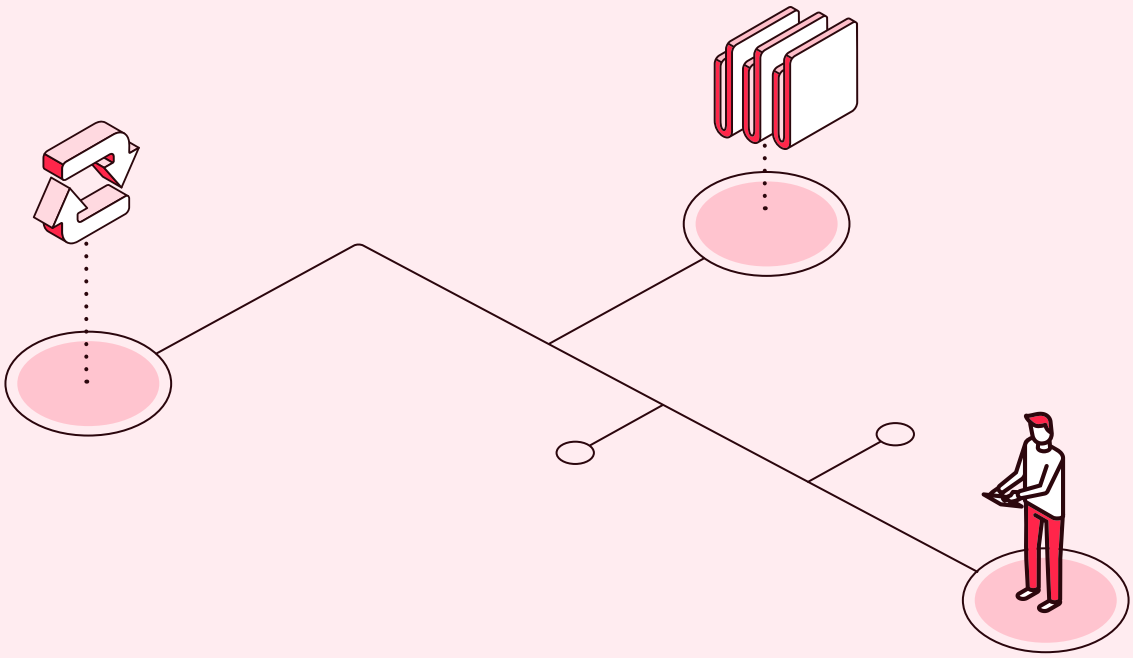
Australia
Australian Government administrative directories.

Spain
Common Directory of Organic Units and Offices (DIR3).

Mexico
Organizational Structure of the Agencia Digital de Innovación Publica.

Spain
Royal Decree 4/2010, of January 8, 2010, regulating the National Interoperability Scheme in the field of Electronic Administration, which establishes some directories:

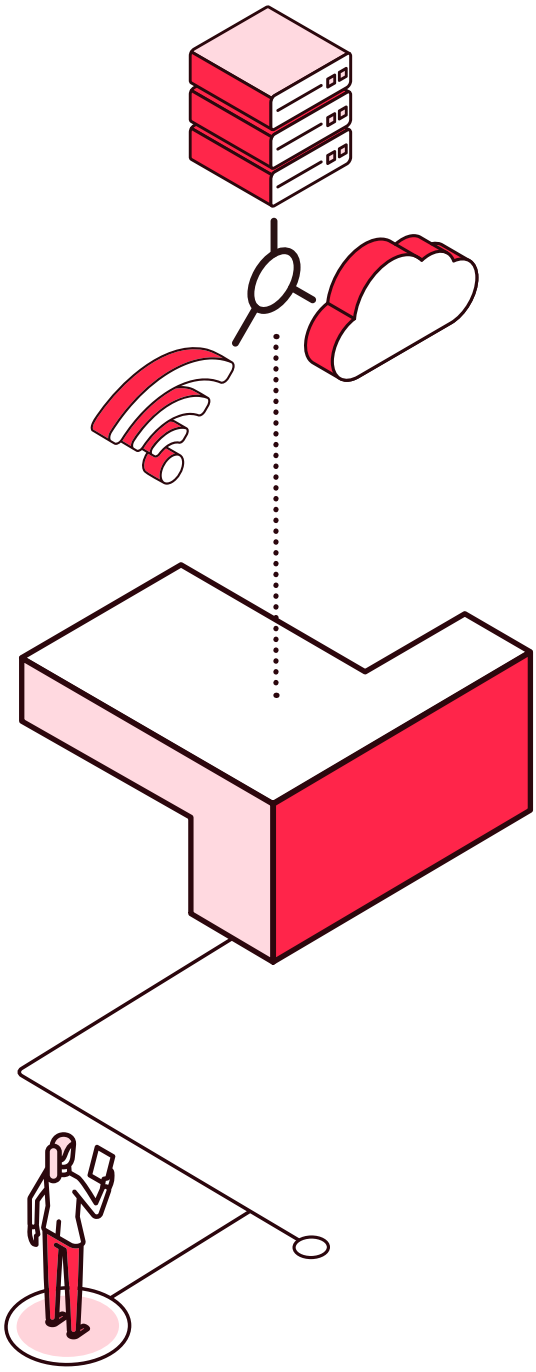
- Inventories of administrative information (article 9)
- Directories of reusable applications (article 17)



INDICATORS

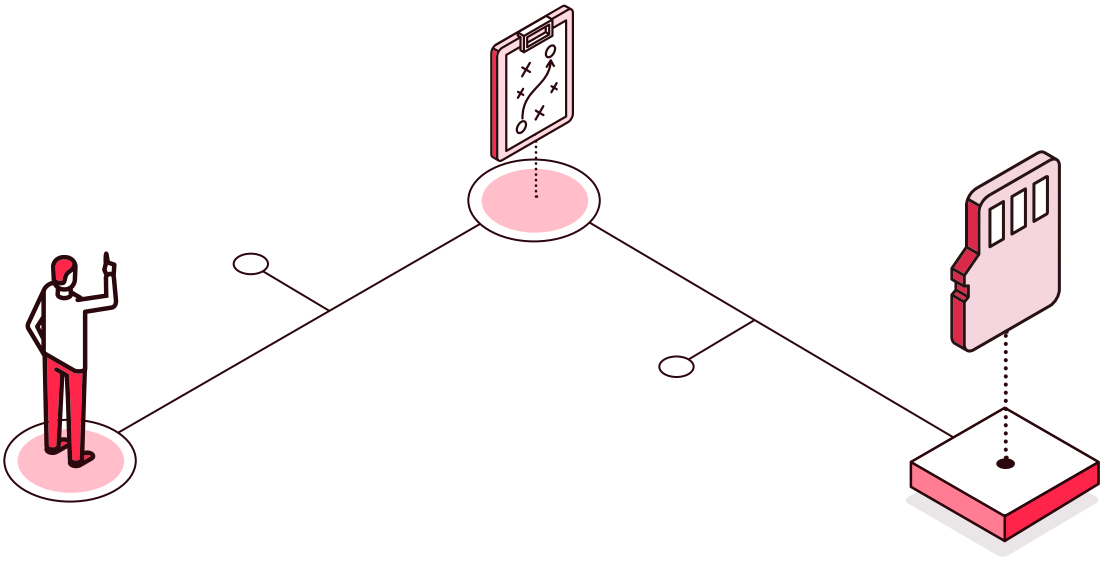
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a directory with all the public agencies in the country?
- Is there a directory of all administrative procedures, formalities, and public services?
- Is there an administrative directory for the exchange of administrative information?
- Is there an interadministrative information exchange system?
- Is there any standard to unify the coding systems used by public agencies?



2.12

Data



A coordinated and holistic strategy and an overall regulatory framework for data governance in the country is essential for public entities and companies to take advantage of the benefits that data offers in a knowledge-centered society and to enjoy the benefits of the Fourth Industrial Revolution.

Such a national data strategy involves broadening the traditional view of data, which focuses on its value in terms of transparency and accountability, and focusing on its potential impact in terms of economic growth, public innovation, and social inclusion. This strategy is more novel and complex and is often less developed than other more classic strategies, but it is fundamental for the country as a whole to unleash the full potential associated with digital technologies, and to effectively harness the use of data.

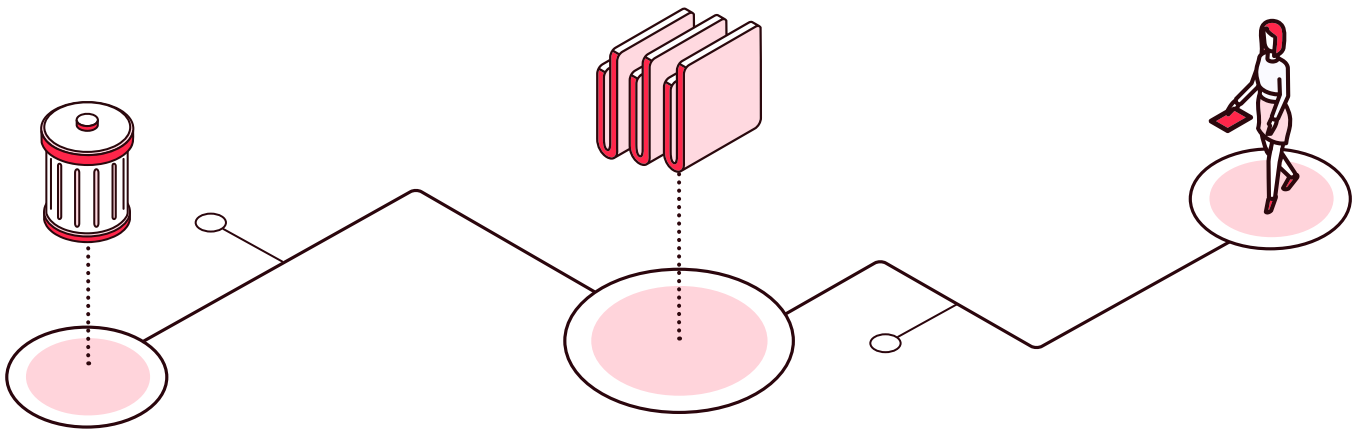
In addition, this national strategy must be understood not only as the set of legal regulations that must be created to provide the necessary support, but also as the accumulation of semantic or technical regulations that must be created in order to be able to treat such data in a homogeneous and uniform manner. For example, the legal regulations associated with the use of data would be those related to data protection, open data, access to classified information, categorization, and levels of access to data. From a semantic point of view, it will be extremely important, for example, to have regulations on data structures for their possible exchange and exploitation, and from a technical point of view, it will be crucial to have regulations such as interfaces for connections to interoperability systems.

DATA REGULATIONS SHOULD BE UNDERSTOOD AS THE WHOLE SET OF REGULATIONS AT DIFFERENT LEVELS THAT, IN THEIR DIFFERENT DIMENSIONS, CONTRIBUTE TO THE USE, EXPLOITATION, AND EXCHANGE OF PUBLIC ADMINISTRATION DATA IN AN ORDERLY MANNER AND WITH CLEAR RULES FOR ALL ORGANIZATIONS.

It should not be forgotten that one of the most important aspects in regulating the use of data are the last stages of the data life cycle, archiving and destruction. In fact, the rules for long-term archiving or expurgation of data, in each area of application of the administration, will require a regulatory pyramid in itself.

This set of homogeneous data regulations will therefore make it possible for data from any government agency to be used in the same way when interoperating or exploiting them for any purpose. In fact, one of the most valuable purposes for public administrations is to be able to exploit information from different origins for statistical purposes, in order to improve the efficiency of public services. To this end, data must be obtained and processed on the basis of the same legal, semantic, and technical rules.

The value of data is indisputable. Public institutions must regulate the promotion of innovation that is enabled by the greater availability of information, but also ensuring its proper use and security, and protecting the sensitive data of individuals. Although the opening of data is important to generate public value, there are certain exceptions when fundamental rights of individuals are violated and/or for national security reasons. In this sense, concepts related to data protection, inclusion, quality, responsible use, and security become essential issues.



A MATTER OF PERSPECTIVE: HORIZONTAL OR VERTICAL

Data issues, such as open data, use and reuse, access to public information, personal data protection, artificial intelligence, and others, are generally more novel than traditional areas of public management. Therefore, from the outset, they are raised as horizontal issues to the sectors that traditionally make up the vertical silos. A comprehensive data strategy should have the appropriate regulations and governance in place to try to overcome the problems of the vertical or siloed view of sectors, and to ensure that the treatment of data is homogeneous.

Thus, for example, the regulation of transparency and access to public information affects all sectors in general, and the institution responsible for its enforcement is transversal to all of them. This regulation and an institution in charge of enforcing it should exist for the rest of the aforementioned issues.

While this has been beneficial because from the beginning it has transcended the existence of vertical silos (imagine how complicated it would be to have one transparency regulation and standard for the education sector, another for commerce, another for industry, and so on), "horizontal silos" have appeared, and it is not uncommon to find transparency regulations that, for example, clash with principles of personal data protection. There may also be data policies that do not contemplate the responsible use of disruptive technologies that use data as an input (e.g., artificial intelligence).

For this reason, a comprehensive strategy is needed at the national level, as well as the associated set of regulations to support the improved use of data to generate value. This strategy, as well as the regulations, must ensure that there is a compatible criterion among the different parties responsible for data-related aspects and that it ensures an orderly operation, avoiding contradictory regulations and making effective use of the data available in a country.

KEYS TO DEVELOPING A COMPREHENSIVE DATA MANAGEMENT STRATEGY

In general, the design of such a strategy is quite new or, in many countries, nonexistent: there is no associated comprehensive strategy that regulates the management and processing of data and encourages its use by the entire digital ecosystem. This creates a problem because it is common to find some of the key elements already in place that should be included in the strategy. It is normal for countries to already have a policy and body responsible for transparency and openness of public data, or data protection, for example.

THE DATA STRATEGY MUST BE ACTION ORIENTED AND AS DYNAMIC AS THE SUBJECT IT DEALS WITH; THAT IS, THE SPEED AND AGILITY IN THE IMPLEMENTATION OF THE RESULTING ACTIONS MUST BE EQUAL TO THE CAPACITY TO REVISE AND UPDATE THIS STRATEGY.

A national data strategy that addresses the above concepts should have three key dimensions:

Data management governance. This will define the rules of the game, including the institutional arrangement and allocation of responsibilities throughout the life cycle of a piece of data.

Talent and digital skills. This will include building the skills necessary for the generation, analysis, and utilization of data, inside and outside of government.

Promoting responsible data use. This will promote and generate spaces for the creation and application of innovative solutions to existing problems.

Data management governance

The implementation of governance is key to the sustainability of the data strategy and the development of a dynamic ecosystem that generates value through the use and reuse of data. Governance will determine—at the national level and at the organizational level—the manner and processes that will be followed in order to make decisions about data. At the national level, as part of this governance, a new data manager should be created or assigned to an existing institution with the objective of enhancing the country's data strategy in a comprehensive manner, ensuring its proper use and security, and protecting the sensitive data of individuals. This officer should have a clear mandate and competencies, as well as implementation capacity, to ensure that his or her mission is differentiated from that of other actors in the same data space, such as those responsible for transparency or data protection.

Likewise, this governance, as it cannot be otherwise, must be reflected in an appropriate regulation. This includes not only its composition, but also the powers and decisions that the legislation recognizes as its responsibility, as well as the level of bindingness for the bodies of the resolutions issued.

In general, a data governance program should include, among others,[26]

- compliance monitoring mechanisms;
- strategy—at the national level and eventually at the organizational level;
- policies—within the public administration and, as mentioned above, at the national level through appropriate regulations;
- standards and quality—definition of data standards and data quality control processes;
- assignment of responsibilities within organizations and for all data flows;
- follow-up on strategic implementation projects, including, among others, the definition of interinstitutional, sectoral, and/or interoperability data dictionaries.

In addition to the institutional arrangement, it will also be necessary to adjust the regulation, in terms of personal data protection, open data, transparency, etc., in order to have a data-related legislation that is consistent, and that allows the maximum use of the data. In the event that such legislation does not exist, the possibility of creating it from scratch is open, ensuring consistency from its initial drafting.

It is essential to emphasize the implementation of the strategy, to prevent it from remaining as a piece of paper in a drawer. In other words, one of the key aspects of governance is also the launching of implementation projects, their follow-up, and coordination among all of them to ensure that the objectives established in the strategy are achieved. To achieve this, it is very useful to have some of the following lines of work:

- Ontological and Semantic Data Definition Working Groups. In fact, this is possibly one of the most important technical actions, and one that must be governed with great care. The description, grouping, and semantic definition of the data to be handled are essential when thinking about a holistic digital government. It would not otherwise be possible to think of automated interoperability and distribution of information if it is not properly structured and such

26. Taken from DAMA (2018).

schemes are not known by the parties involved. Nor would it be feasible to manage reliable and unified statistics, and of course, it would not be able to contribute to strategic decision scorecards. In addition, having the data described in this way can enrich the electronic files and documents established for government interoperability and thus make the exchange of these between institutions much richer because the content of these could be understood in an automated way. That is to say, it is not the same that an organization A receives a file from an organization B that cannot be interpreted beyond the basic information provided such as file number, name of the issuer, citizens involved, among other variables, compared to an scenario in which the institution knows how to automate all the information and data contained in the file because the semantic structures known by both parties.

- Working Group for Follow-up, Coordination, and Control of Implementation Projects. On the other hand, it is important to highlight that governance should also work with the follow-up of the projects of the different agencies that are in the implementation phase of the data strategy. The governance and coordination between them will undoubtedly make the implementation have many more and better synergies and therefore, better results. Other projects, such as the implementation of the digital file or connections with interoperability platforms, will directly benefit from these data strategy implementation projects and, therefore, from the definition and ontological and semantic description of the data.

- Coordination meetings of key stakeholders. It is crucial that data be described and defined from an ontological, semantic, and technical point of view with a clear and simple objective: to maximize its use and, therefore, its benefits. To achieve this, it is essential to have the input of those stakeholders who stand to gain the most from well-structured and well-defined data. Detailed knowledge of each of the sectors will greatly enrich the definition of the data, as well as the attributes and metadata associated with it. Some of these key players are the following:

    - interoperability working groups
    - statistics departments
    - transparency and open-data departments
    - strategic decision-making cabinets

Talent and digital skills

Any sound national data strategy must take into account the digital talent and skills pillar both inside and outside of government. This means including programs ranging from formal education to lifelong learning (*boot camps*, online courses, targeted training courses, among others) aimed at addressing the need for data-related skills across the economy.

In addition, data-linked talent should be redefined to encompass more than just data scientists: data privacy experts, evidence-based policy makers, technology experts, among others, should also be assigned as data-related professions.

Promoting responsible data use

A comprehensive strategy must encourage the use of data in a responsible and impactful way. To this end, it is essential to focus on issues such as data quality and standardization, and the responsible use of data through emerging disruptive technologies.

A relevant aspect is the application of artificial intelligence to public and private data. A comprehensive data strategy must enable the exploitation of this technology, because of the important benefits it brings in fields such as

- clinical diagnosis.
- automated administrative processing.
- the streamlining of judicial processes.

These powerful capabilities and fields of action, however, coexist with great dangers in the case of misuse. Therefore, an ethical use of artificial intelligence and of the data on which these solutions are based must be ensured, controlling the automatic decision-making by algorithms, as well as avoiding the generation of citizen profiles or control mechanisms, both public and private, that violate the fundamental rights of citizens.

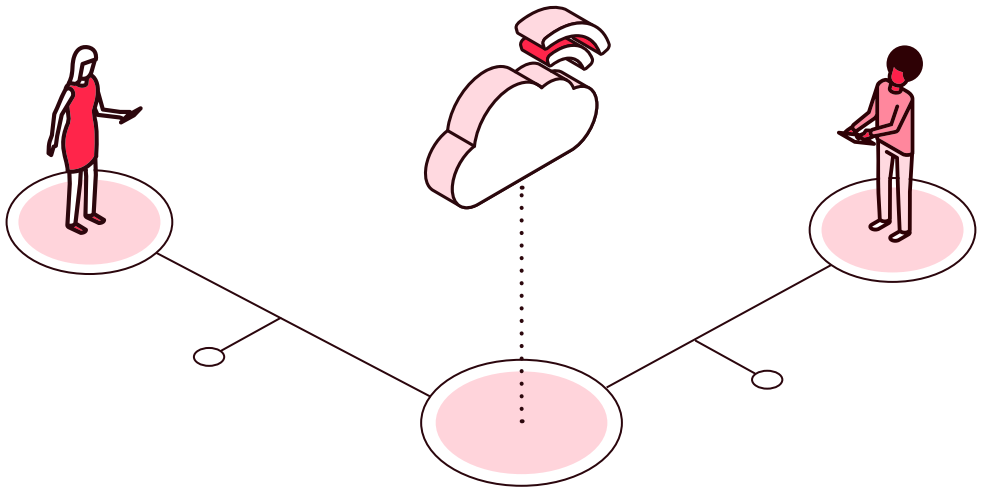
Coordination

To encourage the use of data, regulations must also be aligned with all initiatives in the digital ecosystem, including the private sector. This implies the creation of common master tables and metadata, for both public entities and companies, that enable

- Automated processing;
- Processes that enable automatic information exchanges throughout the country and/or the generation of baseline records (e.g., unique agency codes, standardization of metadata).

This is especially important since this coordination and standardization can simplify all interaction, both of citizens and businesses with public institutions and between each actor and their peers. In this case, it is not artificial intelligence, but automated processing based on data and rules, which facilitates the country's maximum effectiveness and competitiveness by enabling automatic and proactive procedures.

Lastly, the importance of this data, open data, reuse, and other strategies is emphasized in the form of a standard that provides legal support for the actions to be carried out. It will be this norm that should clearly establish the rules of the game and, therefore, draw the red lines and delimit the limits of use of such data. As is usual in regulatory pyramids, the details of this regulation should be included in lower-ranking legislation, such as decrees or instructions, so that they can be flexibly adapted over time.



EXAMPLES

Click on each flag or icon to go deeper

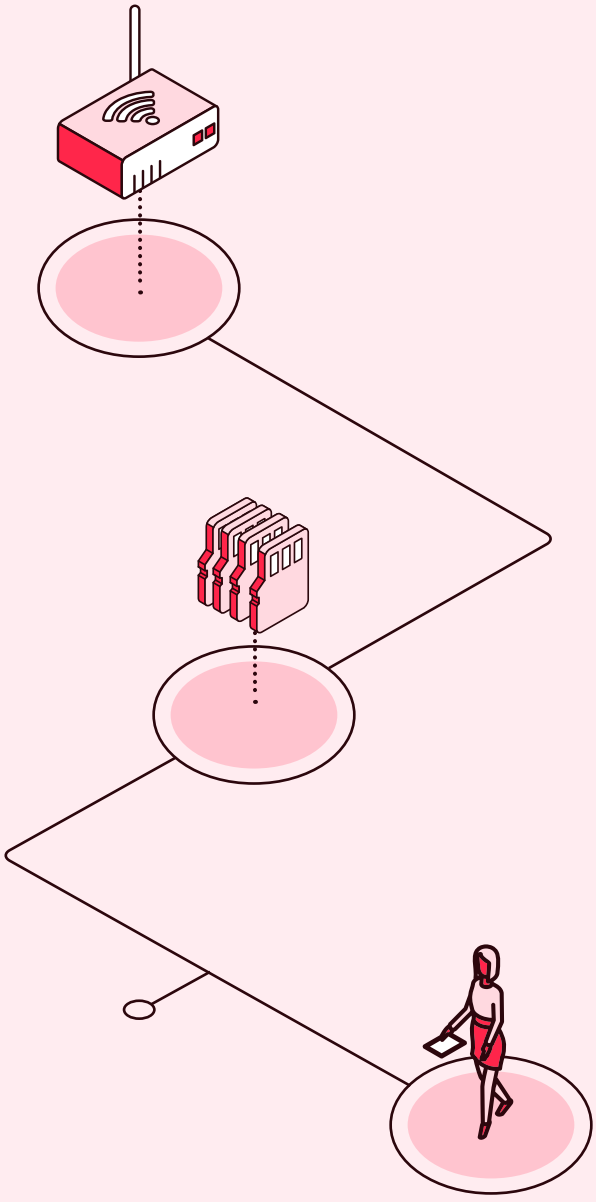
Uruguay
Datos 360 de AGESIC

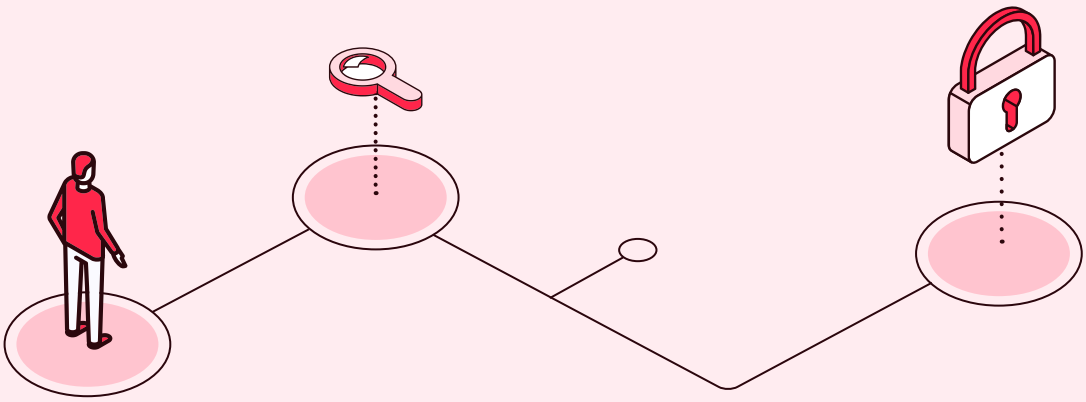
United Kingdom
National Data Strategy

Netherlands
Data Agenda Overheid

Canada
Report to the Clerk of the Privy Council

Spain
Law 18/2015, of July 9, amending Law 37/2007, of November 16, on the reuse of public sector information.

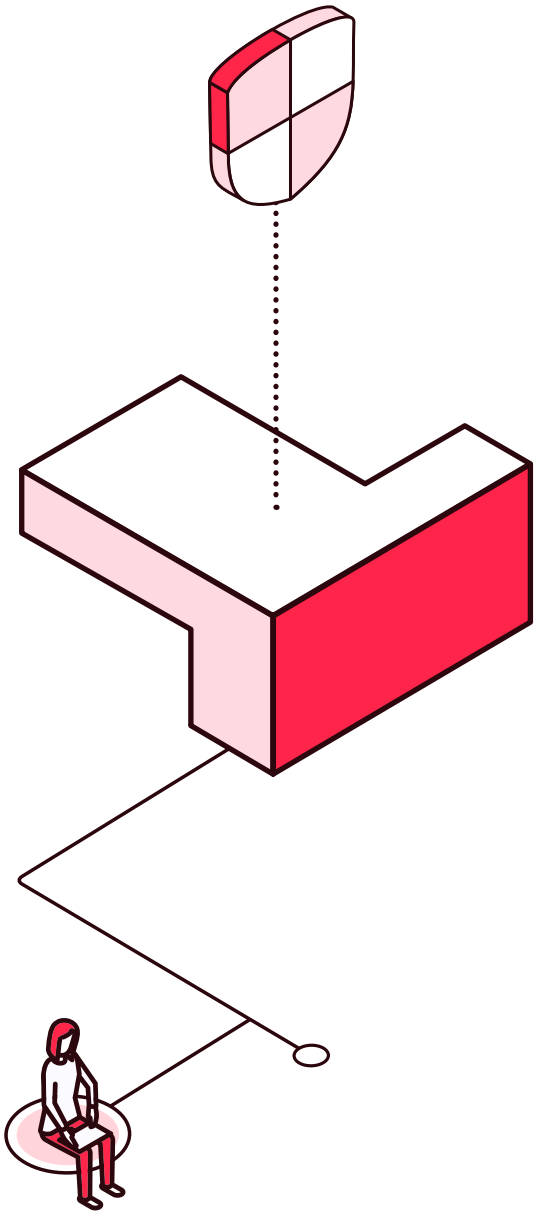




INDICATORS

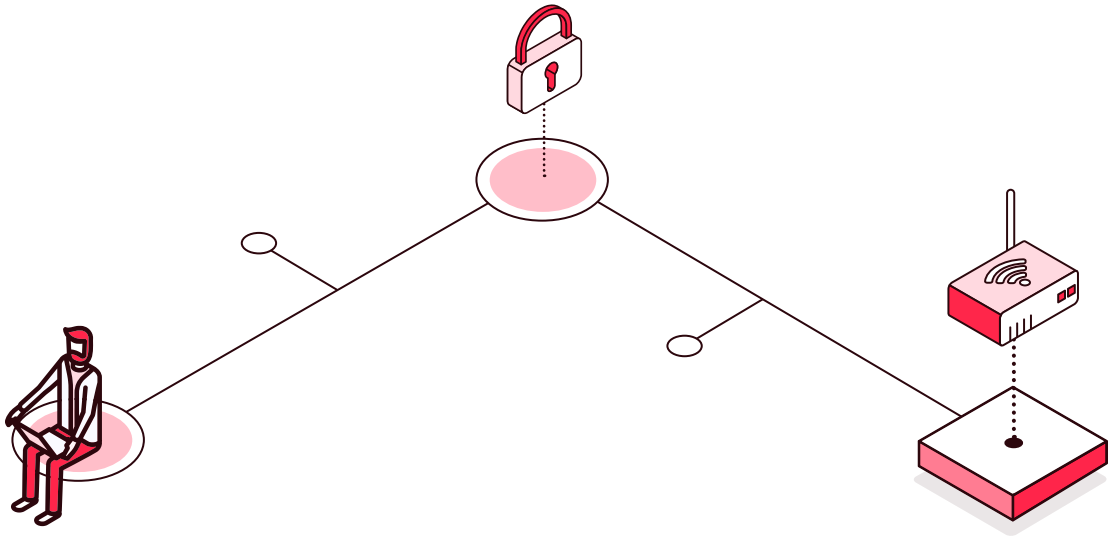
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a specific data strategy or regulation for public entities?
  - If so, does the strategy include the following elements?
    - Ethical use of data
    - Protection of personal data
    - Data exploitation and analytics
    - Statistical models that make it possible to exploit information without compromising privacy
    - Use of artificial intelligence in government data mining
    - Standardization of data within the government
    - Standardization of data between the government and the private sector
    - Data opening



2.13

Cybersecurity



Organizations today are facing a global revolution in governance that directly affects their information management practices. There is a growing need to focus on the value of the information protected and delivered, in terms of services provided. Due to the failures of large organizations in the past few years, legislators, policymakers, and regulators have created a complex web of new laws and regulations designed to force improvements in organizational governance, security, controls, and transparency. Past threats to IT systems and their disruptions from a variety of causes have given rise to the need for specific regulatory guidance on the governance of systems management and protecting the organization's most critical assets, its information, and its reputation.

These systems are critical for the development of the operations of all organizations. Access to reliable information has become an indispensable component for running public administrations and organizations in any country, especially those where information is the business.

This growing dependence on information had already been highlighted more than a decade ago by Peter Drucker in the book Management Changes for the 21st Century, when he said that "the diffusion of technology and the commoditization of information transforms the role of information into a resource equal in importance to the traditionally important ones of land, labor and capital."

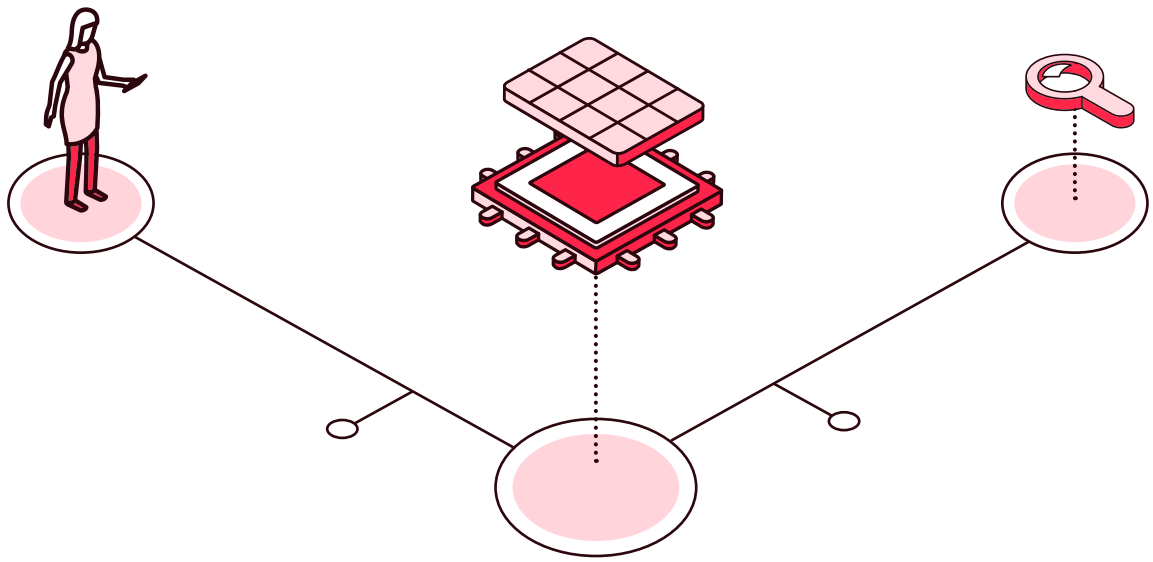
Organizations continue to witness information-related crime and vandalism. Institutions concerned with problems of jurisdiction, scarcity, and inadequacy of resources have not been as successful as they thought in reducing the impact on their activities. Many actions aimed at protecting critical information resources fail, and the responsibility falls on those in charge of the organizations. Clearly, the definition of cybersecurity regulations to protect states from these worrying situations is lacking.

A correct vision of information security must be broad, so that information and the knowledge based on it are adequately protected. However, this does not mean stopping to consider how it is handled, processed, transported, or stored, but also considering the universe of risks, benefits, and processes involved with information resources. Information security, along with other critical organizational resources, must be treated with a total vision in both public administrations and private organizations. To articulate all these premises, it is necessary to conduct a normative activity that supports not only the operational and execution part, but also the management and governance part.

THREAT ASSESSMENT

Effective security requires the active involvement of the highest levels of government in assessing and responding to emerging threats. Therefore, adequate regulations must be the backbone for decision-making affecting the following aspects:

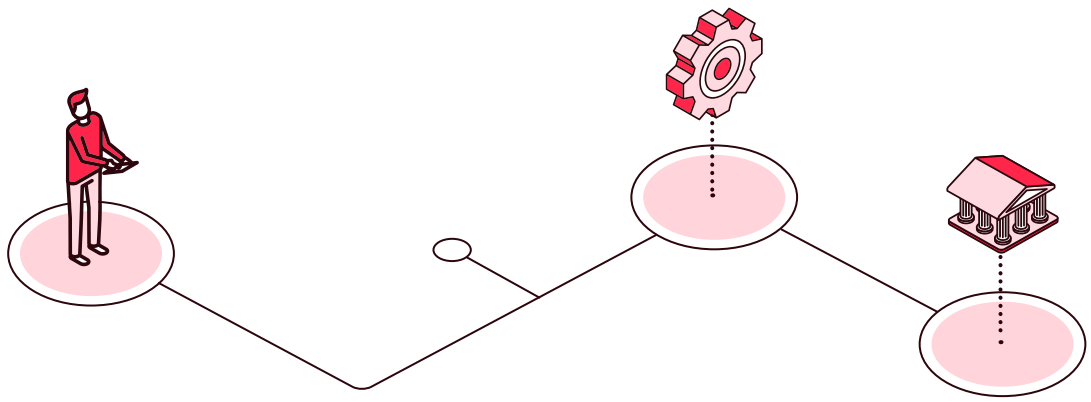
- Understand the criticality of information and information security for the organization.
- Review information security investments to align them with the organization's strategy and risk profile.
- Support the development and implementation of a broad and comprehensive information security program, based on the regulations approved for this purpose.
- Require regular reports to management on the adequacy and effectiveness of the program.



From this perspective, governance committees and the executive management of public administrations should review the following:

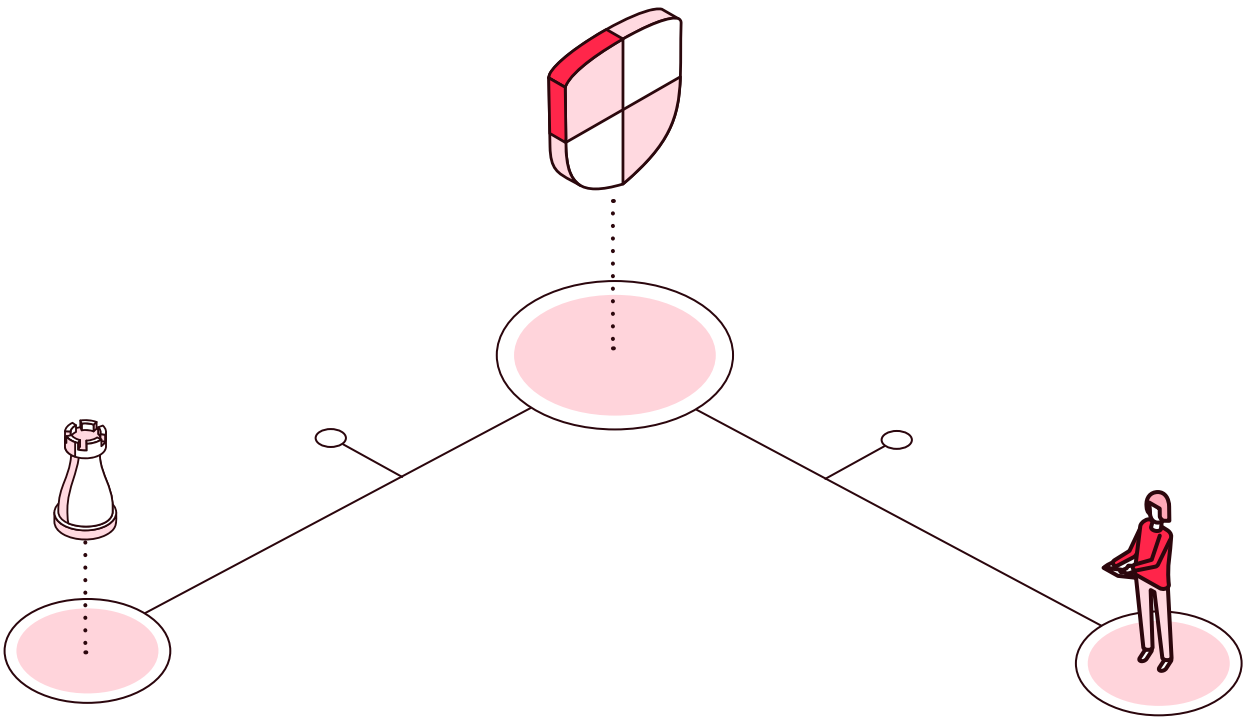
- The scale and return on current and future investments in information resources to ensure they are optimized.
- The potential of technology to profoundly change organizations and business practices to create new opportunities and value while reducing costs.
- Consequences associated with
  - Increasing dependence on information and the systems and communications that deliver it;
  - Reliance on entities outside the direct control of the organization;
  - Increased demand for sharing information with third parties;
  - The impact on the reputation and value of the organization, whether public administration or private sector, when security breaches occur;
  - The need for training or awareness-raising actions to convince senior management of the importance of information security.

IN ORDER FOR STATE ENTITIES, PUBLIC ADMINISTRATIONS, AND CITIZENS TO TAKE ADVANTAGE OF THE COMPETITIVE ADVANTAGES OFFERED BY A GLOBAL DIGITAL SOCIETY, A COUNTRY'S NATIONAL CYBERSECURITY REGULATIONS MUST BE A FUNDAMENTAL PART IN GENERAL TERMS, RECOGNIZING THE GUARANTEE OF CITIZENS' RIGHTS AND FREEDOMS.



Respect for fundamental rights (enshrined in a large number of the Magna Carta of different countries) requires a highly reliable and secure environment for citizens, especially due to the exponential use of electronic channels in the provision of public services. For example, telecommuting, which has been promoted since COVID-19, requires a digital transformation under regulations adapted to the new risks and threats. These security efforts are even more necessary at a time when cybercrime has surpassed traditional crime, with a proliferation of attacks on public administrations with the aim of obtaining illicit benefits or causing reputational damage through *ransomware*, denial of service (DoS), or any form of malware, not to mention the impact of new forms of crime that globally affect the billions of users of social networks and the internet.

In this complex context, it is essential to regulate what to do to protect this new economic and social space, boosted by the digital transformation and the Internet of Things. It is a cyberspace where, at least, the mission will be to guarantee the same rights and freedoms to citizens, government institutions, and public administrations.



CYBERSECURITY GOVERNANCE REGULATORY FRAMEWORK

National cybersecurity regulations must be part of and integrated into the country's security system to be fully effective. In addition, it is required to be properly coordinated with other security actions at the national and regional levels.

The regulatory structure of cybersecurity should articulate the necessary elements described below so that public administrations can have solid pillars of operation in this area:

- A body that supports the national security body chaired by the highest representation of the state, which is responsible for the direction of the national security policy, in all aspects related to the direction and coordination in the field of cybersecurity. This national cybersecurity body will pay special attention to the coordination, collaboration, and cooperation between the different public entities in the field of cybersecurity, as well as between other public entities and bodies with which it must relate.

  Specifically, the national cybersecurity body will facilitate the decision-making of the national security body by analyzing and assessing risks and threats, as well as possible crisis scenarios, raising proposals and initiatives both at the national, regional, and international levels, including cybersecurity response plans. It will also make the assessment of capabilities and conduct or participate in crisis management exercises at the national, regional, or international level.

- A national security department, through which the national security body will operate, which will also serve as a single point of contact to liaise and ensure coordination and cooperation with other countries internationally and in the region.

- A situation committee, with a unique character for the national security system, supported by the former department, with crisis management competencies.

- A commission to facilitate coordination between public entities at the operational level to respond to crisis management situations in the field of cybersecurity, in coordination with all state resources. In addition, it may include responsibilities for the management of public communication.

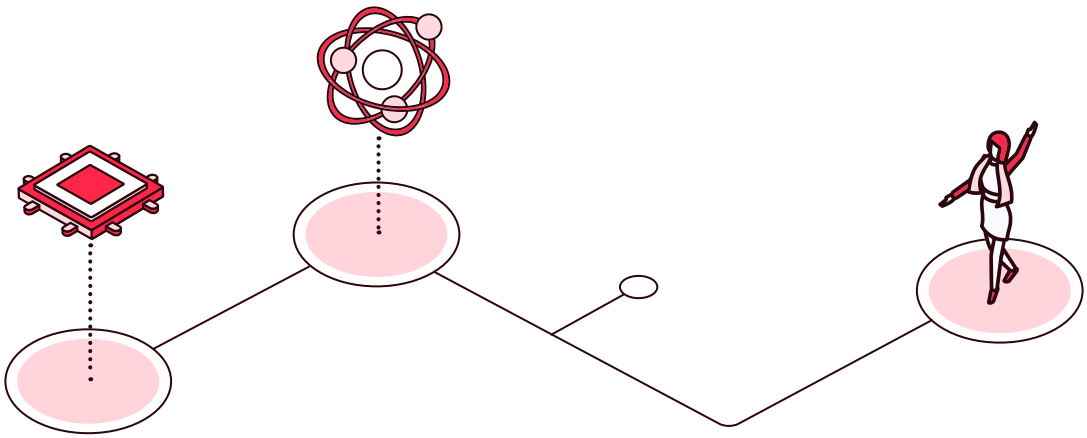
- The public authorities responsible for the security of networks and information systems.

- National, public, and private reference CSIRTs, coordinating competencies and actions, in collaboration with international and regional CSIRTs.

- A forum for public-private collaboration for the enhancement of all the capabilities needed to respond in a coordinated manner to cybersecurity challenges and threats. It may also include responsibilities for talent management in this area.

The definition of cybersecurity regulations should be approached as such a pyramid structure:

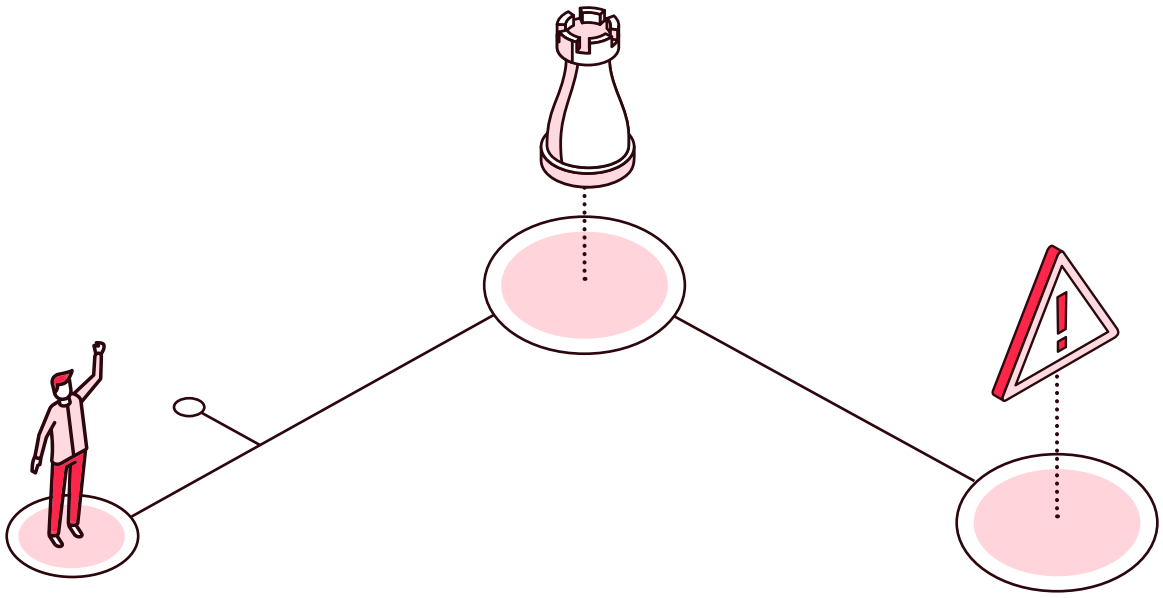
- At the top of the page you will find the regulations referred to the governance area, which includes the following areas:
  - Safety leadership.
  - Security policies (regulatory framework understood as policies and guidelines). Governance and management of cybersecurity is organized in this area.
- At the bottom of the page is the operating regulations it contemplates:
  - Security management (operations, monitoring, and security review).
  - User management (user management and awareness).
  - IT asset security (application security/databases and metadata, computers—hosts, servers—internal network and perimeter security).
  - Technology protection and continuity (physical and environmental controls, contingency plan controls). In this area, some effects are activated whose causes of repercussion will be in the area of governance. In addition, compliance is considered here from three levels: support, technologies, and knowledge.



DIMENSIONS OF *IT GOVERNANCE*

To define the *IT Governance* concept within a cybersecurity regulation it is necessary to integrate the following dimensions:

- **Value delivery:** Based on optimizing safety investments. The optimum level is achieved when the goals established for safety are met, with an acceptable level of risk and at a minimum cost.
- **Risk management:** Reducing adverse impacts to the organization to an acceptable level of risk.
- **Resource management:** Effective and efficient use of the knowledge and infrastructure available for information security.
- **Performance measurement (performance management):** Measuring, monitoring, and reporting on cybersecurity processes, ensuring that the organization's objectives are achieved.
- **Strategic alignment:** Aligning cybersecurity initiatives with the organization's business objectives.



PRINCIPLES AND OBJECTIVES

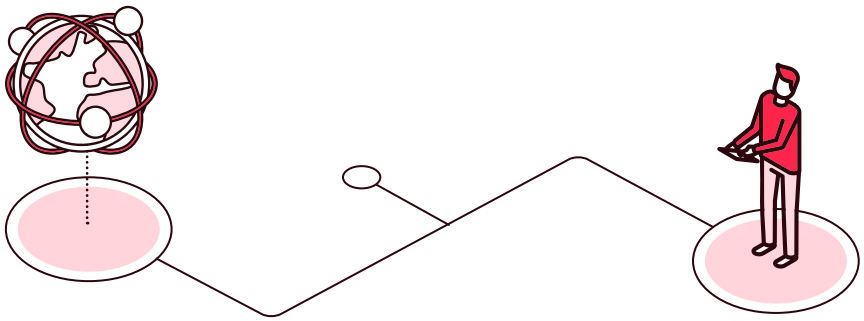
The guiding principles of a global regulation should be established, highlighting, among others,

- the unity of action in the event of cybersecurity incidents;
- prevention and anticipation;
- efficiency in the provision of resources and capabilities;
- resilience as a fundamental characteristic of critical infrastructures to ensure the provision of essential services for society in the face of cyber threats or illicit use of cyberspace.

The safe and reliable use of cyberspace by citizens and public administrations will be formulated as the main objective, thus protecting the fundamental rights and freedoms of individuals and the economic and social development of the country. The specific objectives guiding the state's action will determine the lines of action of the national cybersecurity regulations.

SAFETY REGULATIONS

At the international level, the drafting of cybersecurity regulations has become more important, as they are one of the main tools available to countries to guide their decision-making in this area. The drafting of specific security regulations at the state level to ensure the implementation of the actions and measures described in the previous sections is an activity that has been widely adopted around the world. These regulations can establish guidelines for protecting and improving information security management at the national level and articulate collaboration between countries At the international level, the drafting of cybersecurity regulations has become more important, as they are one of the main tools available to countries to guide their decision-making in this area. The drafting of specific security regulations at the state level to ensure the implementation of the actions and measures described in the previous sections is an activity that has been widely adopted around the world. These regulations can establish guidelines for protecting and improving information security management at the national level and articulate collaboration between countries.



Although in each country each regulatory agency will be responsible for establishing the national security regulatory instruments according to the needs identified, the following is a regulatory framework used by several countries that can serve as a reference:

National Security

National Cybersecurity Act

Specific security regulations

Laws and administrative regulations

General security regulations for the public sector

Criminal laws

National Security Act

- The purpose of this legislation is to regulate the National Security System, which also contemplates cyber threats as one of the risks and threats to national security, its coordination, organization, and direction. It also contemplates which are the key agencies and competent authorities to ensure national security and crisis management.

National Cybersecurity Act

- This is a separate regulatory option from the other risks and threats to national security. The indicated legislation options will regulate:
  - National security policy.
  - The security system.
  - Governance model: National security and cybersecurity councils.

- Regulation of the definition and management of crisis situations: It will be developed through instruments for prevention, detection, response, return to normality, and evaluation.

- National cybersecurity strategy: This is the reference framework for national security policy. It will describe the threats affecting the security of each country, the risks and the analysis of the strategic environment. The strategy will include the importance of ensuring security in cyberspace and the strengthening of capabilities for prevention, defense, detection, and response to cyberattacks. It should also highlight the risk posed to citizens' privacy by illicit activities arising from the misuse and exploitation of cyberspace and how these types of activities impact national security.

Specific security regulations

- Specific security regulations that identify strategic sectors, critical infrastructures and essential services, and provide them with a higher level of security: the guarantee of national security requires the protection of a series of infrastructures and services that are fundamental for the maintenance of the country's essential services. Disruption of these critical infrastructures would have serious consequences for specific territories or for the country as a whole:

  - regulation by the authorities
  - safety measures
  - incident management and reporting
  - incident response mechanisms
  - penalties

Laws and administrative regulations

- Regulation of electronic relations with citizens, provision of electronic services and electronic processing of procedures.

- Regulation of identification, authentication, and electronic signature systems for citizens, civil servants, and professionals. Authenticity and integrity of documents.

- Regulation of electronic channels and means for the provision of different electronic services.
- Regulation of the transition from paper to electronic documents.
- Regulation of electronic archives.

General security regulations for the public sector

- Regulation of security measures consisting of the basic principles and minimum requirements for adequate protection of information and services. It will be applied by public administrations to ensure access, integrity, availability, authenticity, confidentiality, traceability, and preservation of data, information, and services used in electronic media that they manage in the exercise of their powers. The public administrations shall adopt security measures proportionate to the nature of the information and services to be protected contained in the regulation:
  - Security standards and technical guidelines to implement security measures: These include security incident reporting, security auditing, compliance with regulations, and compliance of private entities with equivalent international standards.
  - Mechanisms for responding to security incidents in public administrations: Regulation of the *Computer Emergency Response Team* (CERT) for national coordination.

Criminal laws

- Regulation of cybercrimes.

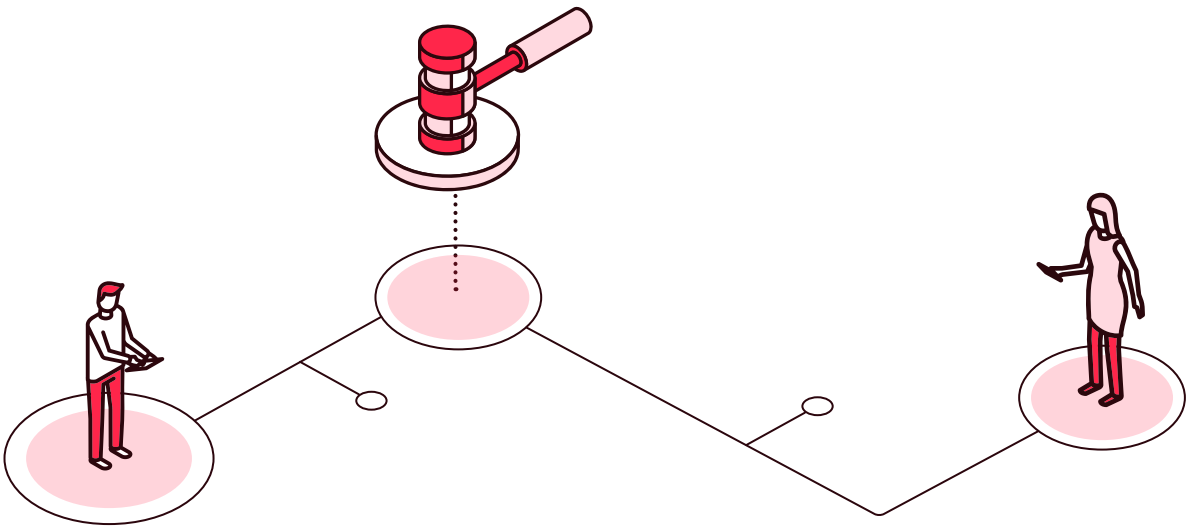
The European Union is a clear example of the regulation of critical infrastructures, which are defined as: "the asset, system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, and the social and economic well-being of the people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"[27].

27. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: https://eur-lex.Europe.eu/legal-content/en/TXT/?uri=CELEX:32008L0114n

The objective of the law and the regulation in this area is to establish a series of protection measures that provide adequate support for the coordination of public administrations, entities, and bodies managing or owning infrastructures that provide essential services to society, in order to achieve effective and integrated global security. The definition of strategic sectors will be specific to each country.

The North Atlantic Treaty Organization (NATO) also provides a definition of critical infrastructure in its *Critical Infrastructure Protection against Terrorist Attacks,* published in November 2014. It states that these are those facilities, services, and information systems that are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, the national economy, public health, and the effective functions of a government.

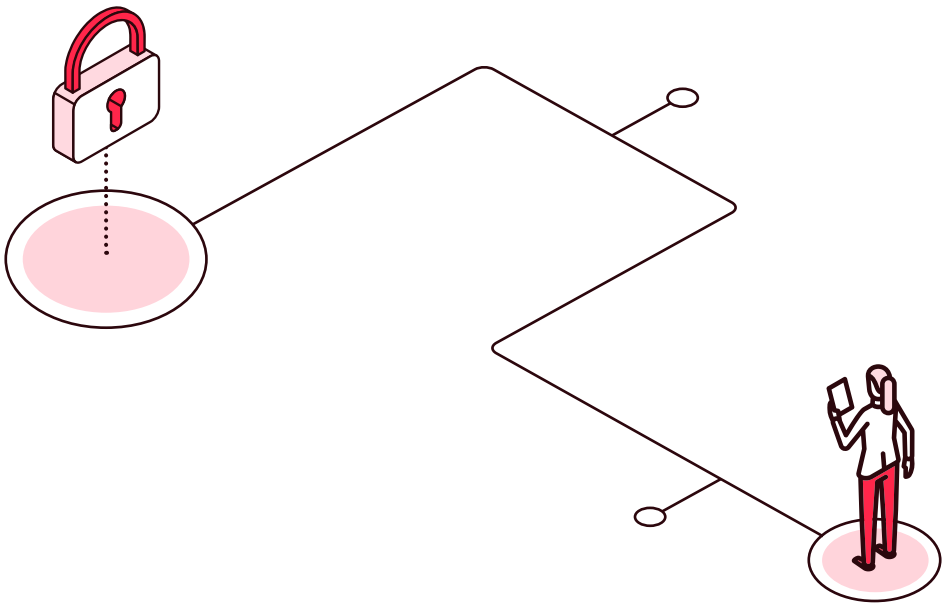
The level of detail associated with critical infrastructure protection regulations varies from country to country. However, all of them refer to the importance of fluid communication between the agents involved in the protection system to ensure the protection of infrastructures. They also stress the need to include critical infrastructure protection plans establishing guidelines for preventive measures to be carried out by the public and private organizations involved in the protection system. Some plans describe a series of security levels, which will depend on the assessment of risks and threats at each security level; they also describe the implementation of measures in accordance with the corresponding level to ensure the operation and maintenance of critical infrastructures, as well as to determine their vulnerabilities and the effects that would arise if they were to cease to function.



LINES OF ACTION AND MEASURES

The implementation of the strategy will be articulated through the following lines of action or measures:

- Ensuring the availability of essential services and the protection of the critical infrastructures that support them.
- Strengthening the legal framework to respond to new types of cybercrime.
- Strengthening the capacity to investigate and combat cybercrime, especially of police forces in coordination at the regional and international levels.
- Building a culture of cybersecurity aimed at citizens, public entities, and companies.
- Promoting the national cybersecurity industry by alleviating technological dependence, with special attention to entrepreneurship.
- Generating national talent in cybersecurity, strengthening knowledge and research, development, and innovation capabilities.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Citizen
Camilo

Camilo is concerned about doing business online. Recently, a virus got into his computer and deleted all his files, and this has led him to have no confidence in the online procedures proposed by his local council. Finally, Camilo takes this concern to the office where he processes the renewal of his cab license, and there he is informed and given a brochure of the cybersecurity measures taken by his municipality, which leaves him much calmer. Next time he will proceed with the procedure through the internet.

Entrepreneur
Ana

Ana is very aware of the importance of cybersecurity. As a chip manufacturer, she has had to include measures to make these pieces of hardware more secure. Since she knows the relevance of this issue, she is particularly concerned as she does not see the country's cybersecurity strategy clearly. She knows that there are isolated initiatives but, as she is well aware, cybersecurity works like a chain: if it breaks at the weakest link, everything is at risk. That is why she is fighting for her country to have an integrated cybersecurity strategy.

Vice minister of health
Sara

If there's one thing that keeps Sara up at night, it's the idea that a cyberattack could crash her country's healthcare system. She knows from the press how previous attacks have affected other healthcare systems, so she has launched the Ministry of Health's cybersecurity strategy, coordinated with the Ministry of Interior's country cybersecurity strategy.

Mayor's advisor
Daniel

Daniel is concerned about the cybersecurity of his municipality. In order to have citizens and companies informed and less vulnerable to cyberattacks, he uses municipal resources (courses, information brochures) to teach basic notions in this area, but he is fully aware that he does not have the resources to protect his own information system. He has therefore prepared a memo on behalf of the mayor's office to request that the country's cybersecurity managers design a national strategy aimed at protecting the digital assets of municipalities.

EXAMPLES

Click on each flag or icon to go deeper

Republic of Korea

General legislation on infrastructure protection.

Republic of Korea

National Cybersecurity Regulation.

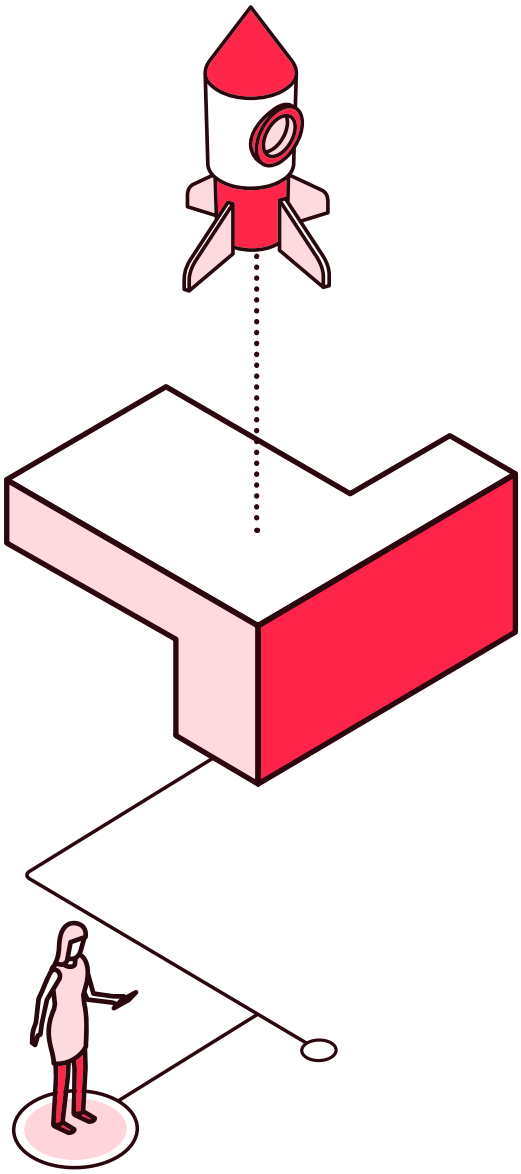
Estonia

Cybersecurity Act

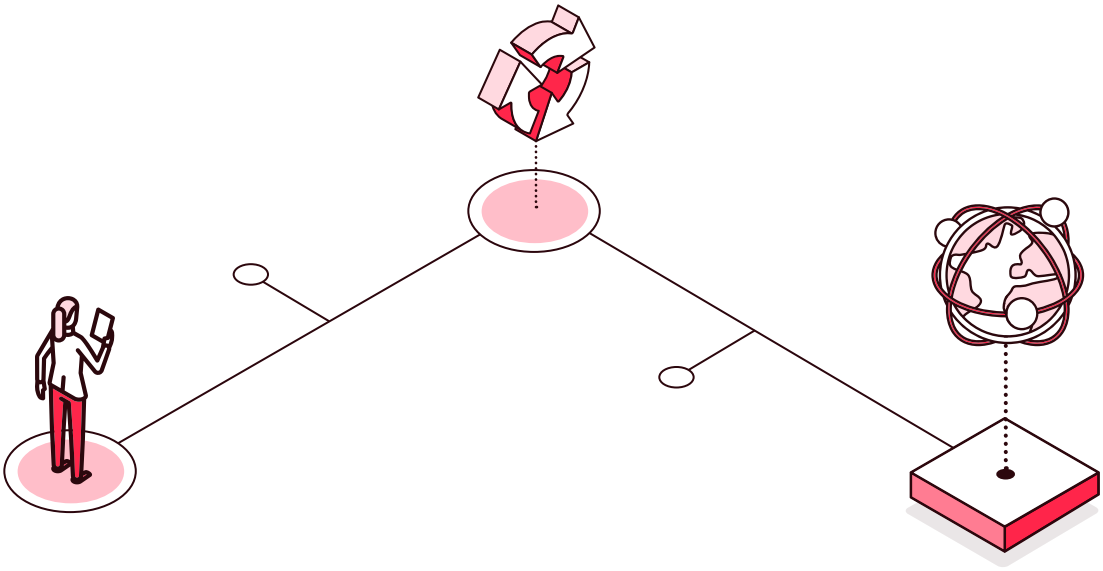
INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there general national cybersecurity regulations?
- Are there norms that define institutional roles and responsibilities in cyberspace?
- Are there specific rules regarding incident response?
- Are there specific rules regarding crisis management and digital resilience?
- Are there specific rules regarding critical infrastructure protection?
- Are there cybersecurity guidelines to facilitate the implementation of secure digital services in different areas?
- Do you handle detailed definitions of cybercrime-related issues?
- Do cybersecurity regulations and guidelines cover all public administrations, including municipalities?
- Does cybersecurity regulation cover public administrations and the private sector in an integrated manner?
- Is there domestic legislation on cybercrime?
- Has the country joined any international cooperation treaties against cybercrime?
- Is there substantive legislation against cybercrime and with respect to ICT security?
- Is there procedural legislation against cybercrime?
- Is there legislation regarding data protection, privacy, freedom of expression, and other human rights online?
- Has the country joined any formal treaties, or does it informally carry out international cooperation against cybercrime?
- Are there capabilities for investigating, prosecuting, and sentencing crimes in the digital real



2.14 Disruptive technologies



The regulatory framework that different governments have applied to the use of technology has been characterized by being neither very intrusive nor blocking; it has been based mainly on data protection and privacy, leaving the power to create and distribute technology in general in the hands of software and technology manufacturers. This decision is not random and is based on two reasons:

- Governments have wished to encourage innovation and have not opted for technological regulation because it can be seen as contrary to a country's technological evolution.
- The technologies used so far did not present any risk to society.

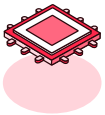
Disruptive technologies are a set of emerging technologies whose application can transform the economy and society through the creation of innovative processes based on the approach and resolution of processes in a radically different way than was currently understood. They are mainly based on the following:

- The information processing capacity of technology is far superior to that of human beings.
- The immediacy of information, something that is increasingly demanded by a society that wants to have personalized services at the same time it requests them.

MAIN DISRUPTIVE TECHNOLOGIES

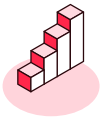
The following technologies have a direct application to the provision of innovative public services, so it is important to regulate them in the short term in the different countries where they already operate:

Big data

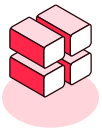


Artificial intelligence

Robotic Process Automation



Internet of Things (IoT)



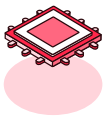
Blockchain

Big data

Public administrations generate and have access to more and more data at no cost, which makes it the cornerstone on which any service and the development of new public policies are based. Thus, the need arises to regulate its management as a regulatory guarantee.

Because its exploitation in any of its different aspects makes it possible to identify new trends in the behavior of society, data are a tremendously useful asset in the development of public services that meet the needs of citizens. Big data allows such exploitation for two specific purposes:

- **Data science:** Prediction and discovery of future behavior through data analysis of past behavior.
- **Data analytics:** Information analysis as an aid to decision-making.

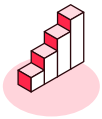


Artificial intelligence

The ability of systems to analyze their environment and make decisions with a sufficiently high degree of autonomy to achieve specific, predetermined objectives. This technology includes what is known as machine learning, whereby software and systems are able to learn from their environment and from the large amounts of information and data made available to them, adapting their behavior to changes in execution conditions, without having been explicitly programmed to do so.

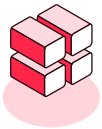
Robotic Process Automation (RPA)

Aims to automate repetitive tasks by implementing software that works as a virtual employee, performing the same simple and repetitive tasks for which a person was intended.



Internet of Things (IoT)

This technology aims to facilitate the interaction between objects and people through the various communication networks available, and then exploit these relationships to generate value-added services to both the administration and citizens and companies.



Blockchain

Allows for the generation of trust between different parties that do not know each other (both the administration and the citizens and companies) through the collection of evidence that guarantees the transactions carried out between each of the actors without having to resort to a trusted third party.

WHY SHOULD WE BET ON REGULATION IN THIS AREA?

- **The generation of hitherto unknown social risks:** One of the characteristics of disruptive technologies is their ability to interact with a dynamic and changing environment. In this context, this type of technology can exploit information and generate new knowledge based on which they were programmed, although this has a high probability of not being fully assessed or reviewed. Society has thus moved from a controlled interaction with technology to machines that have the capacity to make decisions, which entails a risk that must be regulated and which leads to regulatory acceleration. The "what is not forbidden is allowed" approach is common in all governments.

- **Society is increasingly accustomed to personalized services and demands these same characteristics from the services offered by public administrations:** It is no longer enough to offer services based on procedures carried out by individuals and within a reasonable time; it also requires personalized, immediate, and automated attention, with the capacity to adapt to the moment and the characteristics of the service request, all with a legal basis that provides maximum guarantees. These requirements of society lead to the adoption of disruptive technologies by the public sector, although in this case there is the same opacity that generates malpractice or distrust in users. Therefore, it is vitally important that this regulation is aligned with that of the public administrations themselves, which work under a robust legislative framework that ensures and protects the basic rights of citizens and in no case undermines society's trust in the state. The public administration should therefore not be tempted to rapidly adopt technologies that are not regulated, since the rule of law must prevail in the face of the advance of digitalization. Any breach in the confidence of citizens in their public administrations can lead to a standstill in their digital transformation and even a technological setback, calling into question everything that has been done so far, so the regulatory needs of these technologies must be identified and evaluated.

REGULATORY BASIS

Governments must become aware that there is a problem and must therefore establish the basic rules of the game, quickly and safely. Generating a regulatory framework for all cases is currently unfeasible, especially because innovation is unpredictable. Thus, the lead institutions must focus on the regulation of these technologies through a regulatory framework characterized by being the following:

- **Robust and clear:** There must be a global framework that clearly and concisely establishes where, under what conditions, and how these technologies are applied, as well as clearly identifying where not to apply them. Currently, in the compliance framework, there are some private entities that have decided to generate their own regulations, but these types of private initiatives must be encompassed—and if necessary revised—within the common framework. This framework must therefore be clear and concise.

- **Balanced:** So as to support technological development, but safeguarding the rights of citizens without harming the country's innovative capacity.

- **Flexible:** In the face of uncertain situations, it is of utmost importance that the regulation has the capacity to react and that it be swiftly implemented by governments.

- **Universal:** Understood from two different perspectives:

- The use and interconnection of these technologies generally go beyond the national scope of a country. In this context, regulations are required within a common international framework based on an international governance structure for the cooperation of the national authorities involved, in order to avoid the fragmentation of responsibilities.

- Competition among private entities, which may result in the constant search for technological competitive advantages of one government over another.

PRINCIPLES THAT DISRUPTIVE TECHNOLOGIES SHOULD FOLLOW

Once the regulatory framework has been established, and with the aim of making these technologies serve society in the aforementioned terms, the following principles should be established for disruptive technologies in any of their forms:

- Be in accordance with the law, always respecting ethical principles.

- Enable human supervision with control measures, especially with regard to data processing and the generation of new knowledge for concrete actions on people or objects.

- Be solid in the field of security, understood in all its areas: technological and physical.

- Ensure data protection and integrity.

- Be transparent. In the case of generating new knowledge or decision-making by the machines, the process must be documented and explained thoroughly.

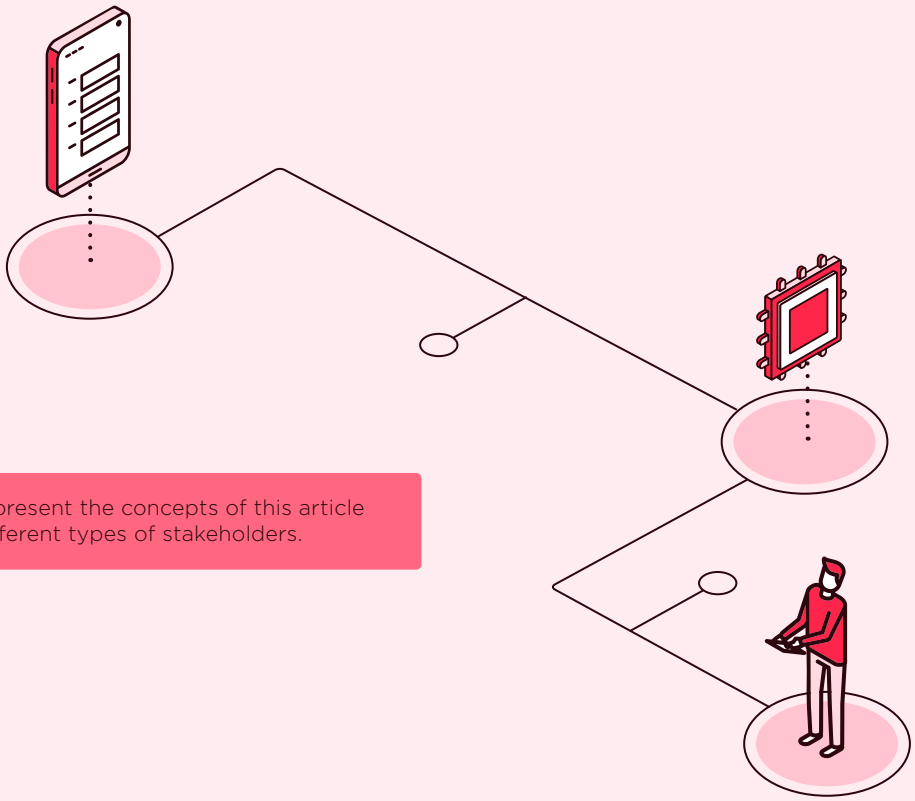
- Ensure nondiscrimination and equity, as well as social and environmental well-being.

- Enable auditing and control of the systems, so that those most responsible can be held accountable.

RELATIONSHIPS AND SEQUENCES

- **Data protection regulations:** There is a direct relationship with the entire regulatory framework applicable to data protection, so it is necessary to review whether this area requires updating.

- **Security regulations:** There is a direct relationship with the entire regulatory framework applicable to national security, so it is also necessary to review whether this area requires updating.



STORIES

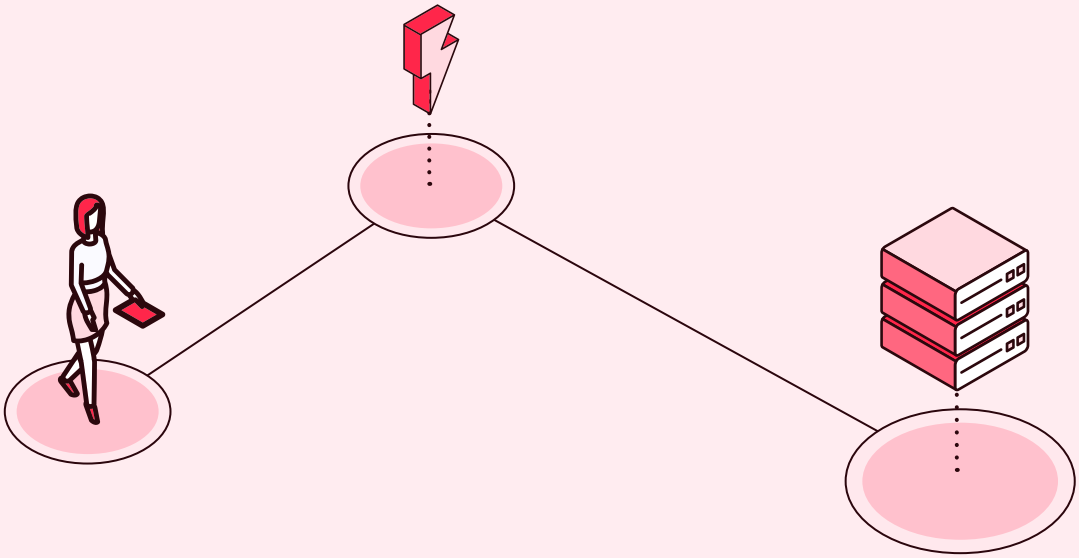
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Citizen
Camilo

Camilo is excited about his smart device that advises him on everything he asks, although at the same time he is concerned that it may listen in without being asked to or make decisions not authorized by him. Camilo does not know if the company that manufactures this device complies with any regulation that protects him if it is defective or makes any mistake that causes damage to Camilo or his family.

Entrepreneur
Ana

As an entrepreneur, Ana has acquired an algorithm that she includes in her product. This algorithm has made a series of decisions that have caused an accident due to a bias in the analyzed data. In this situation, Ana is not sure whether her company or the company that sold her the algorithm will be civilly liable.



Vice minister of health
Sara

Sara is analyzing with her team the information contained in their databases, although there are a lot of them and no conclusive results are obtained. For this reason, they are implementing a *big data process* to obtain these conclusions more quickly and reliably, although it will be necessary to identify the risk of falling into erroneous conclusions that no one reviews. To avoid the risk for people of making automated decisions without human bias, a person in charge is appointed to review the behavior of the algorithm, and, finally, to safeguard the rights of individuals, the information will be anonymized.

Mayor's advisor
Daniel

Daniel has authorized a new software connected to the cloud to improve the processes of the city council. Among other things, it allows him to textualize the minutes and other documents that are routinely generated in his activity. However, he is unclear about the data flow and where the information they generate will end up; much of this information is classified or secret. He thinks that a security framework is needed to allow the use of this type of technology with greater guarantees.

EXAMPLES

Click on each flag or icon to go deeper

European Commission
White paper on artificial intelligence – a European approach to excellence and trust

Europe
Legal and regulatory framework *for blockchain.*

European Commission
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on building trust and confidence in human-centered artificial intelligence.

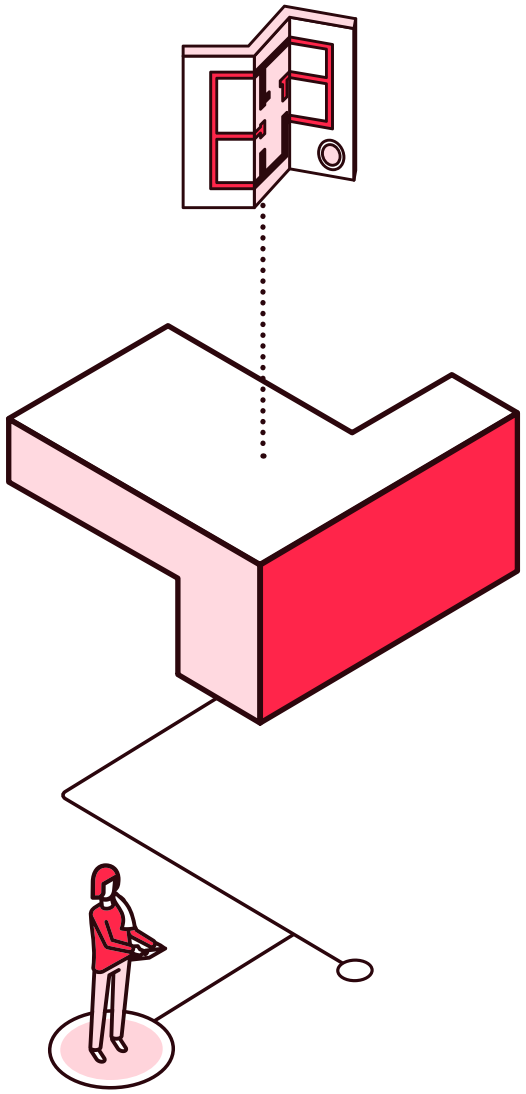
Spain
National Artificial Intelligence Strategy.

OECD
Principles on Artificial Intelligence.

INDICATORS

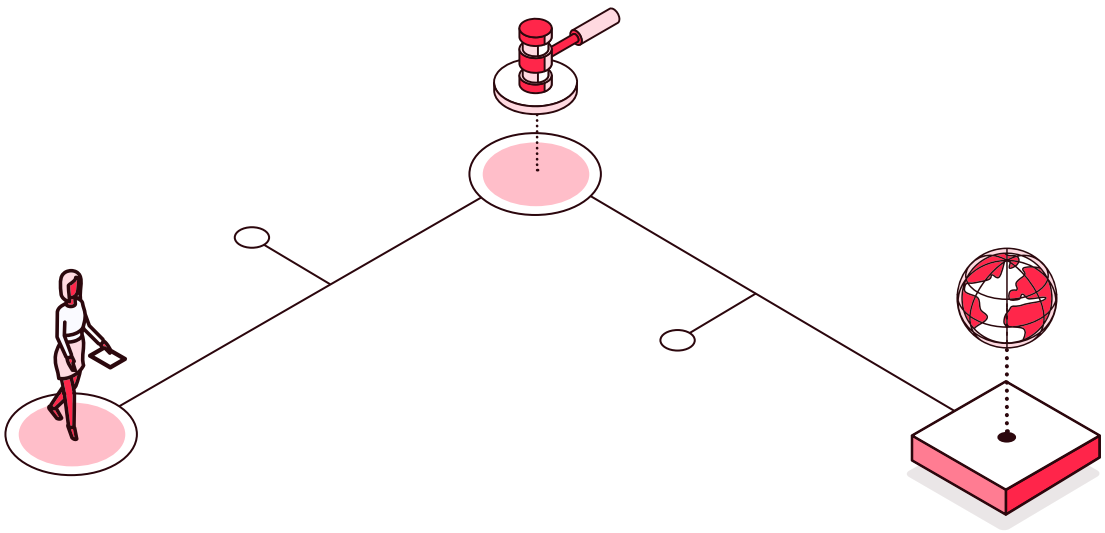
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a code of ethics for artificial intelligence in public administration?
- Is massive processing of citizen information carried out?
- Are scorecards available for the identification of new services required by citizens?
- Do smart contracts apply to citizen relations?
- Is a compliance process in place for the implementation of disruptive technologies?
- Is there oversight over the design, development, implementation, operation, and exploitation of systems based on disruptive technologies?



2.15

Cross-government technical regulation



Within the regulations there is a section, usually at the second or third level, whose functions are as follows:

- Define technical standards for components, structures, and formats related to aspects defined in higher-ranking standards, applicable to all sectors or to a specific one.
- Determine technical and quality criteria for a process or service, in this case electronic.
- Regulate compliance and auditing methods.

Technical standards are usually drawn up by nationally or internationally recognized standardization bodies, which establish specific technical criteria for a product or service. In this case, since the scope of application is usually limited to the national level and the technical normative needs depend on higher-ranking regulations, they are usually drawn up by the administration itself, either through legislative bodies or technical committees.

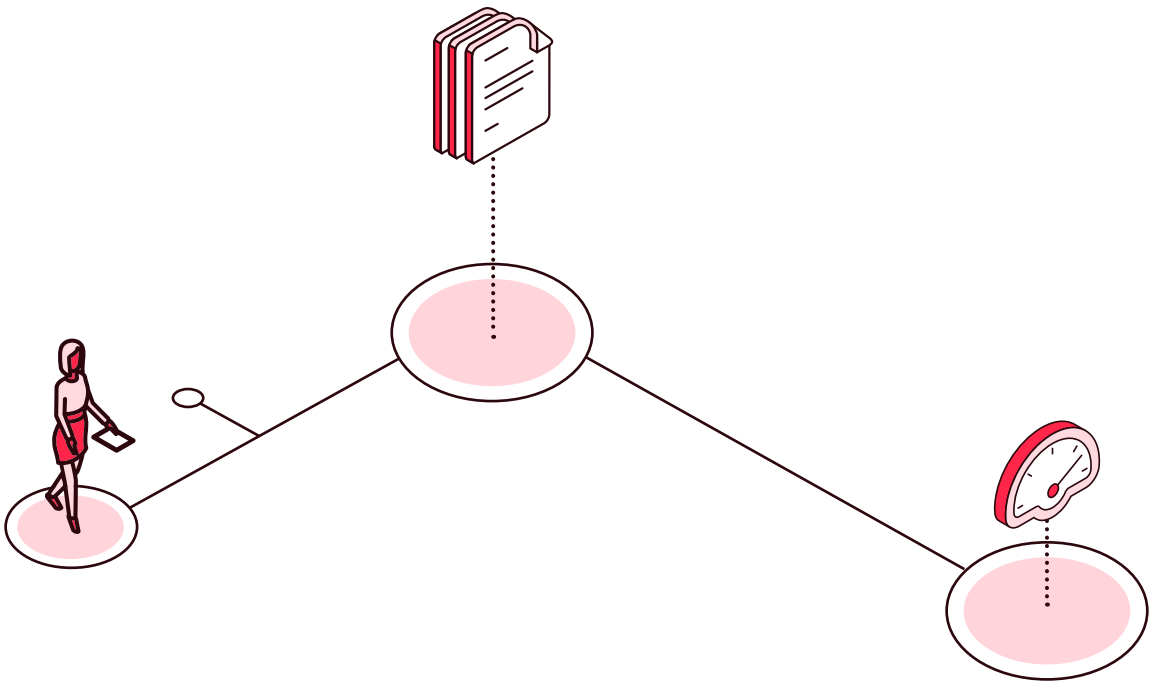
Technical standards are considered cross-cutting because they can be used as regulations both in different sectors that share a specific need and in the same sector, providing the basis for the development of other technical standards based on the previous one. In other words, it is essential to have a set of cross-cutting standards that concretely and precisely define the technical requirements to be met by the systems, the objects of exchange, the processes to be followed, the standards to be applied, etc. This is especially true in the digital transformation scenario, where countless different actors, systems, and technologies are involved.

Thus, the higher-ranking regulations aim to establish a regulatory framework that is sufficiently broad and flexible to provide guarantees for the entire process and to withstand the rapid technological changes, given the high degree of interrelations and interoperability between the different parties involved in the process. This will allow the following to occur:

- Generate the technical stability conditions necessary to create a working framework required in any administration.

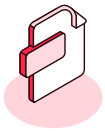
- Ensure the creation of a framework of trust in the private sector when developing standardized solutions applicable to the administration. This will result in greater competition and the elimination of closed market niches, since work will be done on standardized elements, which in turn will result in cost savings for the administration, since what is built for a specific sector can be used for another, thanks to the fact that they are technically regulated in the same way.

As explained below, it is important to define a regulatory strategy that allows for reuse across sectors, identifying cross-cutting components that establish a common technical regulation but at the same time contemplate the particularization of some of its components through sector-specific technical regulation.

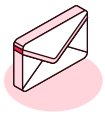


CROSS-CUTTING ISSUES THAT SHOULD BE CONSIDERED IN A TECHNICAL REGULATORY ARCHITECTURE

Electronic file

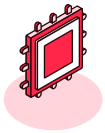


Electronic document



Electronic notification systems

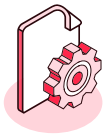
Entry/exit registry systems



Processing engines and systems

Digital identification systems

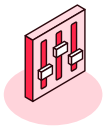
Digital signature systems



Document management and archiving systems

Data Brokerage Platforms

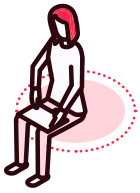
Cross-cutting business objects



Procedures

Catalogs of standards

Connection to communications networks



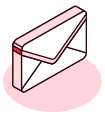
Electronic file

This allows you to define the structure and format of the basic electronic file, as well as the specifications of the referral and availability services. This section must contain at least the following:

- definition of the electronic file and its structure
- definition of syntax for interoperability, formatting, and structure, including xml (xsd)
- definition of the minimum metadata to be covered and the index
- definition of signatures
- considerations for implementation, use, and treatment

Electronic document

- To establish the components of the electronic document, the content, the electronic signature, if any, and metadata, as well as the structure and format for its exchange. As a minimum, it shall reflect the following:
- definition of electronic document and its structure
- definition of syntax for interoperability, format, and structure, including xml (xsd)
- definition of the minimum metadata to be considered
- definition of electronic document signatures
- considerations for implementation, use and treatment



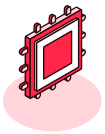
Electronic notification systems

To contemplate the necessary conditions and characteristics that the systems must comply with in order to guarantee electronic notification, including the evidence that any communication must have in order to be considered a "notification" (date and time of sending the notification, date and time of making the notification available, date and time of access to the notification, full reception of the content, identity of the sender and the addressee).

Entry/exit registry systems

To establish the conditions and characteristics necessary for the interconnection of public administration registries and, therefore, the exchange of information between them. It must include, at least, the definition of the following aspects:

- data model for the exchange of entries between registry entities
- technical specification of the standard that will support the standardized exchange of registry entries, including the definition and main features of the standard, the data schema and formats for the exchanged files, the error control and management mechanisms to be applied in the process, the high-level features to be guaranteed by the exchange system used, etc.
- functions and requirements of the exchange system



Processing engines and systems

To reflect the characteristics that the transversal platform for processing administrative procedures will have. It would include, at least, the definition of the following aspects:

- a set of technologies and standards applicable to the definition of business processes
- requirements for the assurance of service levels provided by the processing platform
- requirements for system governance (incorporation of new business processes, access to services, process catalog management, etc.)

- technical requirements to be met by the administrative procedures processing platform
- general safety aspects to be complied with
- establish the characteristics of the traceability system implemented

Digital identification systems

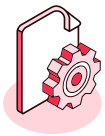
To indicate the set of common criteria on the supported digital identification systems. It shall contain the following:

- definition of the set of standards for the exchange of authentication and authorization information between the different security domains
- catalogs of systems that may be admissible and that may interoperate
- processes for the incorporation and management of new digital identification systems

Digital signature systems

To reflect the set of common criteria on authentication and mutual recognition of electronic signatures to be supported by the documents. It would include, at least, the definition of the following aspects:

- the set of secure electronic signatures that can be admissible by all participants and can therefore interoperate regardless of how many signature policies are established in each organization
- concepts and generalities of an electronic signature policy, as well as the identifying data, actors, and uses of electronic signatures, the possible relationship with other policies, and the considerations for the archiving and custody of electronic signatures
- common formats and algorithms, as well as creation and validation rules
- rules for long-lived signature



Document management and archiving systems

To establish the set of principles necessary for the management of electronic documents from which the electronic file will be nourished. As a minimum, it must include the following:

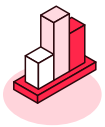
- principles necessary for electronic document management: document management requirements and properties and life cycle of the electronic document, as well as of the management system, from capture to conservation
- programs for processing electronic documents, identifying their form and structure when they are created and subsequently incorporated into the information system
- identification of document metadata at each stage of the document life cycle
- strategies to ensure the preservation of documents, access, and processing conditions

Data Brokerage Platforms

To pool the specifications necessary for the intermediated exchange of data between public administrations. As a minimum it must contain the following:

- definition of the actors involved in the data exchange, in this case the transferor and sender, and the transferee and requester
- establishment of roles, functions, and responsibilities of each of the actors involved in the data exchange
- characteristics, role, and functions of the data brokerage platform
- requirements for the assurance of service levels provided by the data brokerage platform
- requirements for system governance (incorporation of new services, access to services, management of the service catalog, etc.)

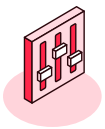
- technical requirements to be met by the data brokerage platform
- general safety aspects to be complied with
- a set of applicable technologies and standards
- characteristics of the implemented traceability system



Cross-cutting business objects

To record and publish data models that are common in the public administration (for example: natural person, legal person, notification, registry entry) and those that refer to matters subject to information exchange with citizens and within the administration. It also includes the definitions and associated codifications for publication in a semantic interoperability repository. It would include, at least, the definition of the following aspects:

- a set of data models to be published
- the technical structure to be complied with for the exchange of data models and their publication in the semantic interoperability repository
- requirements for the identification of data models
- a communication protocol and interaction with the semantic interoperability repository
- a policy for the use of data models published in the semantic interoperability repository
- coding requirements for data models of statistical interest



Procedures

- **Authentic copying and conversion between electronic formats:** To establish the necessary rules for the generation of authentic electronic copies, as well as authentic paper copies of electronic public documents, and for the format conversion of electronic documents.

- **It shall include the following:**
  - general characteristics that an electronic copy must meet in order to be considered authentic
  - definition and characteristics of the different types of copy possible (authentic electronic copy with format change, authentic electronic copy of paper documents, authentic electronic partial copy, authentic paper copy of electronic administrative public documents)
  - requirements for the conversion of an electronic document
- **Digitization of documents:** to establish the set of standards and quality standards for the digitization of documents on paper or other non-electronic media susceptible to digitization through photoelectric means, in order to ensure authenticity. It must establish:
  - the minimum metadata that an electronic document must have after digitization
  - the technical characteristics of the object resulting from the digitization (e.g., minimum resolution in pixels per inch)
  - the guarantees of authenticity, confidentiality, integrity, availability, traceability, and preservation of the digitization
  - the digitization standards that the systems and applications that support the ets must comply with; this must contemplate at most that of the standards catalog standard
- **Declarations of conformity:** To support the demonstration of the conformity of public administrations with all the semantic/technical regulations developed and applied in the field of interoperability.
- **Audit:** To establish the audit procedure to be carried out by recognized conformity assessment bodies. It would include, at least, the definition of the following aspects:
  - evaluation standards, either from the public administration or developed by normalization and standardization organizations
  - evaluation deadlines

Catalogs of standards

To establish a set of standards that meet the needs of all the semantic/technical regulations developed to support it. It would include, at least, the definition of the following aspects:

- a set of standards that will be applied, indicating the object of application for each standard and the state in which it is
- a set of minimum application standards for interoperability and for the development of all the semantic/technical regulations developed
- a procedure for the incorporation of required standards
- requirements for which a standard not listed in the catalog may be used
- a procedure for the maintenance of the standards catalog, including its revision and updating

Connection to communications networks

To establish the conditions under which any body belonging to the public administrations will access corporate communications networks that will support the exchange of electronic data. It must include at least the following aspects:

- network connection infrastructure
- functionalities to be offered by the network support center
- set of network access providers
- technical requirements for connection to network access providers (connection area layout, connection administration, addressing plan, provision of connectivity elements, physical conditioning guarantees, support and incident management services, etc.)
- conditions of access and use of the services provided by the network
- set of agents and roles that will support the provision of the network service

THE ASPECTS CONTEMPLATED ABOVE, AS PART OF A NORMATIVE TECHNICAL REFERENCE ARCHITECTURE, ARE APPLICABLE TO ANY SECTOR, REGARDLESS OF WHETHER IT IS PUBLIC, HEALTH, JUDICIAL, LAW ENFORCEMENT, RESEARCH, EDUCATION, CULTURE, ETC. THEREFORE, WITH THE DEFINITION AND DEVELOPMENT OF THIS REFERENCE ARCHITECTURE, A CROSS-CUTTING TECHNICAL REGULATORY STRUCTURE IS BEING ESTABLISHED THAT IS APPLICABLE AND REUSABLE IN 100 PERCENT OF THE STATE BODIES, WITH THE COST AND TIME SAVINGS THAT THIS ENTAILS.

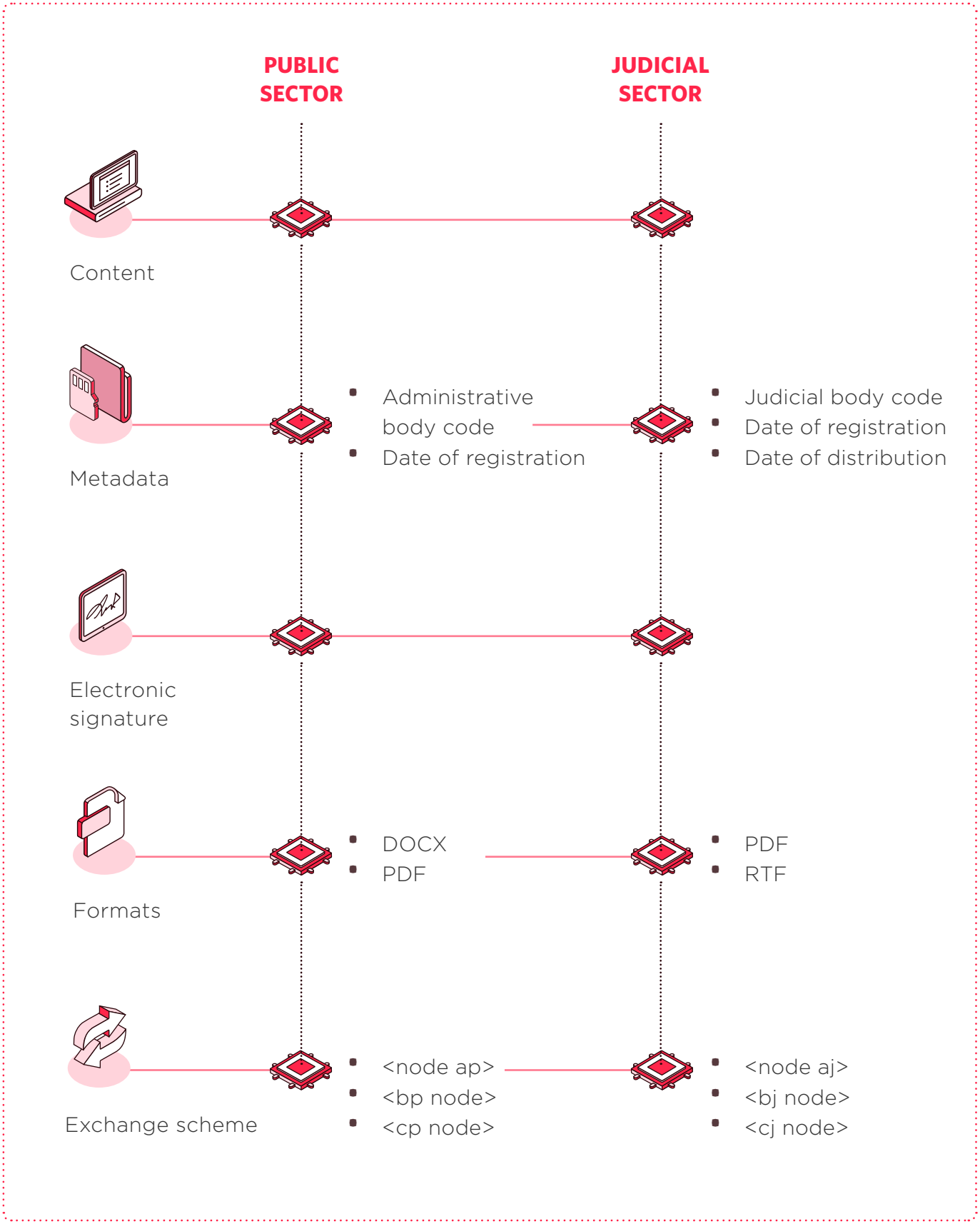
TECHNICAL STANDARDS AT SECTOR LEVEL

Once the technical normative architecture of reference has been established, the technical normative by sector is defined, which will particularize and adapt some elements to the needs of a specific field. In this case, if we take the electronic document as an example, the technical normative framework of reference will establish the technical requirements that an electronic document must satisfy for any sector, such as the following:

- content
- metadata
- electronic signature
- formats
- exchange scheme

However, the technical regulatory framework applicable to the sector would add particularities to those of the above elements that are likely to do so. Thus, although the general structure and the electronic signature would probably remain unchanged for all sectors, other components such as content, metadata, applicable formats, and—of course—the exchange scheme would be modified.

By way of example, in both the administrative and judicial spheres, an important date is the date of registration—that is to say, the moment in time when a document or file reaches the administration. However, something extremely important in the judicial world and that may not be so relevant in the administrative field is the date of distribution from the registry to the judicial body that will hear the case. For this reason, this date of distribution would become an essential metadata in the justice sector exchange environment.


PUBLIC SECTOR
JUDICIAL SECTOR
Content
Metadata
Administrative body code
Date of registration
Judicial body code
Date of registration
Date of distribution
Electronic signature
Formats
DOCX
PDF
PDF
RTF
Exchange scheme
<node ap>
<bp node>
<cp node>
<node aj>
<bj node>
<cj node>

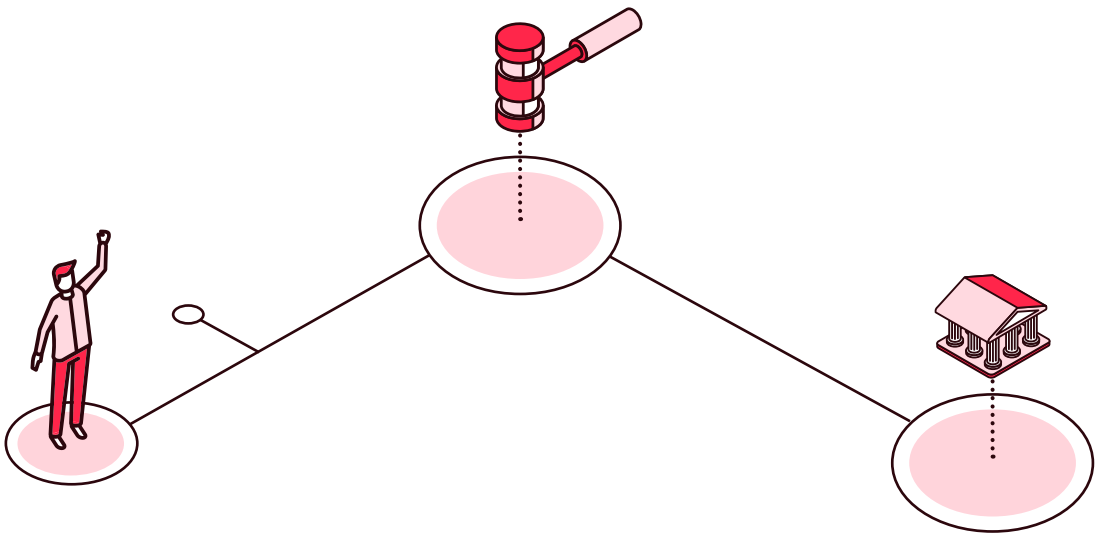
In this way, through the application of a top-down technical normative design methodology, cross-cutting, flexible, and reusable normative infrastructures would be created for all sectors, reducing the cost of maintenance. It should be noted that prior to the creation of such structures there must be a consensus in the legislative body or committee, because the general structure must be respected to ensure interoperability between sectors.

ASPECTS PRIOR TO ANY ACTION

- **Catalog of applicable standards:** As mentioned above, there are nationally or internationally recognized standardization organizations, so it is advisable, before developing public technical standards, to identify the set of applicable technical standards of these organizations that could be reused and referenced. It should also be borne in mind that the use of this type of technical standards entails longer and less flexible processes for their modification, so it is advisable to analyze the advisability of their use.

- **Governing body of the regulatory framework:** When defining the applicable technical regulatory framework, it is advisable to establish a coordinated national strategy in this regard, as mentioned above, establishing reference technical regulatory architectures that can subsequently be adapted by sector.

- **Reference standards:** When developing technical standards, it is advisable to analyze the development of standards in other countries to identify synergies and lessons learned that can be applied internally.



STORIES

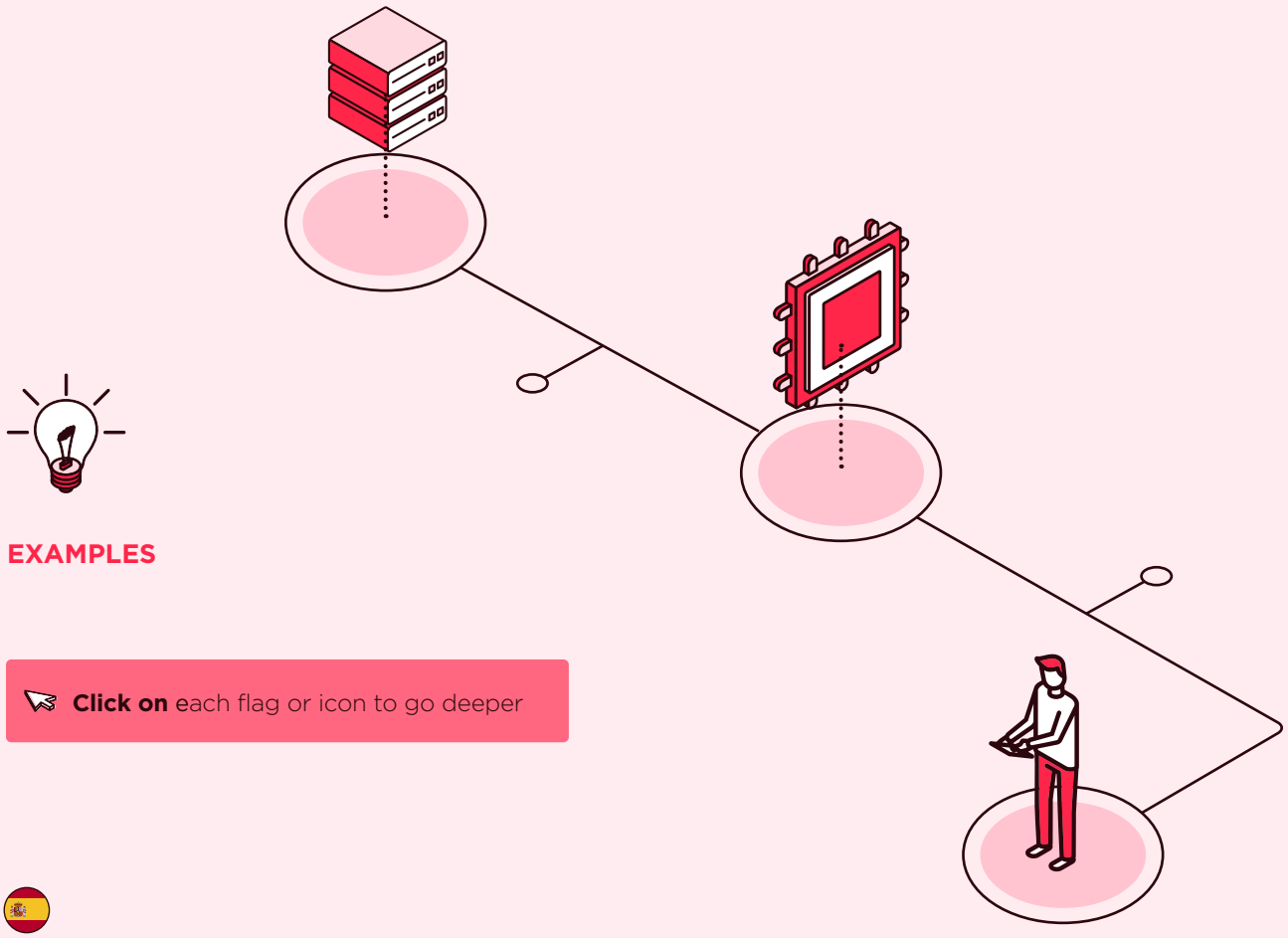
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders.

Citizen
Camilo

Camilo has decided to subscribe to the electronic notification service in his country, initially provided only by the Ministry of Finance and the Ministry of Labor. He is very happy because he receives all notifications on his smartphone, and he can also open the documents and electronic files he receives. After a few months have passed, he realizes that he can also receive notifications from the hospital where he is treated and from the general traffic directorate, and for this he did not have to do anything. He is surprised that, regardless of the sector providing the service and the difference in the content of the documents and files he receives, he can access all services from his smartphone in the same way and without having different applications.

Vice minister of health
Sara

Sara has authorized the incorporation of all hospitals to the state's cross-cutting electronic notification platform, where in addition to sending notifications, attached information such as electronic documents and files can be sent. After a few months she is surprised by the speed with which they have been able to incorporate the entire network of hospitals to this service. She asked the technical managers of the project, who told her that the incorporation was relatively simple, given that the notification system is completely standardized, which allows integration with very clear technical criteria.



EXAMPLES

Click on each flag or icon to go deeper

Spain
Regulation of the Electronic Administration (Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations).

Spain
Regulation of the National Interoperability Scheme (Royal Decree 4/2010, of January 8)

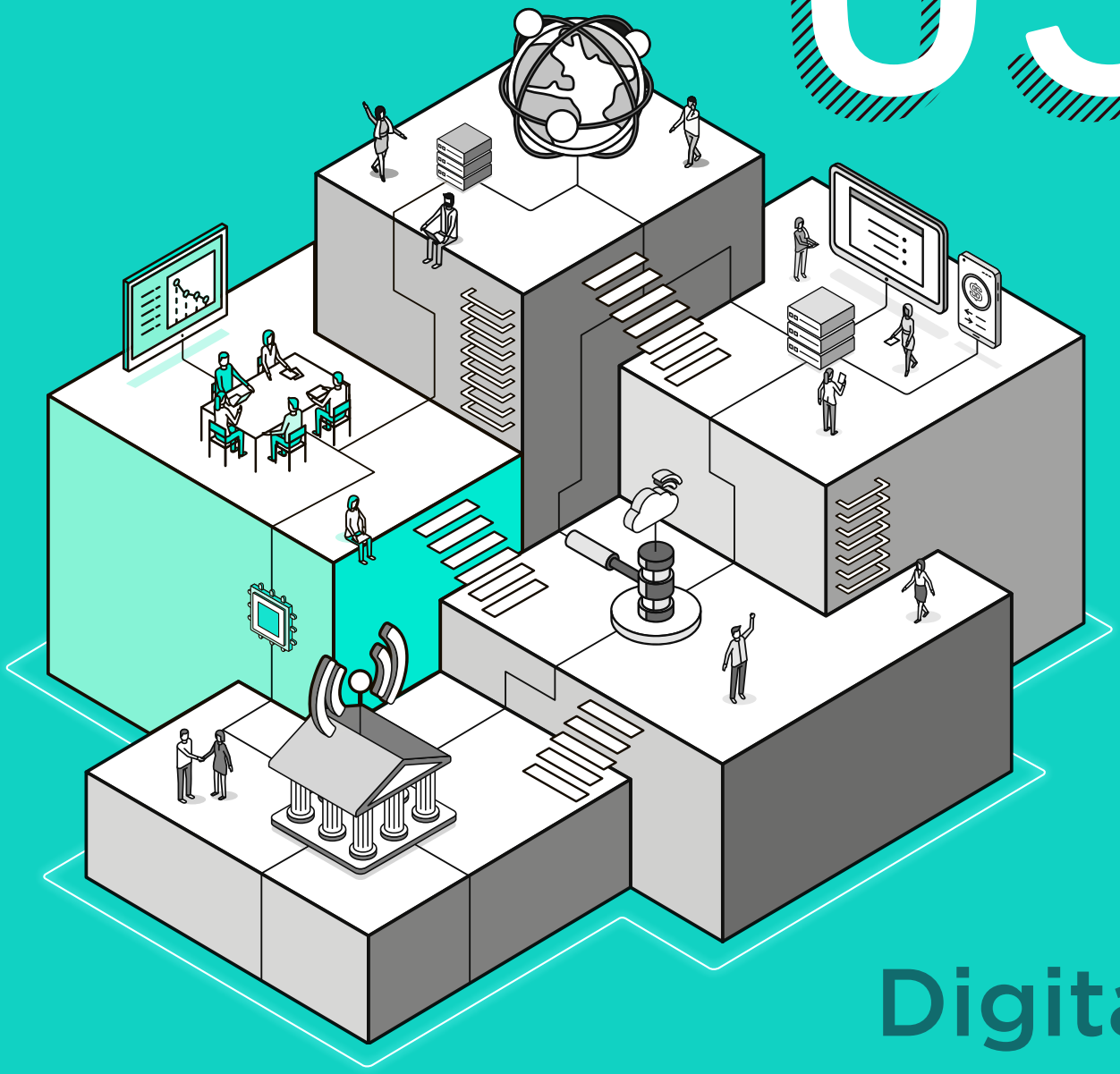
Spain
Technical regulations

Dominican Republic
Cross-cutting regulations related to the use and implementation of information and communication technologies, management of web portals, interoperability between government agencies, among other issues of national relevance.

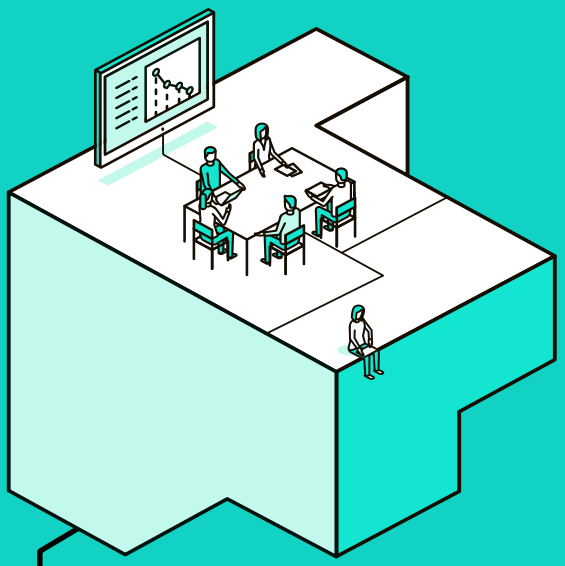
Chile
Standards and guidelines on digital transformation, including the *Technical Guide for the Integration of the Single Key and the Document Management Guide,* are available on the Digital Government portal.

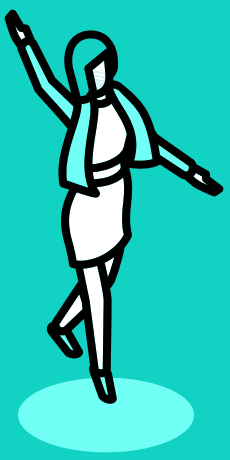
CHAPTER

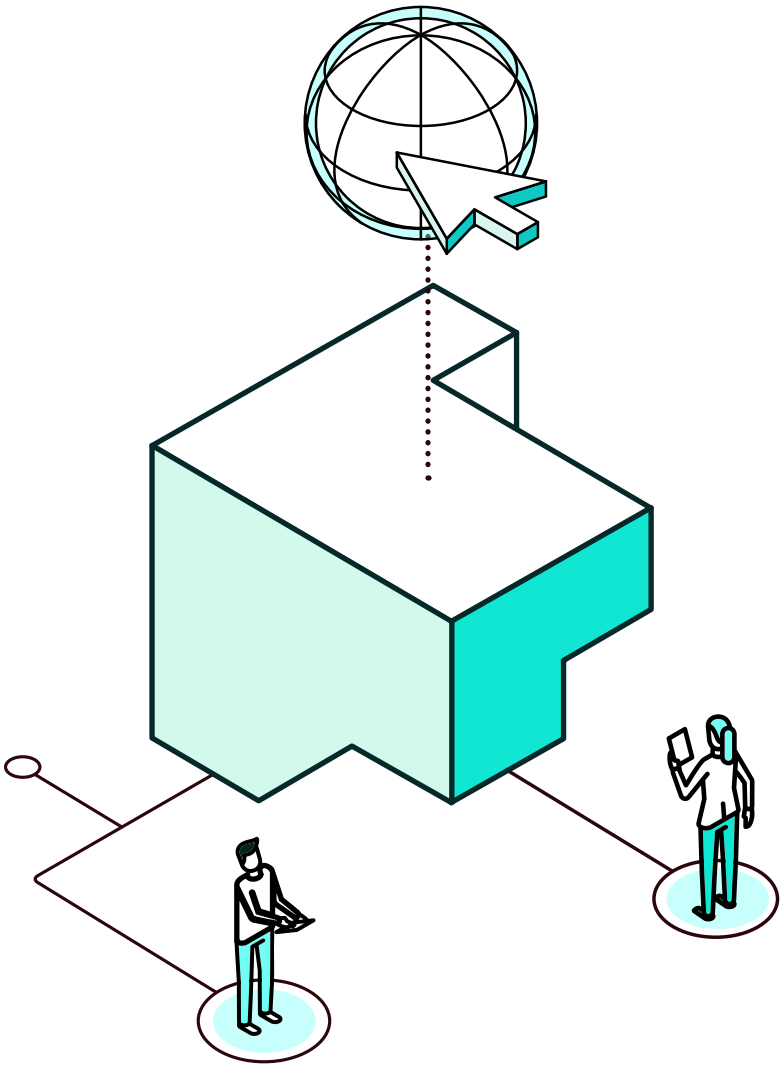
03



Digital talent and change management

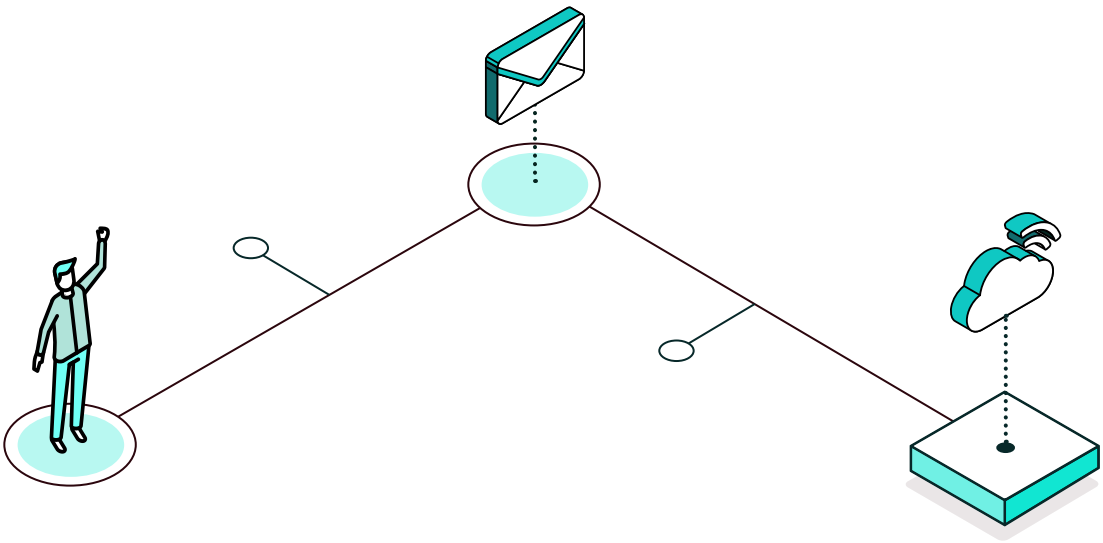






3.0

Introduction



A sine qua non factor for the development, implementation, and adoption of a country's digital transformation is human talent. The different roles required for this transformation—be it the creation of tools, their implementation, or their use—require different skills. Often, these are new or underdeveloped, so specific efforts are needed to fill gaps. These are not only hard skills in technology, but also soft skills:

- understanding of digital and its possible applications (e.g., for leaders of public institutions)
- communication, negotiation, and persuasion (e.g., for those in charge of implementing digital systems that modify or replace existing systems)
- computing and internet use (e.g., for users, whether citizens or companies)

This section describes different approaches to address the talent gaps that digital transformation can expose, as well as the new positions that become essential on the road to a new digital administration, or how to manage change in the administration and public employees. In this way, the following topics will be addressed, in order.

De tal forma, se abordarán, en su orden, los siguientes temas:

The importance of having the right positions to lead and manage digital transformation.

The training of public employees

Change management

The relationship with the citizen

Public-private collaboration

THE IMPORTANCE OF HAVING THE RIGHT POSITIONS TO LEAD AND MANAGE DIGITAL TRANSFORMATION.

Key positions such as the CIO, the CTO, the CISO or even the CDIO, if created, are fundamental figures that have in their genes to ensure the success of these transformation processes. It is absolutely necessary to break with past models of ICT management to move into new management formulas, more agile and above all collaborative, with specific roles and oriented to product and customer. In addition, the key figure of the *sponsors* or agents of change will be explained, who are often the real heroes of the success of digital transformation. These are the profiles of public employees who champion the transformation process and promote it among their colleagues, acting as the tentacles of those responsible for digital transformation at headquarters and offices.

THE TRAINING OF PUBLIC EMPLOYEES

Is a fundamental element to ensure that they have the necessary knowledge to face the new administrative processes, a new digital workplace. Generating specialized training itineraries focused on the different roles of the organization will ensure the training fit in each of the profiles. Undoubtedly,

training, and the more personalized the better, has a direct influence on the motivation of public employees and, therefore, on the transformational capacity. Public employees feel that they are part of the change and confident that their knowledge is adequate to face the transformation.

CHANGE MANAGEMENT

Is possibly one of the most important aspects in ensuring the success of digital transformation. There are few things that generate as much return on investment in this type of project as making the users who are the object of the digital transformation feel that they are part of the change and the main actors in it.

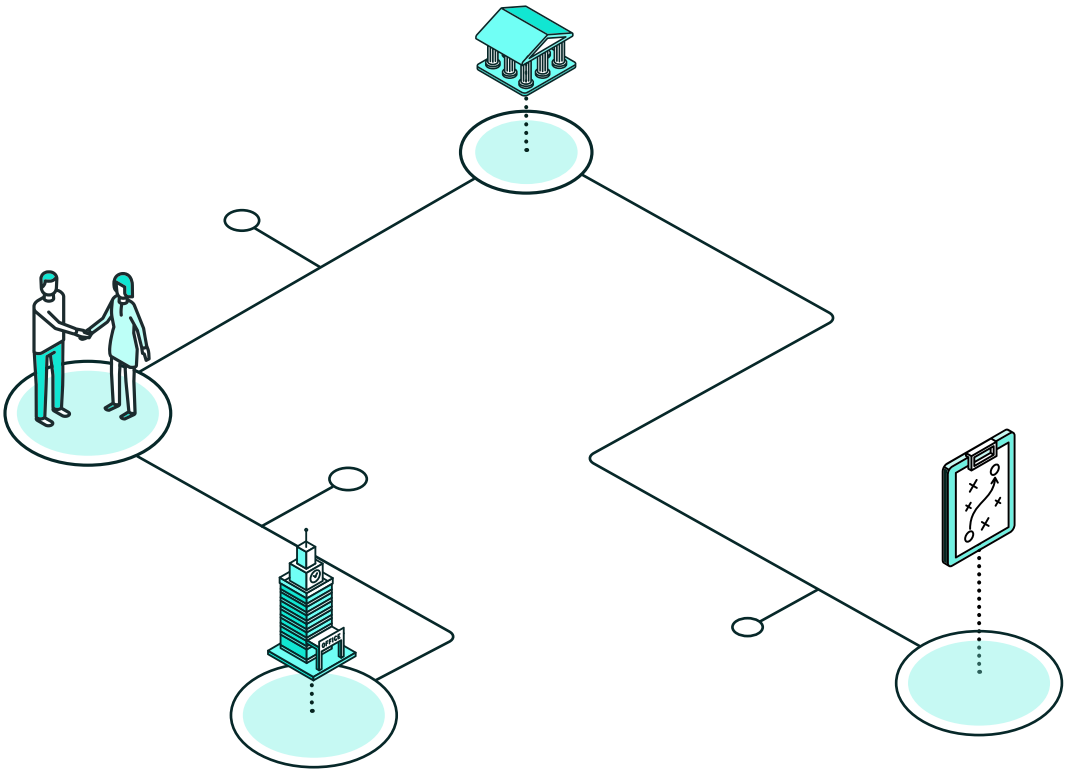
Endomarketing techniques or internal communication become key aspects to be dealt with internally, but in these strategies the external part is not usually given relevance. However, the identification of the main stakeholders that will be affected or the communication channels with them will be of vital importance to ensure that all these *stakeholders* are being managed, from an expectations point of view, in an adequate manner. In this sense, active listening also becomes one of the main tools because, as in the private sector, there is nothing that satisfies users more than being listened to, heard, and having their requests or needs met. Thus, active listening should focus on understanding what users need and what new tools should be adapted to be more useful or ergonomic (from a digital point of view, of course), since, in many cases, the first versions of information systems that are created do not fit 100 percent to the reality and needs of users. For this reason, the public employees who are going to use the new information systems must participate in the design phases of the applications, but they must also have an active voice when making requests and suggestions on the successive adaptations of them.

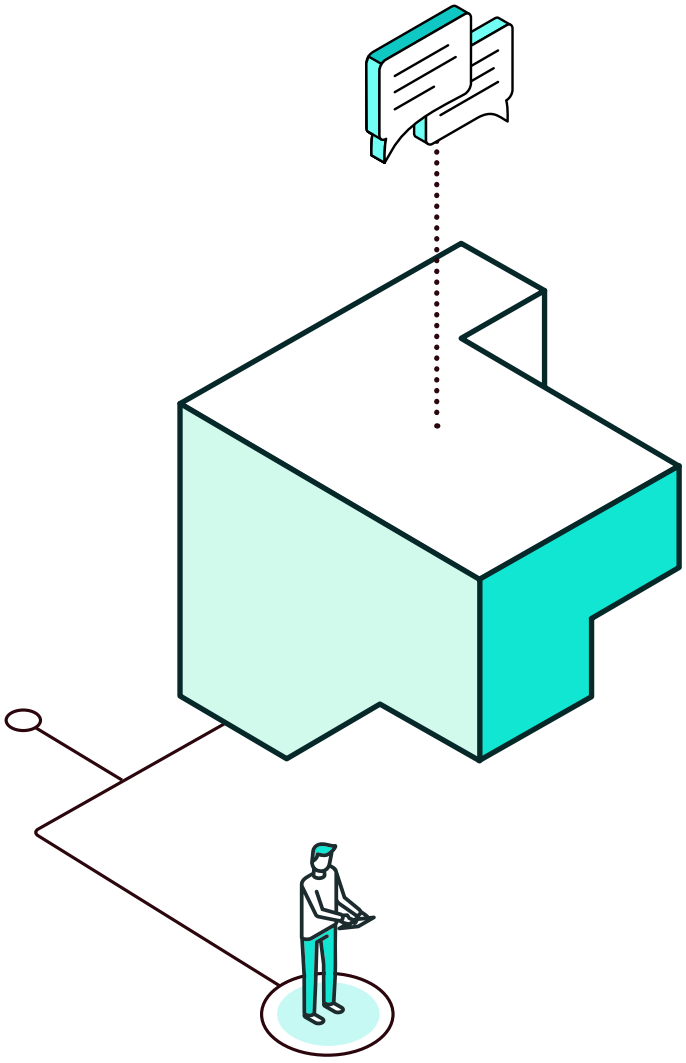
THE RELATIONSHIP WITH THE CITIZEN

This is the final link in the chain, the objective and the reason for these transformation processes. It is the object and responsibility of the country to work actively to ensure that citizens have better digital training and, therefore, as far as possible, to close the digital divide, enabling digital services to have an increasingly greater penetration and use. That is why it is so important to work on a good strategy and regulations for accessibility and usability, as it will ensure that digital services are easy to use for citizens with limited knowledge or experience related to information technologies.

PUBLIC-PRIVATE COLLABORATION

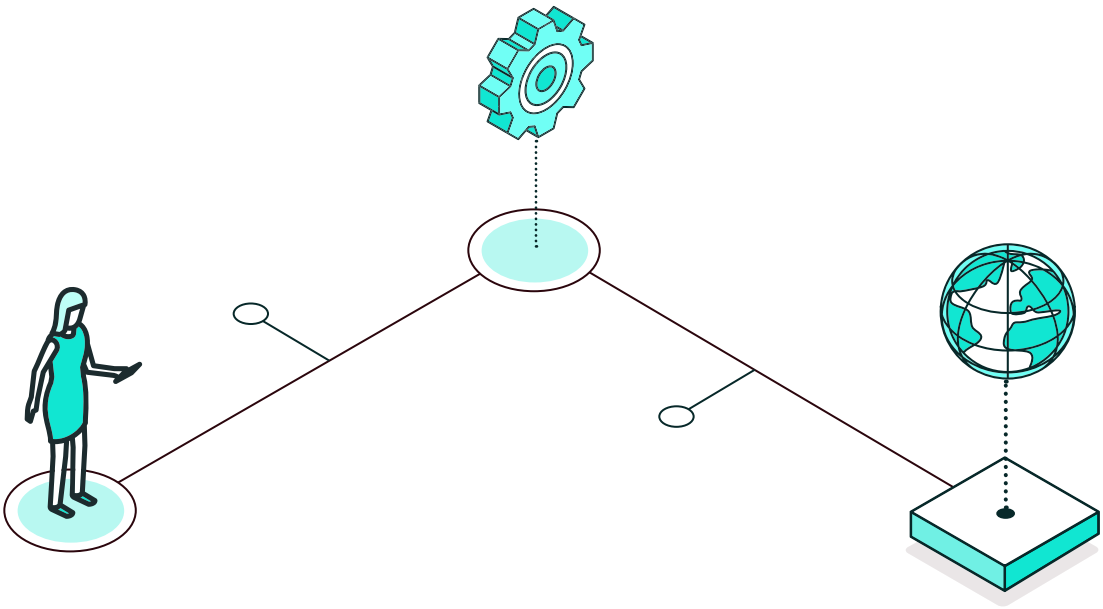
This aspect is closely related to the rest of the headings in this section, since it is clear that the administration alone cannot work on digital transformation without the need to interact with the private sector. It is precisely the private sector where innovation is usually generated, where investments are made in new technologies and algorithms, where much more specialized profiles are usually trained. This is not due to a lack of investment by the public administration or a lack of capacity of its public employees, but mainly because, due to the legal security of administrative procedures, these are usually much more rigid and slower than in the private sector. For this reason, in large digital transformation processes it is absolutely essential to cooperate actively with the private sector, seeking alternative forms of collaboration and financing that allow the administration to take advantage of the flexibility of the private sector, without violating the legal security of its procedures. At the same time, the private sector should be able, in this way, to grow the economy and participate in the digital transformation of the administration, of which it is undoubtedly both a provider and a user.





3.1

Key roles for a digital government



The world is changing, and the administration is no stranger to this. Public agencies are facing challenges and situations hitherto unknown, and this is driving them to develop with greater demand and speed a digital transformation that allows them to meet the demand and digital expectations of citizens and companies with which they interact, especially those younger citizens or more dynamic companies in the use of technologies. In many cases, they are being required to reinvent the way in which they interact with them, in order to provide a more agile response to their needs.

In recent years, even before the COVID era, it was common for the public administration to carry out transformation initiatives aimed at optimizing its resources and operational processes to improve its services. However, this is no longer enough. This last year has seen a true digital revolution caused by the change in relationships and in the way we operate, and this has also been transferred to the way we relate to the public administration. The level of demand and the demands of citizens and companies is much higher, and therefore the IT areas of public bodies not only need to adjust and optimize the way in which they operate and provide services to citizens, but must also meet these new demands with agility and with the incorporation of innovative delivery and service development models.

As an IT area, then, questions arise such as the following:

- What do I need to do to optimally meet the new demands?
- What IT organizational model do I need to be efficient, reliable, and resilient, yet agile, flexible, and innovative?
- What figures and roles does a public body need to lead the digital transformation?

In addition, consideration should be given to the coordination required between the leadership positions of the digital transformation lead institution and the digital transformation leadership of the vertical sectors, a matter discussed in more detail under the heading of lead institution and governance mechanisms.

Before answering these questions, we first show which aspects should be considered key in a digital transformation process. This will allow a better understanding of the new needs at the organizational level, the competencies of these key figures, and roles within this transformation process.

KEY ASPECTS OF DIGITAL TRANSFORMATION

Simplicity of the IT ecosystem

Spending efficiency

Fostering innovation

Agility

SIMPLICITY OF THE IT ECOSYSTEM

Complexity represents the natural state of an IT environment. The recommendation is always to seek maximum simplicity in all IT dimensions (organization, processes, information systems, infrastructure, etc.). That is why strategies to use cloud environments and services should always be present in the transformation approach of the business architecture of any organization, of course, with a technology leader with the ability to address these changes.

FOSTERING INNOVATION

The IT department must become a true digital innovator, becoming an ally of the organization's management. They must work in a coordinated manner to help the organization develop new digital services for the citizens and businesses with which it interacts. As a lynchpin and essential component of the development of innovative digital services, and therefore the path to digital transformation, we will find ourselves with the ability to address a strategy and revolution in the way information and data assets are managed. The leadership taken in this area will also be critical to the success of the agency in its transformation process.

SPENDING EFFICIENCY

One of the most frequent concerns that often arises is the perceived lack of visibility into spending and the level of quality of services provided within the IT area. Improving the alignment and processes of all levels of IT spending should also be one of the priorities of any digital transformation process.

AGILITY

The top management of an organization, understood as the so-called C-levels (Chief x Officer), is facing an unprecedented level of change in their organizations. The aim is to create cross-functional teams that can respond and create new IT services on demand through agile working models.

THE CATALYST FOR CHANGE OR TRANSFORMATION IS USUALLY DOMINATED BY ONE OF THESE FACTORS. BY PUTTING THE FOCUS ON ONE OF THESE DIMENSIONS, AT THE EXPENSE OF THE OTHERS, YOU SIMPLY TRADE ONE CHALLENGE FOR ANOTHER.

THE ROLE OF THE C

Given the current economic context, agility and the promotion of innovation C-levels should be considered as the most relevant pillars to develop any transformation process of any public administration organization. Therefore, it should be those C-levels of the IT area who lead this transformation, specifically the following:

C-LEVELS OF THE IT AREA

CIO - Chief
Information Officer

CDIO - Chief Digital
Information Officer

CDO - Chief
Data Officer

CTO - Chief
Technology Officer

CISO - Chief Information
Security Officer

Sponsors

CIO – CHIEF INFORMATION OFFICER

The CIO is the head of an organization's IT area or department. Traditionally, his figure has been associated with the establishment and planning of technological actions for the optimization of the IT operation management model. However, in the last decade, their functions have been continuously rewritten, leaving aside the more operational responsibilities and becoming true "partners" or strategic managers for public organizations, working together with the rest of the staff in the management of other areas or departments. This, however, is not enough: nowadays, the heads of an organization expect the CIO to also drive innovation and new ideas that benefit citizens and companies—in short, to lead the digital transformation of public services.

The CIO's functions are therefore expanded or, better said, reoriented. His more operational functions, as the person responsible for managing the IT function, must be delegated to other IT management profiles, while he must focus on revitalizing the relationship with the heads of other areas or departments of the organization and orchestrating the availability of those innovative IT services required by the organization to fulfill its functions and responsibilities. The aim, then, is to provide technological services that enable the organization to respond effectively to the new digital demands of citizens and businesses.

Main characteristics to be evolved in the CIO's functions

- **Moving from operational manager to leader of the agency's management:** No one doubts the value of technology in fulfilling an agency's responsibilities. This is why the CIO must become a key figure and a full member of the organization's management. Given this less technical and operational vision of the CIO, he or she is expected to advise and guide the board in the use of technology and contribute to the improvement of the public services provided from a strategic point of view.

- **Focus on improving public services:** The CIO is expected to prioritize IT effort and spend on initiatives that have the greatest impact from a citizen service point of view, while reducing and optimizing internal departmental effort and simplifying the management of the IT operations underlying the service delivery itself. Outsourcing services or strategically leveraging cloud or Software as a Service (SaaS) initiatives will facilitate this.

- **Coordinate with other management profiles in the IT area:** The CIO must also assume the role of leadership and coordination of the other management profiles in the IT area of the organization in any digital transformation process.

- **Being an entrepreneur, creator, innovator, disruptor:** Instead of fulfilling and responding reactively to the needs expressed by the rest of the organization's areas to perform their functions, they expect the CIO to be visionary and entrepreneurial, capable of identifying new opportunities to improve services to citizens and to be more efficient and differentiated with the support of technology.

- **Go beyond their technological capabilities:** The CIO is expected to have strong leadership, communication, and motivational and inspirational skills. He or she must be a role model and, as such, must have the influence to attract and retain talent.

- **Adopt an agile model:** The continuous emergence of new technologies and the need for an agile delivery model are key elements in the bid to compete and meet the needs of citizens and businesses. This forces IT areas to adopt agile operational and organizational models, with cross-functional teams and simplified governance approaches. The CIO must be one of its greatest advocates and one of the leaders of this cultural change in the IT organization.

- **Defending a data-driven organizational model:** Making efficient use of an organization's information assets (becoming a data-driven organization), interoperating, and making them available to third parties (reuse of public sector information) are of significant importance in any digital transformation process. The CIO, supported by the CDO, must take responsibility for leveraging the information managed by the organization and exploiting it as a source of value for the development of new services.

In short, there are many responsibilities that fall on the CIO in a context of digital transformation: he must assume new functions with a more entrepreneurial, innovative, and disruptive character to guide this new transition path to make his organization completely digital, while continuing to attend to his responsibilities in the more operational part of the management of the IT operation. However, in many public organizations, this situation is not viable, and part of these responsibilities are delegated to other profiles, or, directly, the leadership for the digital transformation is assumed by another profile.

CDIO – CHIEF DIGITAL INFORMATION OFFICER

A new role, the Chief Digital Information Officer (CDIO), is taking the lead for digital transformation. He will act as a catalyst and driver of change. He will bring a new culture, mentality, and new ways of working in the organization. In short, it is the person who assumes the most innovative, entrepreneurial, and disruptive functions in the company. To carry out his or her functions, the CDIO generally reports directly to the CEO and has the capacity to coordinate the CIO, other leaders or managers from management, or other units of the organization, and, of course, those leaders or *sponsors* identified in the change management process.

Areas of competence of a CDIO

- **Innovation and digital fluency:** It was previously mentioned that innovation must be part of the culture and DNA of the organization in any digital transformation process. It is not enough to only develop new technological solutions or new services that are made available to citizens and companies; it is necessary to go a step further and really build a culture and a model that allows the continuous generation of innovative and differential solutions. In this context, a leader is required to drive this culture throughout the organization and take responsibility for the associated change management process.

  Many organizations consider that this function should be carried out by the CDIO instead of the CIO, who is usually more focused on the operational part and, on many occasions, "putting out fires," rather than on the development of the innovation culture. The CDIO, therefore, will be in charge of initiating and supervising any innovation process that is developed in the organization, but he/she should not do it alone or with his/her team; it is necessary to also involve managers from other areas that have been identified as key people in the change management process. In this way, the innovative initiatives that are launched will have the appropriate level of penetration and assimilation to become part of the organization.

  The CDIO should also incorporate the CIO in this process. Technology must enable the tools that allow this cultural change and also go through its own innovation process that facilitates the development of digital solutions required by the organization.

- **Data-driven model:** Although it might seem that leveraging data for the benefit of digital transformation should be the responsibility of the CIO, it is appropriate to create a center of excellence in charge of developing the skills, competencies, and solutions needed for this purpose. The question here, then, is who should be responsible for this center of excellence. It seems appropriate that it should be the CDIO, provided that the organization considers the processing of all its information and the development of analytical solutions for the creation of new innovative services to be key to the transformation. The CIO, in collaboration with the CDO, will be in charge of the data platform and the rest of the pieces that will make up the global ecosystem of data management and integration.

- **Adoption of the agile model:** The adoption of an agile model should not only be taken to the IT environment, where the CIO has full responsibility, but it should be applied to the entire development life cycle of innovative digital solutions, from its initial phases of discovery or ideation to its subsequent prototyping and final development of the product or service. It is in these initial phases where the CDIO has full responsibility. As a key figure of innovation and ideator of new disruptive services for the organization, it is the one who must:

    - Promote the adoption of agile models for the creation of new services.

    - Assume full responsibility in this initial phase of service discovery together with your team of experts and other key figures belonging to other areas of the organization.

Subsequently, the development of the solution should continue with an agile model in the IT area, under the supervision of the CIO but always in coordination with the CDIO.

CDO – CHIEF DATA OFFICER

In addition to the figures of the CIO and/or CDIO as key roles in any organization's digital transformation process, there are also other IT management profiles that must be in perfect coordination with the CIO. As mentioned above, the development of a global data management strategy and the orientation toward a *data-driven* model will be key in promoting innovation in the organization and are therefore fundamental pillars of its digital transformation. In this context, the figure of the CDO emerges, who, in coordination with the CIO, will assume responsibility in the data center of excellence for developing this strategy and will be its driving force from a technological point of view.

Responsibilities of the CDO

Like the CIO's functions, the CDO's responsibilities have also evolved according to the technological context. In recent years, there has been a true data revolution, also fostered by the growing maturity of cloud services and the development of new analytical techniques for information processing. This has also led to significant changes in the competencies of this role, going from being responsible for data management and governance to having responsibilities in the digital transformation of the organization and in the development of services for citizens and companies.

Therefore, there is a qualitative leap in the CDO's responsibilities. In previous years, the CDO acted as another IT manager who provided support to the CIO to provide services required by other areas of the organization to improve and optimize its own activity. However, nowadays, in those organizations immersed in a digital transformation process, the CDO is already part of that innovative culture

and assumes responsibility for the cocreation of new innovative citizen services around data. Thus, he/she must be in charge of the following:

- **To propose the platform on which the new digital solutions should be created:** This should be based on the needs established by the CIO and other transverse leaders of the organization with responsibilities in the creation of such solutions. This platform should be raised in a general way, since it is not scalable to give particular solutions based on a particular unit or area of the organization.

- **Provide insights and new opportunities:** As an expert and responsible for the data area, you should enable the CDIO, CIO, or people involved in the development of new digital products to get more out of the data managed by the organization.

- **Promote the data culture, its interoperability with third parties, its reuse, and data analysis autonomously in the organization:** The CDO must provide the necessary tools, and of course access to the organization's global information (and other sources of public administration information), so that the agile teams in charge of developing digital solutions can use them. This autonomy will be key in the adoption of an agile work model and the culture of innovation.

- **Incorporate a model of continuous improvement and maturity as a data-driven organization.**

CTO – CHIEF TECHNOLOGY OFFICER

The CTO is the role that assumes the responsibility and technical direction of the IT area. As in the case of the CIO, their functions have also evolved in response to the demands of citizens and the digital transformation of organizations. Digital transformation requires an organization to focus more on innovation and the incorporation of emerging technologies, and this requires a technology leader and visionary, someone with a vision of how new technologies can transform the agency's service-delivery model and who can advise the CIO on decision-making.

However, this does not mean that other functions of a more operational nature, also associated with the CTO, are no longer his or her responsibility; quite the contrary. The CTO must also be responsible for establishing an efficient model for the operational management of the IT area. The CTO's responsibilities have therefore evolved and expanded along the same lines as those of the CIO. His role remains complex and multifaceted. Generally speaking, the CTO must support the CIO and work alongside him or her to ensure that the technology and IT organization are enablers, not barriers, to the agency's digital transformation.

Main areas of responsibility and functions of the CTO

- **Facilitator of the development of digital solutions:** As part of the development of new digital solutions, the CTO also plays an important role as an IT expert, aware of the technological trends in the market and the use that other organizations (and private companies) are making of them in their innovation models. Therefore, we could say that the CTO is a "driver" or "prescriber" of new technologies in the organization to be incorporated as part of the development of new innovative services.

- **IT alignment and responsibilities of the organization:** The CTO, as the IT area's chief technology officer, must ensure that the technology is being used correctly and that the organization's overall technology platform or ecosystem follows appropriate guidelines and guidelines that make the most of it to be used as part of the new digital services. It must act, therefore, as responsible for the organization's enterprise architecture.

- **IT Innovation:** The CTO must act as a technological visionary and a key change agent for the IT area. He/she must internalize the culture of innovation applied globally in the organization as part of the digital transformation process and transfer it, in coordination with the CIO, to the rest of the IT specialists and professionals in the area.

- **IT operation:** The CTO must be a person of total confidence of the CIO and, as such, must assume full responsibility for the day-to-day IT operation. This will allow the CIO to focus to a greater extent on other tasks of a more strategic nature and leadership of the digital transformation process. The CTO in the performance of these functions will have a closer relationship with IT suppliers and their contracting processes and will supervise the global IT service management processes.

CISO – CHIEF INFORMATION SECURITY OFFICER

When it comes to security, the *Chief Information Security Officer* (CISO) is the person in charge. This role is also essential to support the CIO's objectives.

Functions of the CISO

It could be said that, beyond the more operational part of IT security management, the CISO will have two main areas of action:

- **To make the agency see security as part of its responsibilities or functions:** The objective is to change the vision of security and technological risk management as a technical problem and bring it to a more strategic level. The agency must be "evangelized" about the benefits of investing in security and the value provided by proper compliance with adequate security policies. Therefore, it will be the responsibility of the CISO to develop processes that enable and facilitate decision-making on risk and other security issues (such as compliance with regulatory frameworks related to information security). In addition, they must develop processes and mechanisms to protect the agency from security threats or other cybersecurity events that could jeopardize the continuity of services to citizens and businesses.

- **Supporting the CIO or CDIO in identifying opportunities:** The CIO taking on greater responsibility as the leader of the digital transformation process and focusing his time and efforts on business development presents certain opportunities to other IT management profiles. In addition to having greater responsibility for the organization's security strategy, what is really a major change for the CISO is the possibility of also being involved in the development of new ideas and the generation of new opportunities or the improvement of services and products through the incorporation of the security dimension. The CISO must pay close attention to all the security aspects in the world of cloud services, artificial intelligence, or machine learning, and how these can provide greater added value to a given digital service.

SPONSORS

Beyond the leaders or main roles identified and described above, there is a profile that in most cases does not have the same recognition but is essential in any digital transformation process: the sponsors or agents of change that are scattered in the organizations, in different areas or departments. In the change management process, these are identified as those leaders who are sensitized, motivated, and involved with the change from its early stages and who understand that, from their area of responsibility, they must support change projects and initiatives.

What characterizes the sponsors of change?

- They are public employees of different ranks and levels and from different areas or departments with an interest in adopting digital trends to help the agency modernize.

- They begin first as digital advocates and, over time, become seasoned digital transformers.

- Although they do not always have the experience or authority to lead a transformation process

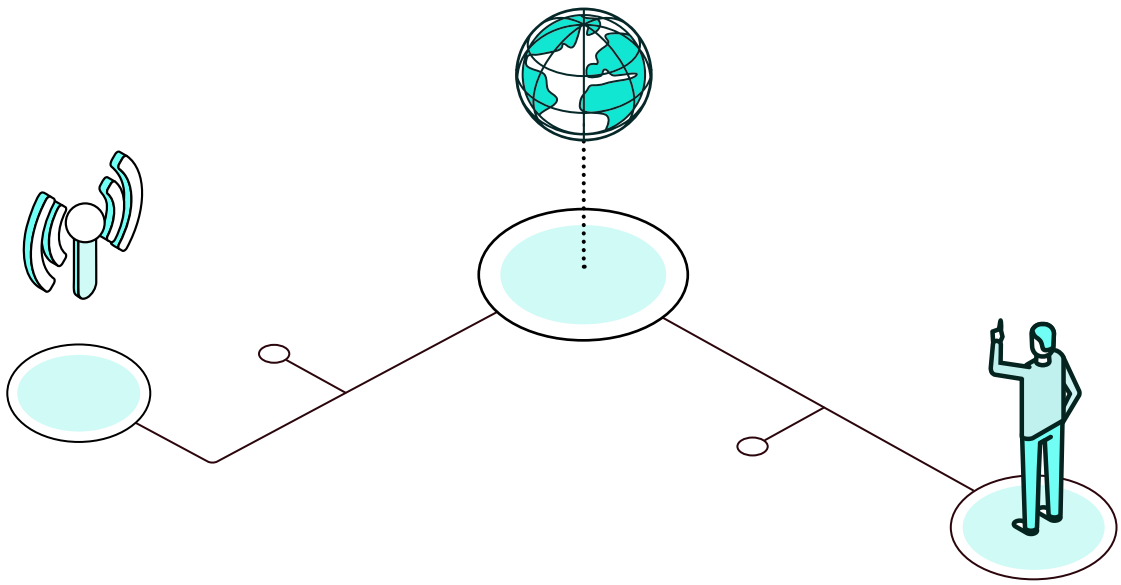
at a global level (for that the organization already has other roles as described above), they recognize the impact of digital and are motivated to help the organization adapt.

- They provide capillarity for the implementation of the principles and criteria established by the CIO/CDIO itself to bring about this change of culture toward digital. They are vital catalysts to promote initiatives and projects for the adoption of this new model and for the development of new digital solutions.

A VARIABLE STRUCTURE

In short, to achieve a truly successful digital transformation, it is imperative that governments adapt to the new organizational forms of IT governance. Thus, not only the institution leading the digital transformation, but also the different vertical sectors with responsibility for technology and digital transformation will have to make changes to their structures. There are different possible configurations and different scenarios that will have to be analyzed on a case-by-case basis. The CDIO/CIO/CISO combination must be tailored to each circumstance to provide the most effective results possible.

It is necessary to clarify that, obviously, depending on the organization of each state, the CIO/CDIO/CDO/CTO/CISO structure will vary to adapt to the most efficient solution. In smaller countries, it will be most common to find a CIO/CDIO at the national level with CTOs delegated to different organizations, or hybrid models in which there may be a national CIO and some CIOs in larger organizations with coordination between them. The same goes for the other figures, such as the CISO or CDO: it is usual for there to be a CDO or CISO at the national level and, depending on the size of certain organizations, new figures proliferate that hold these roles, which are so necessary in digital transformation processes.



EXAMPLES

Click on each flag or icon to go deeper.

Japan
Institute of Digital Government, Waseda University. They measure the development of e-government and take into account the figure of the CIO.

United States
CIO Council

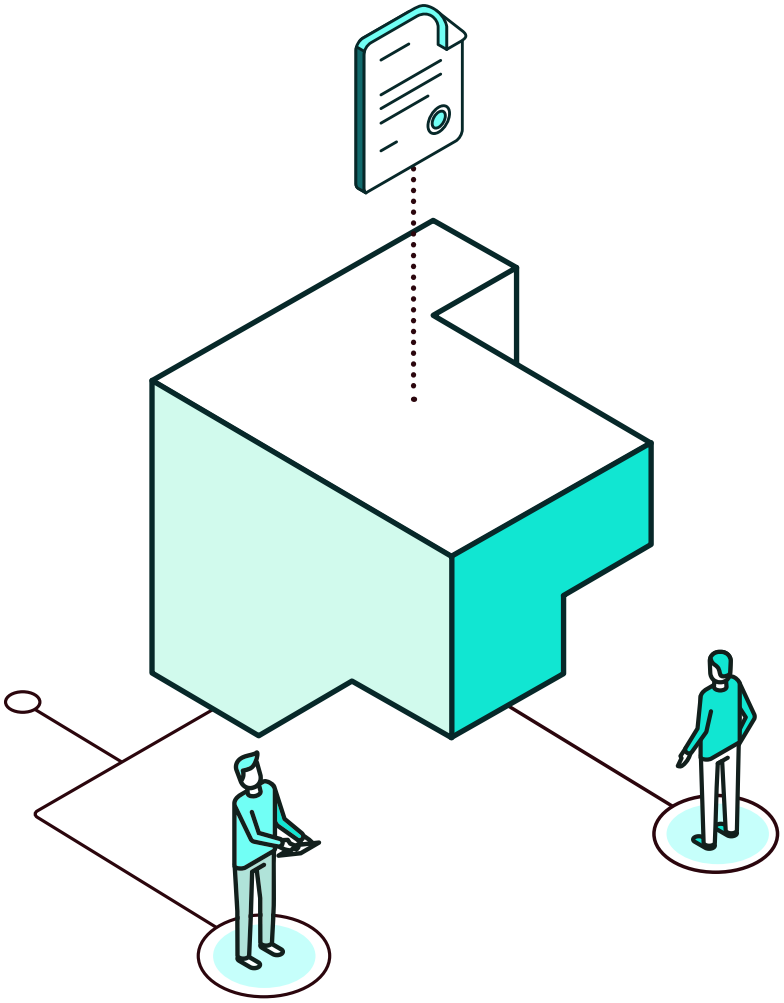
Turkey
Government Chief Digital Officer.

United Kingdom
IT Leaders.

INDICATORS

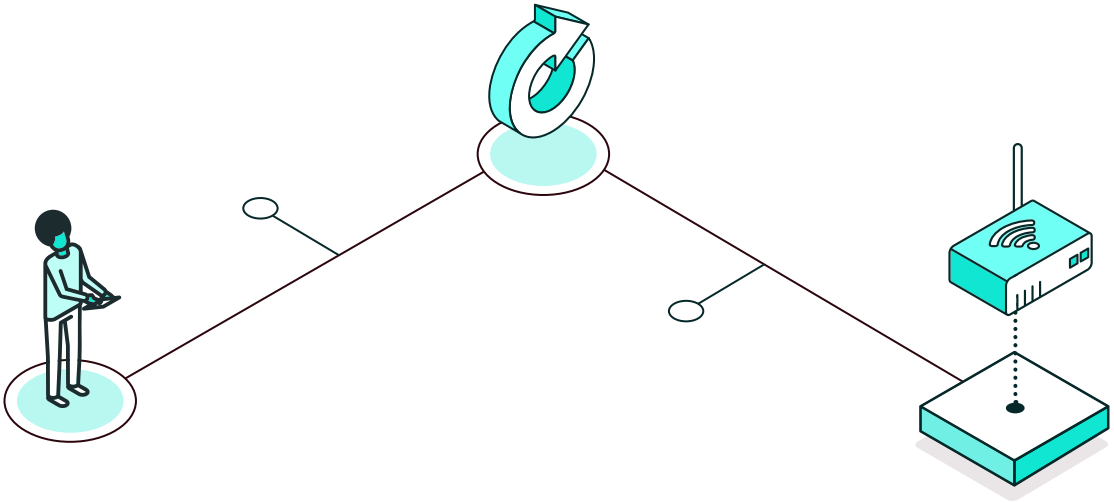
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there formalized roles focused on the digital transformation of the state?
- Is there a CIO/CDIO at the national level?
- Are there CIOs/CDIOs in other agencies?
- Is there a national CISO?
- Are there CISOs in agencies?
- Is there a national CDO?
- Are there CDOs in agencies?
- If there is more than one of the profiles described above, is there formalized coordination between them?



3.2

Training of public employees



Digital transformation has the potential to significantly change the tasks of public employees, eliminating some, modifying others and introducing new ones. This change may generate resistance, create capability gaps, or waste existing internal capabilities. Therefore, a strategy is required that responds to these challenges, facilitates the updating of knowledge and functions, and provides the opportunity for the human resources of public institutions to perform new functions and become agents of change.

Public employee training must be approached from this performance and productivity perspective, but also from the perspective of developing the interests of the public employee, to ensure that he or she is truly part of the change. In this sense, training should pursue a threefold objective:

- acquiring new knowledge and skills necessary for the productive development of the job or the transition to another
- fostering the personal and professional motivation of the employee
- strengthening the organization to which it belongs in order to achieve its mission and objectives.

Training represents one of the levers of the change management strategy in the digital transformation (together with others, such as communication), and must be conceived in a transversal way to identify the changes, diagnose the needs arising from them (new needs and current shortcomings), and define a road map or training plan, aligned and coordinated with the rest of the actions of the change management strategy. It must be understood as a continuous process, aimed at providing knowledge and competencies that improve performance and quality of life at work, involve public employees, and foster their commitment to the institutions and to transformation. *This continuous process should begin when the employee joins the administration*, based on his or her previous

competencies and skills and in consideration of the role to be performed, and should be progressive over time according to the transformations undertaken by the organization and its interests, in order to guide the employee's continuous professional development.

WHAT SHOULD THE TRAINING ENABLE?

From the point of view of each professional, the training should:

- develop specific competencies to meet the new challenges brought about by the transformation.
- enhance skills (both existing and new), knowledge, and experience.
- facilitate greater decisional autonomy for each professional, strengthening confidence and security, and reducing or mitigating the effect of change.
- improve opportunities for promotion and advancement.
- provide improved job satisfaction.

From an institutional perspective, it should:

- improve service quality and efficiency levels.
- make management more flexible in order to cope with rapid transformations and adaptations to the changing environment.
- provide the necessary conditions for each employee to contribute with his or her capabilities and performance to a better achievement of the strategic objectives and goals.
- detect talent.
- provoke leadership.
- encourage intrapreneurship.
- recognize and reward commitment.

THE KEYS TO A TRAINING PLAN

The training plan is a facilitating tool to help achieve the objectives of digital transformation. It must be focused and conceived from a strategic management perspective and not as an isolated effort focused on defining and delivering courses to meet the requirements of training hours per employee. Therefore, it is necessary to establish mechanisms for measuring the results obtained and for continuous improvement.

This instrument must be designed by each vertical sector and must be aligned with the global change management strategy defined by the lead institution. The plan will be structured taking into account the following premises:

Development of digital competencies

Boosting transformational leadership

A unique training tool

Definition of training itineraries by profiles

A unique training tool

DEVELOPMENT OF DIGITAL COMPETENCIES

- These are understood, from a broad perspective, as the acquisition of sufficient knowledge (know-how) and skills to use technological tools (know-how), innovate, and be able to make decisions (know-how) that contribute to the digital transformation of the organization to which they belong. In this sense, the idea is to develop a curriculum with at least four subjects of different nature, all of them related to the development of digital capabilities:

- **Subject 1. Soft skills:** As part of this block, actions will be defined that will serve to provide change professionals and leaders with the necessary tools to promote and implement change collectively and successfully within the organization. In this way, it will be possible to understand the overall strategic vision and mission.

- **Subject 2. Fundamentals:** Specific content on the implementation of projects under the selected methodological framework to address the digital transformation strategy. It has to do with the principles, procedures, communication mechanisms, and tools for the development of projects and new operations.

- **Subject 3. Digital: According to the publication DigComp 2.0:** *The Digital Competence Framework for Citizens*,[28] from the European Union's Science and Knowledge Service, there are twenty-one digital competencies that all citizens must currently have in order to participate in the information society. These fall into five areas:

  - Information and data literacy
  - Communication and collaboration
  - Creation of digital content
  - Security
  - Problem solving

  As part of the training plan, actions should be addressed within this subject to ensure the development of these digital competencies. This or another competency framework can be used to address this subject.

- **Subject 4. Technical:** Aims to deepen the specific technological concepts of the digital transformation strategy and the tools acquired for its implementation. It involves the development of skills in the use of specific technologies specific to each sector, either proprietary or market.

28. DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. | EU Science Hub (europa.eu).

BOOSTING TRANSFORMATIONAL LEADERSHIP

- Usually, those in positions of responsibility may be the least aware of the changes involved in digital transformation and the most resistant to them, although they are responsible for leading, mobilizing the organization's human resources for action, and ensuring the benefits of the digital transformation processes. For all these reasons, it is necessary to focus on, train, and support the managers of the institutions in a special way. It is also common to have to make specific interventions in middle management, not only to make them aware of what can be done with the new tools, but also to radically change some processes in order to make them more effective, considering—precisely—that digital transformation changes the way of doing things.

DEFINITION OF TRAINING ITINERARIES BY PROFILES

- The profiling must have been previously carried out within the change management strategy in a broad sense, segmented by leaders (top management), middle management, and technicians. It is necessary to gather in a single journey, and by profile, the following actions:

  - **Initial training (onboarding):** Influences the experience of the public employee from his first days of work. The actions defined will be aimed at optimizing the adaptation time of the new professional (informing about the organizational structure, processes, and tools) and involving him/her in the transformation process from the beginning, fostering commitment and loyalty to the administration's project.

  - **Continuous training:** Acts on identified and/or anticipated needs and, based on these, determines the most specific training actions, adapted and aligned to the organization's transformation strategy and the continuous development of professionals to generate digital competencies linked to job performance. It allows functions and personnel to be reoriented, without resulting in a situation of extensive redundancy of personnel.

  - **Specific training:** Involves actions aimed at recognizing and rewarding the performance of those professionals who are most committed and involved in the digital transformation. They are not, therefore, part of the common itinerary, but are specific in terms of the development of professionals with greater predisposition and talent. The aim is to create valuable programs with itineraries linked to career performance and leadership.

A UNIQUE TRAINING TOOL

- The institution must make available to all vertical sectors a tool with the following main functions:

  - serve as a portal for dissemination, support, and consultation for professionals, so that they can consult the training offer, register for available courses, and have access to a library of training materials
  - enable management, monitoring, and evaluation of the training plan
  - make space available to carry out training activities
  - share and manage knowledge, either explicit (documented as the library of materials) or tacit (not formally documented)

TRAINING SUPPORT DIDACTIC MATERIALS

- These must be available in different formats and have high pedagogical quality, so that they offer training support or are the fundamental training solution for learning. In the current context, we have to bet on digital contents in order to offer multimedia presentation forms, animated formats, and audiovisual material that bring the professional closer to knowledge in an attractive way. In this sense, and given our habits of agility and immediacy with respect to digital channels, it is worth highlighting a type of material that is increasingly widespread and especially valid for reinforcing knowledge, expanding and complementing information: *microlearning.* These are digital content 3.0, distributed either through videos or short pills on a specific topic and structured around a clear and concrete learning object, in order to maintain attention and improve retention of concepts. This type of content is ideal to be consumed either when a professional has a specific need, or in the so-called valley moments, since they require less time and availability.

SECTORAL TRAINING PLANS

Each vertical sector must in turn create its own training plan based on the change management strategy, taking into account the resources available and the training methodology. This plan should be developed (not only reviewed) on an annual basis to update, incorporate, or maintain in force those actions that are key for the organization. Specifically, the main activities to be carried out for the development of these specific training plans are described below:

Diagnosis of training needs

Definition of the training itineraries for the different profiles

Description of the training actions

DIAGNOSIS OF TRAINING NEEDS

- This should be based on the mission and vision of the digital transformation strategy, the organizational culture of the vertical sector developing the plan, and the programs and projects that are part of the digital transformation. It is necessary to analyze the impact that will be generated in the processes and in the current way of working, in the professionals and in the organization itself, identifying the barriers and resistances that can be generated before the change and detecting the needs. In addition, it would be relevant to specify the segmentation of the impacted professionals (training profiles) in accordance with the general framework and adapt it according to their particular idiosyncrasies, number, distribution, and impact of the change.

DEFINITION OF THE TRAINING ITINERARIES FOR THE DIFFERENT PROFILES

- For this it is necessary to consider the objectives of the initial, continuous, and specific training for each of the profiles. The itineraries gather all the training actions to be implemented during the year for a specific profile. The profiles will be used to group those with common needs and simplify the number of itineraries for easier planning. This will be beneficial not only in planning, but also in execution. The needs are analyzed separately and then content blocks containing different training actions are created.

DESCRIPTION OF THE TRAINING ACTIONS

- The plan includes the details of all the training actions to be implemented, the selected methodology, and the didactic contents, as well as the duration, the schedule, and the place where they will be carried out. The training actions may vary between lectures, monographic training sessions, best practices, working groups, etc., being flexible in design to adapt to the needs of the company. They are flexible in design in order to adapt to any of the situations required. It is advisable to innovate in the type and methodology of the actions to generate commitment and interest in participating. Each training action will contain, at least, the following information:

  - Target groups (i.e., the training profiles to which it is addressed). It should be taken into account that the same training action can be present in more than one itinerary, since it applies to more than one training profile.

  - Quantitative goals or objectives, based on the following:

    - potential students, based on geographic distribution and, if applicable, organizational distribution

    - expected objectives (percentage of trainees trained/percentage of potential trainees).

  - Description of the pedagogical modality to be followed in the training (face-to-face, online, or blended).

  - Means or training materials required according to the established contents and the pedagogical modality.

  - Method of evaluation by training action (developed below).

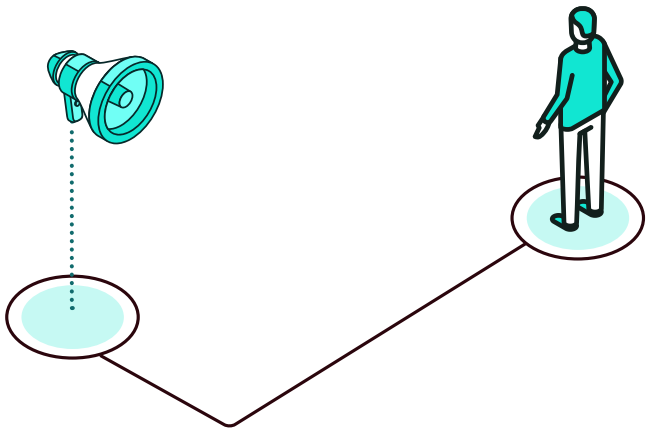
  - Timeline.

A NEW WAY OF LEARNING

As indicated above, the plan will be made up of different training actions that will be developed combining both the online modality, through the Learning Management System, and face-to-face and *blended* (or *blended*) training. At this point, however, a new trend is to be noted, which incorporates the *synchronous modality of online training*, implemented through virtual classrooms for the delivery of lecture sessions. In this way it is possible to share, in real time, the following:

In reality, it is developed as a traditional lecture methodology, where there is an expert teacher, a small group of students, a planned agenda, and the date, time, and duration for the training session; the only difference is that the session is mediated by technology, which allows the use of virtual classrooms instead of physical classrooms. This has the following advantages:

- audio and video
- presentations
- desktop and applications
- virtual whiteboard
- session recording
- chats
- quick surveys



- **Flexibility:** Professionals can choose when to take the training at the time and/or day that best suits their needs and interests, without it interfering with their daily work and improving the perception of training, which is conceived more as a service than as an obligation.

- **Efficiency**: It avoids travel, consuming only the time necessary for training. This eliminates the feeling of wasting time.

- **Quality:** An expert trainer is available to the professionals at all times. Given that the trainer is also relocated, the best professionals can be called upon for this role. The number of students per training action is much smaller than when it is carried out face to face, since there is no need to make the most of the space (an average of five students per training session in synchronous training compared to an average of fifteen students in face-to-face sessions). Obviously, attending to a small group of five people allows for more individualized and higher-quality teaching.

TRAINING FOLLOW-UP

Finally, it is necessary for each vertical sector to build a model for monitoring and evaluating the training plan. This does the following:

- It allows to know the degree of compliance with the objectives.
- It helps in defining more effective training plans.
- It contributes to the monitoring of the change management strategy led by the lead institution and to the continuous improvement of training and sharing experiences and results with other vertical sectors and showcasing their success stories.

The monitoring model will make it possible to measure the training plan, taking into account four aspects:

- **Quality:** Assessing the satisfaction of professionals with respect to the entire training cycle.
- **Results:** Related to the number of professionals who successfully complete the training actions. Indicators are established, such as total number of training actions, total number of professionals trained, total percentage of attendance according to type of training, or total percentage of dropouts in each action.
- **Efficiency:** This has to do with the number of resources that have been necessary to satisfactorily achieve the quality and effectiveness indicators proposed in the training plan, with the benefits reverted on the organization and with the economic impact.
- **Impact:** Will help to understand whether the training has had a *positive impact on the performance of the professionals.*

All of the above provides an overall picture of the results and *impact of training as a lever for transformation*. It is interesting that the results, in addition to being reported so that they can be analyzed individually and as a whole, are shared, either in small working groups, made up of managers from different vertical sectors and rotating on an annual basis, or in large meetings where outstanding experiences are shared and solutions to common problems are proposed, or through both actions.

HIGHLIGHTING THE VALUE OF INVESTMENT IN TRAINING AND THE ADVANTAGES IT OFFERS IN THE TRANSFORMATION PROCESS ENDORSES THE TIME AND RESOURCE EFFORT MADE BY ORGANIZATIONS AND ENSURES THAT THIS KEY PART OF THE DIGITAL TRANSFORMATION IS NOT ABANDONED OR UNDERVALUED.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara conducts periodic evaluations of perception and results for the staff of her ministry. Since it became mandatory at the national level to provide short courses and summarized information on digital transformation to managers and middle management (for example, very short videos or manuals ideal for people who have little time), the effectiveness has soared because these officials now know the possibilities and have not only opened up to change, but also promote it. Sara is also happy because the Ministry of Modernization in her country has just included digital skills in all hiring processes to incorporate personnel. She feels satisfied because this means that new recruits will be prepared for the challenges that are likely to come in the next few years.

Mayor's advisor
Daniel

Daniel started last week in his new position as advisor to the mayor of his city. The city council where he works has an *onboarding* plan that includes a training itinerary for the first days of the public employee. Daniel appreciates these actions as they will help him to optimize his time and have a greater degree of adaptation in his new position.

Entrepreneur
Ana

Ana is an entrepreneur and passionate about technology. She tries to be always up to date and is bothered by tedious procedures with the administration. However, lately she finds well-trained professionals who know the tools and make her life easier. Her perception of public service is changing.

EJEMPLOS

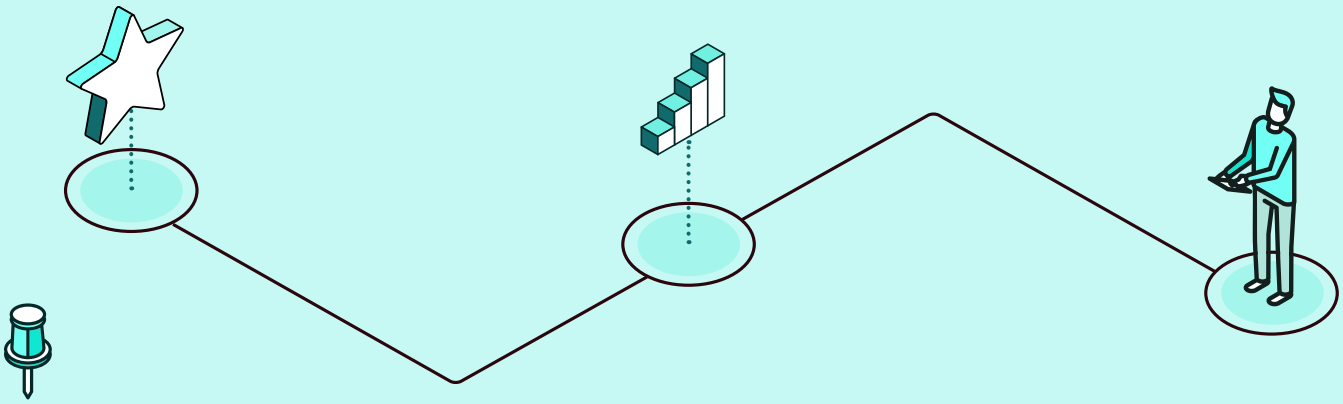
Click on each flag or icon to go deeper.

Korea
National Human Resources Development Institute

Canada
Digital Academy

United Kingdom
Collection
GDS Academy courses

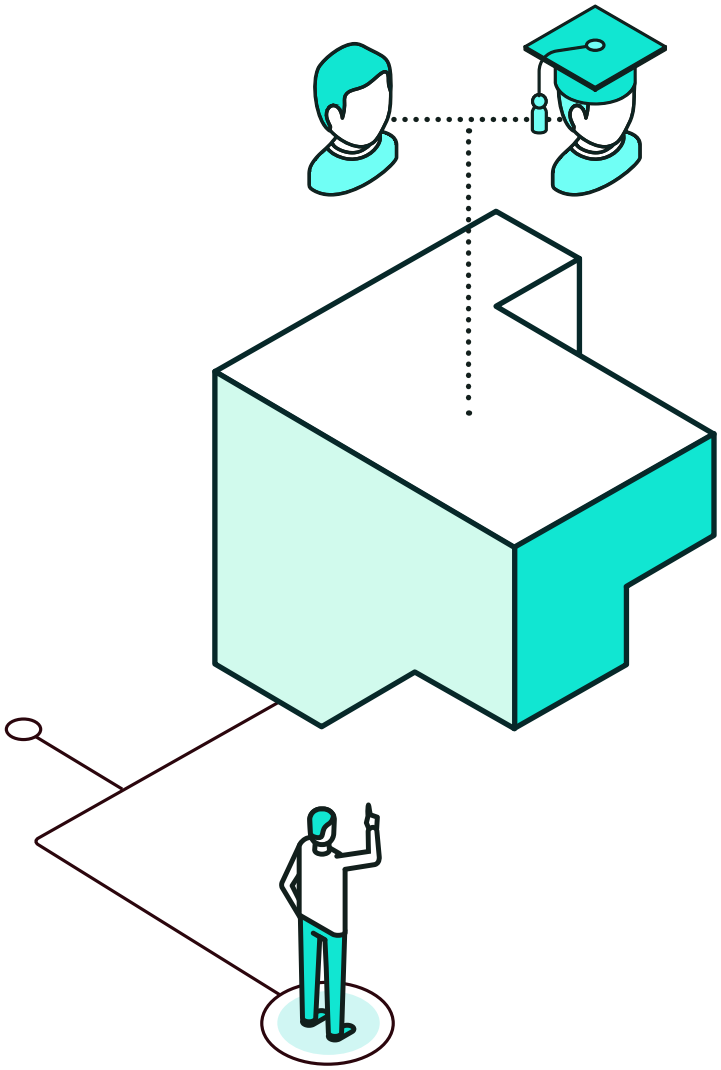
Spain
The National Institute of Public Administration



INDICATORS

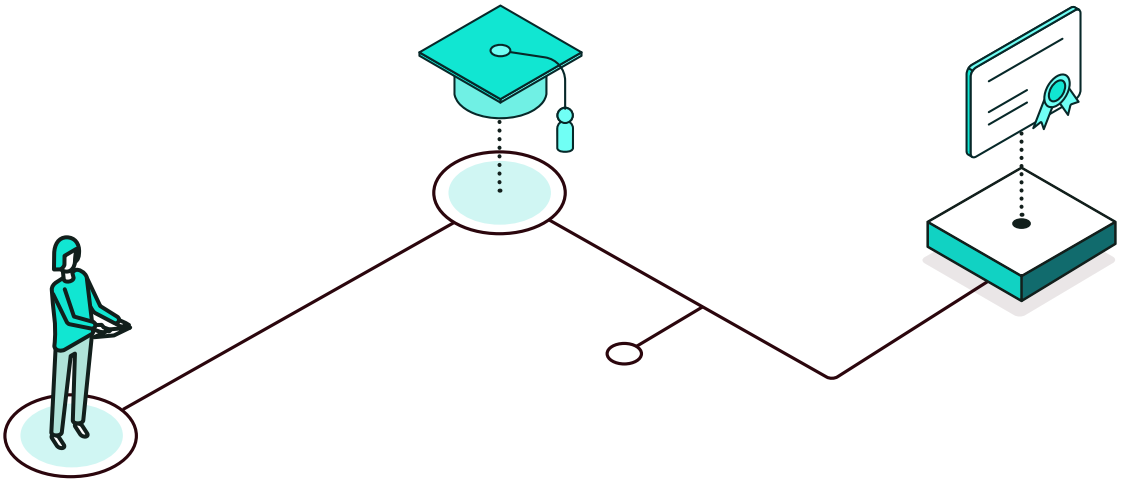
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a training/training plan or something similar on digital issues for public employees? If so, does the plan contemplate the following:
  - Specific actions for managers?
  - Training in advanced topics (e.g., data analytics)?
  - Training on good governance issues and/or the promotion of citizen participation?
  - Change management training?
  - Content on new ways of working (e.g., agility, citizen-centered design)?
  - Collaboration with educational institutions in the country?
- Is there a unified training access tool for public employees?
- Are there specialized training itineraries by profile?
- Are there specialized onboarding trainings for new staff members?



3.3

Organizational change management



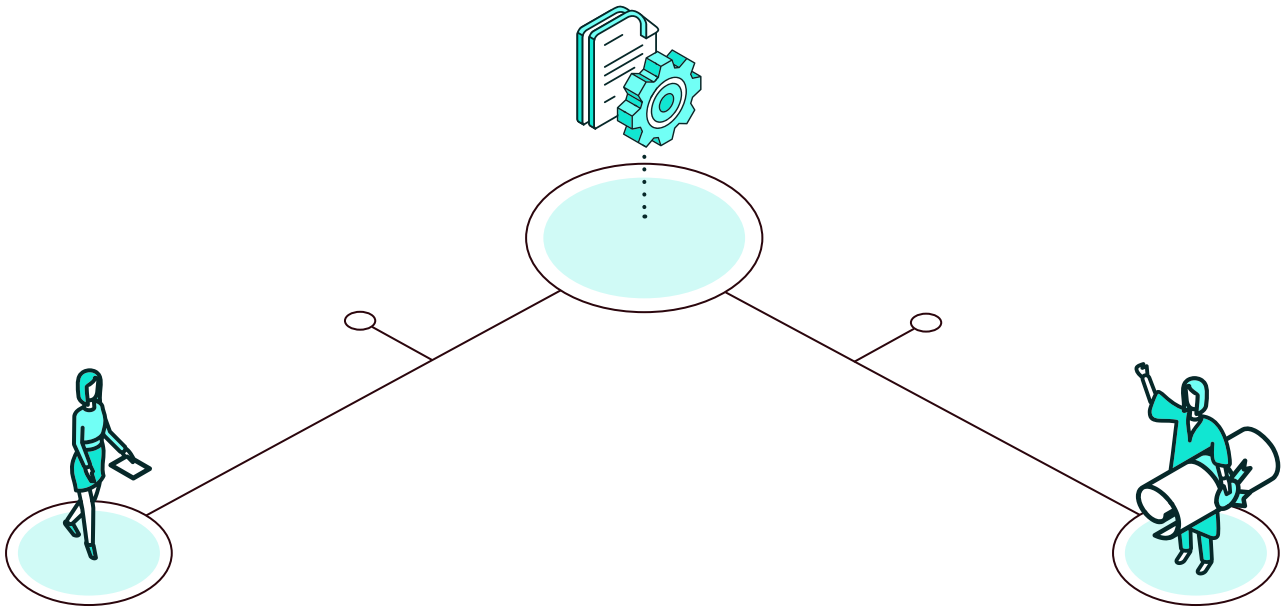
Digital transformation implies a paradigm shift, both in the internal workings of the public administration and in the way in which public institutions and the citizenry or the business community relate to each other. Although in net terms these changes will be positive for all the groups involved, at the individual level they may generate resistance, in some cases as a product of inertia—that is, people are used to doing things in a certain way that the digital transformation bursts in (for example, the citizen who asks for a permit and waits for the paper with the stamp as proof of the procedure duly done). However, in other cases, resistance may be due to entrenched interests: people may be benefiting from the *status quo*, which is suddenly threatened, from the civil servant whose tasks will cease to exist to the entrepreneur whose business will become irrelevant. Since this resistance has the potential to hinder or completely block the advancement of digital transformation, it is important to identify and address it proactively. This section discusses a number of measures that can help smooth the transition.

When institutions or organizations face a digital transformation process, they focus their attention, investment and resources on the production, settlement, and evolution of services through their application portfolio. However, they leave in the background the origin and destination of the service itself, which is none other than people, usually applying less method, less investment, less structuring, and homogenization in the relationship, service, and support processes. In this sense, the efforts and resources made available are similar in all organizations. However, there is a big difference when it comes to how they have approached the adequacy of people in their digital strategy. *The human element is key* to achieving real transformation.

On the other hand, resistance to change, or rather, low confidence in such change, is a problem that management will face in its transformation process, and that can lead to frustration and demotivation, producing an adverse effect on the objectives that drove the transformation.

It is easy to understand that managing change is necessary, almost obvious; what is more complex is to understand why, for what purpose, how to do it, and with what tools. The fundamental objective of change management must be to obtain a high rate of acceptance and recognition of the services generated by the digital transformation. To do this, it will be necessary for the lead institution to set up a change management unit that provides comprehensive coverage to the vertical sectors and to all technological projects through a common strategy capable of providing homogeneity to the process, valuing the investment made in a planned manner and measuring the results systematically. Usually, these change management units, as well as their associated plans, are created for long periods of time, over the long term.

THE EMPHASIS ON METHODOLOGY IS ONE OF THE KEYS TO A GOOD CHANGE MANAGEMENT STRATEGY DUE TO THE IDIOSYNCRASY AND EVOLUTIONARY NATURE OF DIGITAL TRANSFORMATION PLANS.



SUCCESS FACTORS FOR ADDRESSING CHANGE

Create a specialized change management unit

Promote leadership alignment (*sponsors*)

Identify stakeholders

Use endomarketing techniques to build loyalty among users/benefactors of the services

Base the strategy on peer coaching and cascade training systems

Reuse of communication channels and omnichannel trend

Drawing up project-specific change management plans

The importance of support

Listening plan

Follow-up and coordination of the change management strategy

Evaluate the level of change adoption

CREATE A SPECIALIZED CHANGE MANAGEMENT UNIT

This specialized unit will be in charge of:

- covers all transformation projects;
- marks the change management strategy;
- defines a standard methodology;
- provides a cross-cutting service to all vertical sectors;
- shares resources;
- reaps the benefits of experience;
- ensures adoption of the change;
- is efficient, proposing as a maximum the protocolization of change management activities;
- is flexible, adapting to the reality and needs of each project;
- is sustained over time, by reusing existing resources and previous experiences;
- is methodical, designing a common framework to guide the implementation of all projects.

PROMOTE LEADERSHIP ALIGNMENT *(SPONSORS)*

It is not possible to carry out an agile transformation without leaders who are sensitized to the change from the early stages and who understand the scope of how it will be carried out and what they must do from their responsibility to support the projects. Sponsors must share the strategic vision, convey the objectives pursued, and act on the attitudes of the people over whom they exercise their leadership. The following are fundamental in this area:

- Identify such leaders/sponsors of digital transformation in the different vertical sectors.

- Define a leadership management plan that:
  - assesses the level of leadership commitment to the transformation plan.
  - reports on the scope of the plan.
  - defines the degree of involvement required for each leader.
  - identifies the key issues to be considered.
  - gives a traffic light to the level of risk detected.
- Know the type of leadership, perception, knowledge, and opinion of the leaders regarding digital transformation.

IDENTIFY STAKEHOLDERS

To do this efficiently, a *stakeholder matrix* can be created, one of the most important tools to support change management, which provides a complete view of the agents affected by the change. Based on this matrix, the following can occur:

- Potential conflicts are identified.
- The effort is more accurately dimensioned.
- Communication strategies are defined.
- Participatory approaches or reduction of the power of antagonism are promoted.
- The results of the agents' management activities are monitored.

The *stakeholder* diagnosis and matrix update will be live throughout the transformation. This implies that the instrument should be reviewed periodically to update its information to ensure that it includes all affected groups according to the status of the transformation plan and that its classification is correct.

USE ENDOMARKETING TECHNIQUES TO BUILD LOYALTY AMONG USERS/BENEFACTORS OF THE SERVICES

It is necessary to redefine the concept of user that we use to refer to the public employees affected by the transformation or to the benefactors of these services (either other professionals related to the administration or the public). A change management strategy must be built from a current concept, linked more to needs and interests (i.e., understanding the user as a customer of the services provided by the organization to motivate professionals to change).

It is useful for these purposes:.

- Design *endomarketing campaigns*, with clear objectives and detailed actions aimed at specific targets and measurement indicators.
- Visualize the technological systems and services as products/brands, implementing a commercial plan that includes the creation of a name, a logo, and actions for its launch where the benefits and advantages of the new product are clearly explained.
- Design innovative content for the new product or brand in different formats so that it can be disseminated in different channels.
- Use conventional marketing techniques, as well as the most innovative ones, to build customer loyalty for services and technological systems. In short, use sales techniques to sell the digital transformation. It will be the task of the governing body to select those projects/systems/services that, due to their impact, are propelled through these techniques, although all vertical sectors can propose others or address this strategy within their specific change management plans.

BASE THE STRATEGY ON PEER COACHING AND CASCADE TRAINING SYSTEMS

: Involving all public employees is the factor with the highest success rate when it comes to managing change. A nonaggressive way to achieve this is to use peer-to-peer training methodologies, which allow managing the know-how of the professionals who have participated in the definition of the transformation, since they will be the ones to train other professionals. The level of acceptance in peer-to-peer training is higher than when dealing with other external trainers, since they have the ability to focus more on the problems or shared perception and highly diminish the rejection or resistance to change.

It is interesting to create a network of internal trainers within the sector, with professionals from the different organizations, allowing their rotation according to the stage of the transformation, so that everyone can be trained or be a trainer. When the knowledge is not inside, it is possible to resort to external trainers and implement the cascade training system: from external knowledge to the network of trainers and to the rest of the organizations.

Cascade training is reliable as a training methodology since the fundamental objective is that the *training reaches the greatest number of people in the shortest possible time*, which will be one of the great strengths of the transformation projects. In addition, it has the following advantages:

- it unifies content criteria.
- it applies training to the reality of each territory, delegation, or center.
- it reduces the cost of travel (time and money).
- it shares experiences, time, and space with colleagues from different institutions.

REUSE OF COMMUNICATION CHANNELS AND OMNICHANNEL TREND

Over the last few years, administrations have made many efforts in order to have digital or analog communication channels for different audiences. These channels have been refined and generally work, have been internalized, and are part of the existing relational culture. Therefore, the following are recommended:

- Reuse efficient channels and influencers to convey messages of strength.
- Identify the communication channels established in the different sectors and their organizations, analyze which are the most efficient, and tend to unify them. It is not a matter of using all of them—only those that guarantee effective communication according to the transformation project being addressed.
- Create quality content only for the selected channels. It is not necessary to create new channels if the available ones work, and if not, they should be improved and adapted to the needs of the projects.

DRAWING UP PROJECT-SPECIFIC CHANGE MANAGEMENT PLANS

The main objective is to draw up a *Specific Change Management Plan* (SCMP) for each project, for which the vertical sectors will be responsible within the framework of the strategy. This instrument will contain all the necessary information on the project and the planning of the communication and training actions to be developed. The PEGdC will contain:

- the scope of the project.
- relevant milestones.
- objectives.
- training actions.
- the communication model.
- planning, resources, and measurement indicators that provide follow-up to the overall strategy.

THE IMPORTANCE OF SUPPORT

Another essential tool of change management is support. As important as training or communication, the implementation of good support, which works and is quickly and easily accessible, is key to the success of the strategy. Those impacted by the change need to know exactly what the support tools are, when they will be available, and how they can access them.

LISTENING PLAN

One of the key points of a change management strategy is listening. *Feedback* from technology users, product managers (systems), and support centers must be collected in a planned and deliberate manner. To this end, a listening plan can be created, which define:

- on which projects active listening will be conducted;
- improvement objectives;
- who are the agents that contain the valuable information;
- how this information will be collected and analyzed.

Support centers constantly receive a lot of information about what are the main aspects of a service or system that repeatedly does not work, is not usable, or more often is not accessible. This information, generally scattered throughout the organizations, is not analyzed even though it is a highly valuable source for decision-making. It is necessary to perform a conscious and programmed listening, which must be periodically reviewed and compared.

FOLLOW-UP AND COORDINATION OF THE CHANGE MANAGEMENT STRATEGY

It is essential and necessary to carry out the follow-up of the PEGdC of each project individually by each vertical sector. For this purpose, a Gantt chart or diagram, designed by the change management unit in its strategy, can be used as a standard resource that unifies the structure for monitoring each PEGdC. This standardization will allow the organization:

- Coordinate and follow up the execution of the global strategy, both in the internal dependencies of change management activities and in those that affect other projects, resources, sectors, organizational units, etc.
- Monitor each pegdc individually, which will facilitate the coordination, identification, and management of the dependencies that arise with respect to other activities of the transformation project it covers.

EVALUATE THE LEVEL OF CHANGE ADOPTION

One of the main challenges in a change management strategy is the objective measurement of the impact and progress achieved since, unlike other indicators, change management has an important qualitative component. The monitoring of indicators to measure the adoption of change is fundamental, as it justifies the objectives of the different change management actions. It also makes it possible to *evaluate knowledge, understanding, acceptance, and commitment to the implementation of the transformation.*

To assess the degree of adoption achieved, a *scorecard* can be drawn up *consisting of four blocks or dimensions of compliance, each with its own indicators (KPIs):*

- **Execution perspective:** This is to measure the degree of compliance with the change management strategy and its degree of progress and achievement. Indicators will be defined to obtain metrics of what was planned versus what was executed in terms of actions, recipients, time, and budget.

- **Stakeholders' experience:** Aims to provide information on the quality of the change management service and the consistency of the actions carried out with the expectations of those who are its benefactors. To measure this dimension, indicators of satisfaction and assessment of the perception of the implemented actions are usually used.

- **Impact of the actions:** These indicators measure the level of fulfillment of the objectives of the actions carried out. In the design of the change management strategy, strategic objectives will have been defined in correspondence with their measurement indicators. Thus, all the actions included in this strategy respond to the achievement of these strategic objectives through specific objectives. Indicators in this dimension are, for example, those that measure the level of learning achieved in training, or those that measure the understanding of messages in communication actions.

- **Behavioral change:** To assess it, indicators of acceptance, stabilization, and sustainability in the organizational culture, derived from the transformation projects, are defined. It is usually measured at three key moments during the implementation of the change management strategy:

    - At the beginning, before any action is taken.

    - When 50 percent of the strategy implementation has been exceeded.

    - At least one more time before the end of all actions, with the objective of being able to make decisions toward achieving change when there is still time and budget available to achieve it.

Continuous improvement underlies the entire evaluation process. It should be borne in mind that digital transformation takes place in an environment of innovation, dynamic and changing by the very nature of the development of new technologies and trends. This will mean that it will be necessary to review the strategy and adapt the actions planned to new realities and needs. However, the measurement and monitoring parameters should be sufficiently robust to be sustainable, since the main objective of the strategy is to manage change, whatever it may be.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo is characterized by his involvement in social issues that concern his municipality. The municipal government sent him a letter inviting him to participate in the project to modernize and digitally transform the transparency platform of his municipality. They wanted him and twenty other citizens from different fields and professional areas to take part in the round table where topics such as transparency, access to information, and citizen participation would be discussed so that they could contribute ideas and evaluate the existing systems.

Entrepreneur
Ana

Ana manages a company with two hundred employees and plans to grow this year and invest in technology. She wants to find information on grants for companies in her country to boost the digital economy, but the reference websites have changed, and she has been told that applications must now be processed online. However, Ana calls the support phone number and quickly accesses the information and manages her application more easily than before, and without queues and travel.

Vice minister of health
Sara

Sara is aware that digital transformation in the health field is an important step. This is why she wants to join forces in the team of health officials to achieve a real digital transformation in the processes. He has brought together fifteen people from his team to create a specialized change management unit. These leaders have the attitudes and skills to meet Sara's annual objective.

Mayor's advisor
Daniel

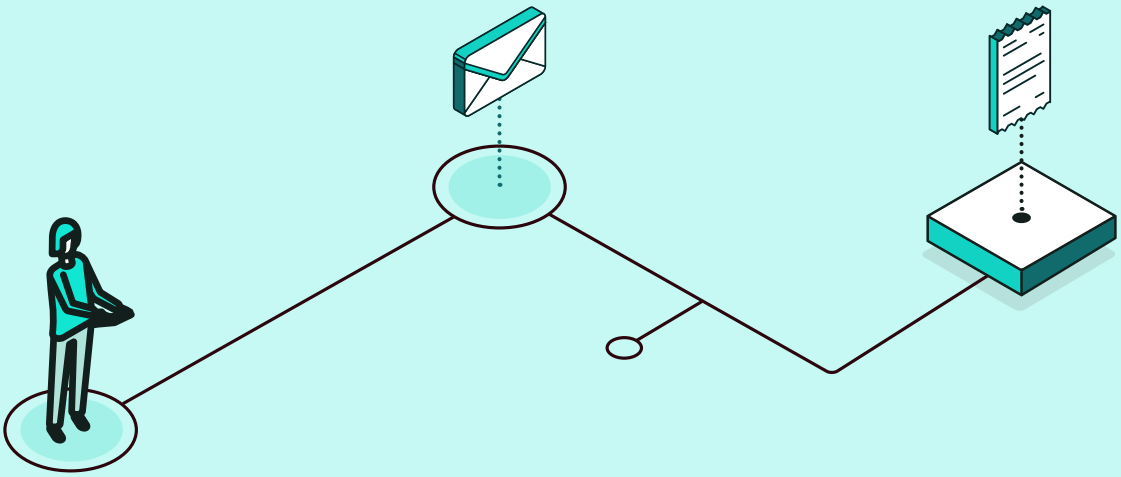
Daniel is a young, tech-savvy guy who is passionate about staying on top of digital trends. He has been approached to be part of the change coalition, so he will be a strong *stakeholder* to lead the change effort and ensure that the rest of his peers join him.

EXAMPLES

Click on each flag or icon to go deeper.

Spain
Proyecto de Gestión del Cambio para la Transformación Digital en la Comunidad de Madrid

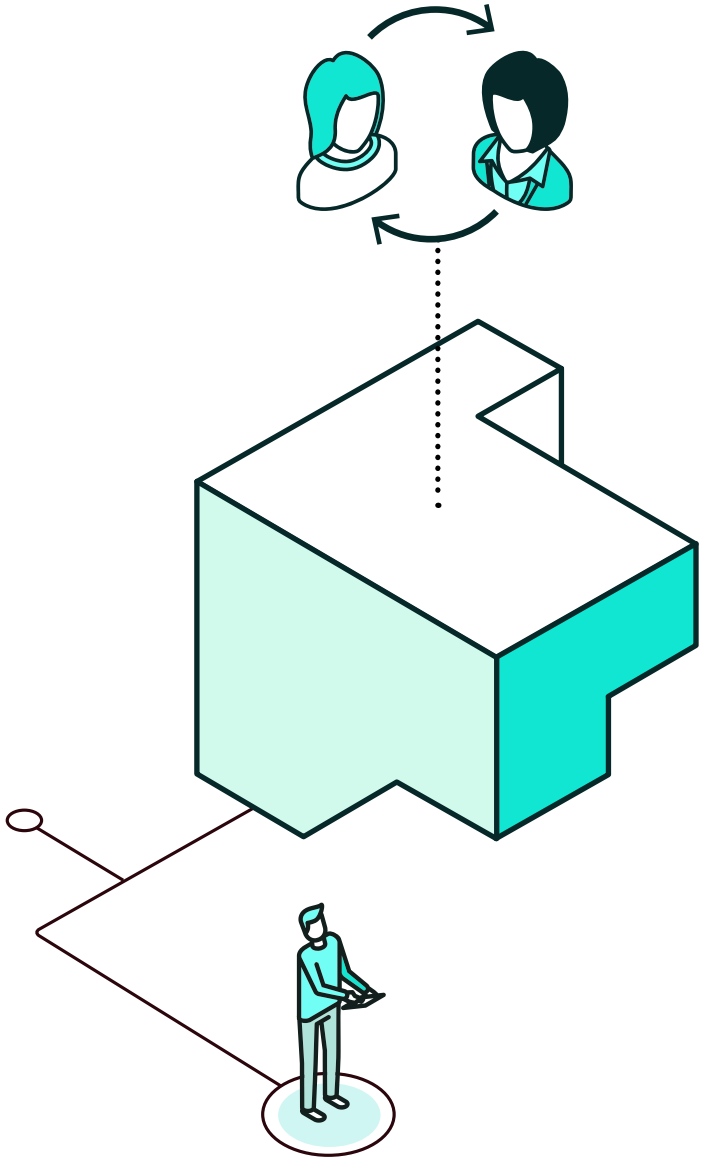
Dominican Republic
Change Management- Ministry of Public Administration



INDICATORS

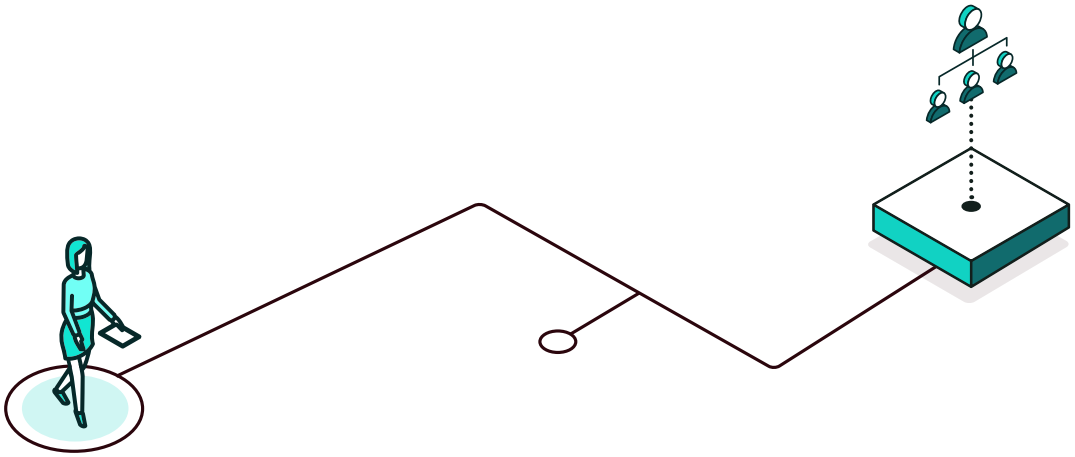
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is change management driven by senior government management?
- Have you identified the analysis of audiences that will be impacted by the change initiative in a stakeholder matrix?
- Do you have a communication strategy?
- Do you have an internal train-the-trainer strategy?
- Do you develop project-specific change management plans?
- Do you assess knowledge, understanding, acceptance, and commitment in the implementation of the transformation?



3.4

Relationship with citizens in a digital context



Digital transformation drives the creation of new digital tools, not only for training, but also for other purposes, such as optimizing the country's competitiveness, achieving greater access to citizen services, etc. Therefore, the educational and social system must be oriented to take advantage of them. Training is a key element in meeting three challenges:

- The danger of aggravating nonexistent inequalities in the country through digital transformation, which are deepened by giving greater benefits to people who are already more advantaged.
- That citizens can get jobs that require ICT knowledge and skills, both in the public and private sectors.
- Ensuring that digital solutions are used by as many people as possible.

LIKE ANY OTHER STRUCTURAL REFORM PROJECT, DIGITAL TRANSFORMATION GENERATES TENSIONS IN THE STATE AND ENTAILS THE RISK THAT CERTAIN DISADVANTAGED GROUPS WILL BE DISADVANTAGED, WIDENING THE GAPS IN SOCIETY.

Under the premise that all citizens have the same rights, in a country's digital transformation it is important to have an associated strategy that bridges the existing gaps in society (for reasons of location, economics, age, education, gender, disability, etc.). For example:

- If the rural environment is not connected and the city is, digital processing will save time and money in carrying out procedures for people living in the city, but not for those living in rural areas, which will increase inequality.

- If advanced services based on cell phones are implemented, those who have a *smartphone* will be particularly benefited compared to those who do not have a cell phone, thus increasing the differences.

It should be borne in mind that people who do not have the skills to interact digitally or who do not have access are generally those who have the greatest need to interact with the state. However, technology itself can lead to the reduction of these gaps if adequate planning is done to take advantage of this potential. As in all cases, the starting point must be a diagnosis of the situation, identifying the main gaps that exist in the country, and then palliative measures must be proposed for each of the areas and weaknesses observed.

SOME EXAMPLES OF ACTIONS TO REDUCE GAPS

- Promote the extension of connectivity to rural regions.

- Provide transactional services through telephone systems (which reduces rural, age, and educational gaps).

- Establish multiservice offices (also known as integrated service centers, ISCs).

- Incorporate clear language in communications (both written and verbal) of the public administration.

The important thing is that for each digital transformation project, the impact it will have on the gaps identified in the diagnostic phase should be studied, and corrective measures should be proposed to reduce them, rather than increase them. The incorporation of actions in each project is facilitated if there is a general framework—a plan or strategy—that generically identifies the types of gaps that may exist and the types of solutions that can be considered.

CITIZEN TRAINING

Special attention should be given to the citizen training strategy, which is a comprehensive plan that seeks to train citizens in new digital competencies that are either required or generate benefits in a new digital environment. This allows citizens to interact in a digital environment, be able to appropriate new digital solutions and benefit from their use.

In order for the citizen empowerment strategy to work, at the very least, it will have to:

- disseminate information about the digital transformation and develop a communication plan to raise awareness of the opportunities that this transformation brings with it.
- provide timely training for citizens to take advantage of the possibilities of icts, with transition plans in those abundant cases where operation is becoming increasingly digital.
- reorient the education system to take advantage of the new opportunities offered by the digital transformation.

DIGITAL TRANSFORMATION FORUMS

Another additional line of work in relations with citizens in the mission of minimizing the digital divide, and which in a broader sense also includes groups and companies, are the digital transformation forums. These are spaces for collaboration in which both public administrations participate, directly or through representatives that include all of them, as well as associations, companies, citizen representatives, and other prominent members of civil society or the private sector, to promote the digital transformation of the country in a collective and collaborative manner.

Public administrations interact with citizens, companies, and other public entities, who are affected by all digital transformation projects and whatever changes they imply. As such, it is common to organize formal forums where issues are discussed between institutions and where the actions undertaken are communicated so that citizens and businesses understand the changes they imply. These spaces are interesting to the extent that they give a voice to actors who, as well as being affected by the digital transformation, can be a fundamental part of its success.

IF THERE ARE FORMAL DIGITAL TRANSFORMATION GROUPS IN PUBLIC ADMINISTRATIONS, SINCE THE PUBLIC STAKEHOLDERS WILL BE SIMILAR, A GOOD PRACTICE MAY BE TO ASSOCIATE THE FORUM FOR COLLABORATION WITH THE PRIVATE SECTOR OR ACADEMIA TO THESE GROUPS.

It is positive that the forum has a space (online) where:

- information is shared;
- the topics to be discussed are published;
- supporting documentation is submitted;
- the conclusions that emerge are presented.

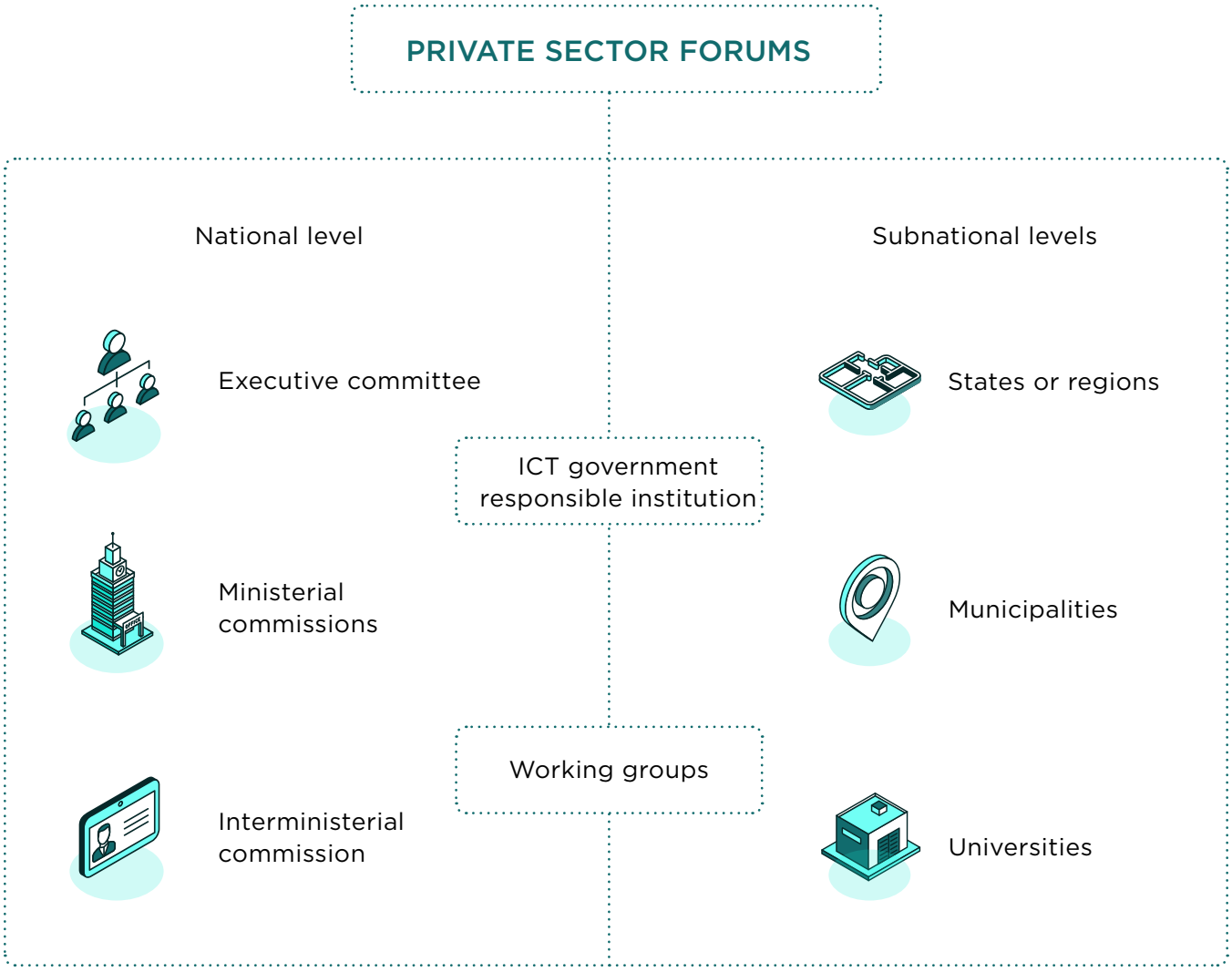
This serves not only in terms of transparency, but also to stick to the commitments made.

It is also useful to have a fixed and planned calendar, with plenary meetings, where agreements can be reached that are binding and allow progress to be made with certainty in the country's digital transformation. The weight of the agreements can vary, ranging from a document that is published (for transparency and public pressure) to a rule that turns the agreements into regulations. In any case, it is worthwhile that the work is not only carried out around these plenary meetings, but can be maintained through the specific groups, or with a permanent committee, in the periods between meetings.

It is also convenient to have a collaborative work space, from the technological point of view (see, for example, https://administracionelectronica.gob.es/comunidades/forofacturae), to facilitate the work of the forum.

Finally, given the general characteristics of the forum, it is important that, although face-to-face meetings are held, they can also be followed and allow participation by videoconference. This eliminates the physical location gap, so that associations or companies located in places far from where the meeting is held can also feel that they are participating in the country's digital transformation.

On the other hand, a key requirement for the success of the forums is the existence and adequate empowerment of the lead institution, since it is this institution that must lead the forums and act as a hinge with the regulation that may be needed or with the institutions related to the projects to be discussed. In this sense, the main product of the forums, in order for them to have a real impact and not simply consist of words, must consist of agreements on regulations, new common services, or changes involving them, so that they must affect practically all the technological proposals appearing in the document.



IN CONCLUSION

We must not forget at any time that the digital transformation of the public administration is done by and for the citizens. Therefore, it would make no sense if they did not have the necessary skills to access the new digital services that the administration makes available to them. Thus, all the actions listed here, such as developing a strategy, training citizens, or setting up forums, are just examples of some of the many initiatives that can be implemented. Above all, in any format, it is very important to always maintain an open channel of communication with citizens to inform them firsthand of progress, as well as recommendations for use, manuals, information, etc., and to use this same channel to listen to their opinions and needs.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo is in charge of the neighborhood association in his neighborhood. Thanks to the transformation forum, he has been able to share the problems that people with disabilities in his neighborhood have in carrying out administrative procedures, which has raised awareness among public entities to include accessibility concepts in digital public services.

Mayor's advisor
Daniel

Seeing the new tools at his disposal, Daniel wants to take advantage of them to change and improve the functioning of the municipality. The problem he faces is that he has no one who knows how to adapt the municipal regulations to this new scenario.

Vice minister of health
Sara

Sara is investigating how to adopt international principles such as the one that prevents asking citizens for documents that are already in the possession of the public administration. When she looks for ICT professionals to implement this regulation, she cannot find them in the country. Sara is saddened because she is going to have to contract these services internationally, which will not only make the work more expensive, but will also mean that the associated knowledge will not stay in her country.

Sara managed to convince the ministry's management to update the texts on the website and documents. Now, instead of being written in legal language, which she honestly sometimes did not even understand, the texts are expressed in simple language and present the information in a clear and understandable way.

EXAMPLES

Click on each flag or icon to go deeper.

Colombia
Plain Language Program.

Korea
Global Academy y Korea ICT Learning Program (KoIL).

United Kingdom
Assisted Digital Support Program

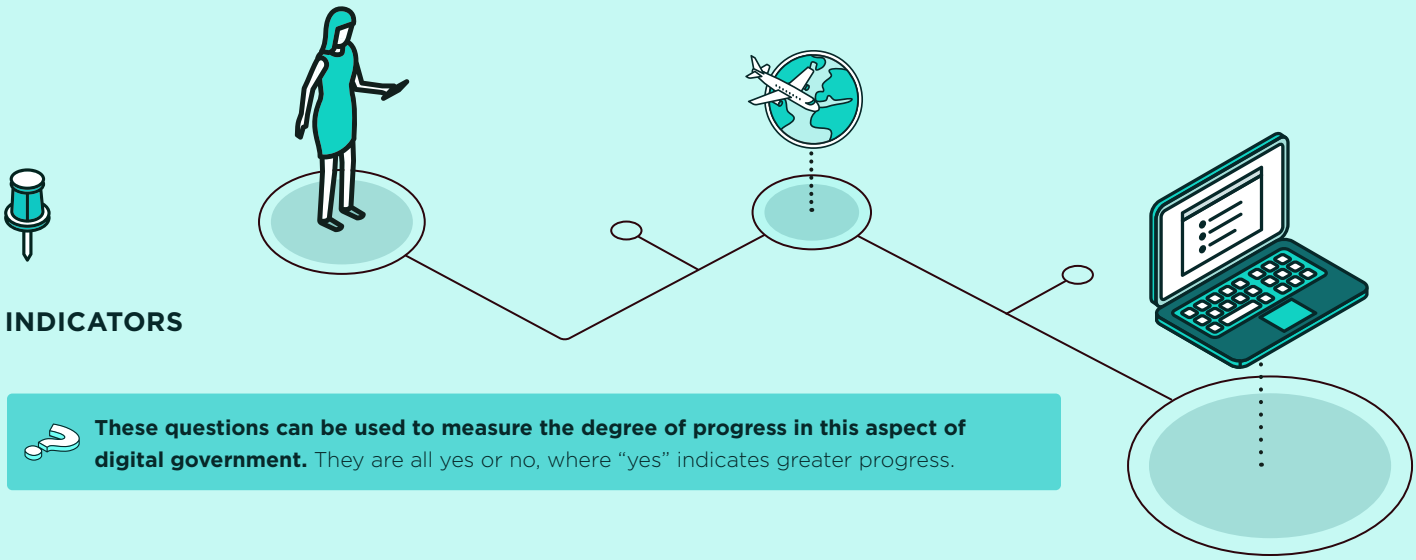
Estonia
Estonian Lifelong Strategy 2020.

Australia
"Be Connected" Program

Spain
Spain Digital Plan 2025.

Spain
There are vertical (sector-specific) forums between the public and private sectors for certain technology projects, such as electronic invoicing. There are also general forums, such as the electronic file, document, and archive forum, not restricted to a sector or project.

Uruguay
Ceibal Plan



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

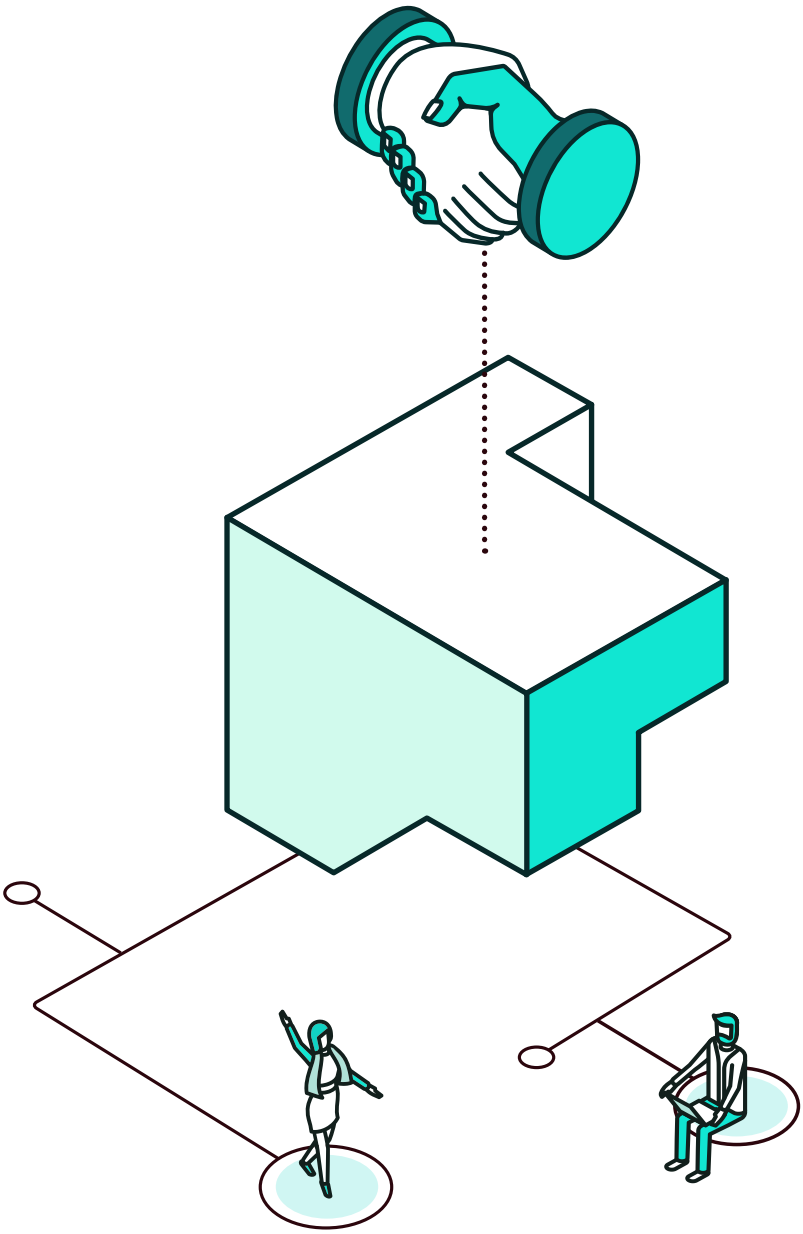
- Is there an ICT training strategy for citizens?
- Are the following groups covered by the training strategy?
  - women
  - senior citizens
  - ethnic minorities
  - inhabitants of remote areas
- Are there cooperation agreements with universities or educational organizations to facilitate the training strategy?
- Is a target number of people to be trained included?
- Are there citizen service centers that explain how to interact digitally with the public administration?
- Is there a plan to bridge gaps, address inequalities, or expand opportunities for disadvantaged people, whether it is part of a specific plan for this purpose or other material (e.g., digital strategy)? If so:
  - Do you foresee potential gaps in the following aspects?
    - urban/rural

- genre
- age
- disability
- socioeconomic status
- educational level

- Does it offer a diagnosis of the existing gaps?
- Does it provide different types of concrete solutions that can be implemented?
- Is there a budget allocated for the implementation of the plan?

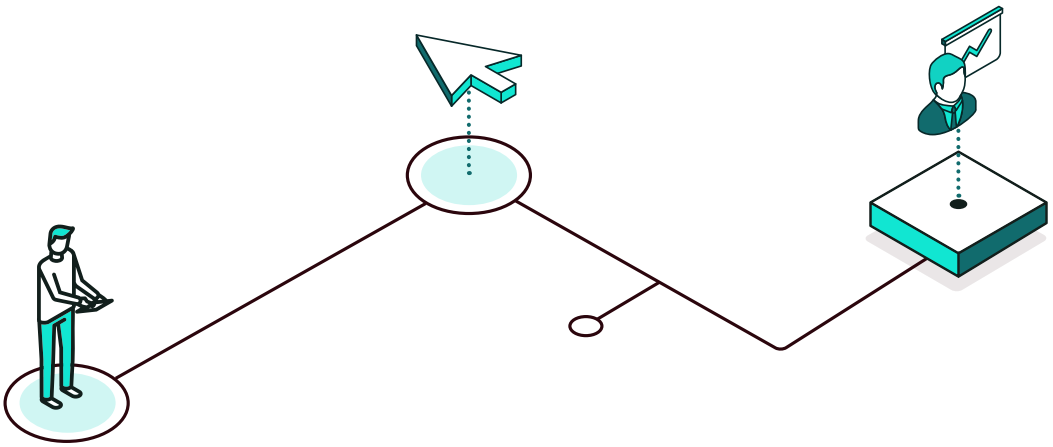
› Is there a forum in which stakeholders outside the public administration can share their needs, preferences, and experiences about digital transformation with government representatives? If so:

- Do you have an established schedule?
- Does it enable virtual participation?
- Do you publish the topics to be discussed in advance as well as the topics discussed and the decisions taken?
- Does it issue binding provisions?
- Includes the participation of the following:
  - Companies?
  - Citizens?
  - Organized civil society?
  - Business associations?



3.5

Public-private collaboration



Public-private collaboration is based on the following fundamental premises:

- **Digital talent:** Mainly aimed at creating added value in public administrations.
- **Cogovernance:** Understood as the codecision framework regarding the sharing of responsibilities and risks inherent to the evaluation, design, and implementation of those projects that are carried out jointly.
- **Change management:** Understood as the key element to successfully materialize the creation of the talent that the private sector contributes to public administrations in the execution of joint projects.

It is true that in some countries it may be a somewhat disruptive formula, by making certain parts of the acquisition of the talent sought through bidding processes more flexible. Talent, as an added value, must be understood as the contribution of highly qualified resources, increasingly demanded by the public administrations of all states, without which a true digital transformation process would be unthinkable. These profiles, today, mostly reside in the private sector; hence the need to seek the appropriate mechanisms to create a binomial based on public-private collaboration.

In this sense, it may be thought that the attraction of talent provided by private entities to public administrations entails a disproportionate economic increase for the states. However, this conviction has turned into a problem that is difficult to solve, since this type of resource requires, in most cases, a qualification based on high-level certifications and continuous training processes that, in no case, can be passed on from the private company to the public administration. In fact, the trend over the last five years, in private organizations of varying sizes, is that a large number of these resources prefer to work in private entities, outside their countries of origin, in response to the market economies of the states that have a higher purchasing power. Now, how can this problem be solved? It is certainly a concern for the private sector that provides services to the public sector to retain talent, a problem that is not usually considered by most countries.

When it comes to proposing a guaranteeing regulation that provides maximum security in legal terms, the driving vehicle validated by the states is the development of bidding processes, which are based on a regulation focused directly on the needs posed by the administration, together with the responsiveness that the private sector can provide, collaborating to obtain the maximum overall benefit in what would be called a *win-win* situation. The public administration must be the driving force behind the country's digital transformation, but to do so they must foster collaboration with the private sector and social organizations in order to find and offer new innovative solutions to the demands of public services.

THE BEST OF TWO WORLDS

As society advances, so do the services demanded by citizens, and in general terms the new challenges to which the administration must respond are increasing. However, it cannot and should not address all the challenges alone, among other reasons because it has finite resources and therefore its capacity is limited. In order to consolidate and advance in the digital transformation process of the administration, it is necessary to count on all stakeholders, both from the public and private sectors, so that they are aligned and feel that they are actors in the transformation process.

Faced with this fact, the different countries have typically opted for two solutions:

- Increasing public assets: A measure that results in models that are not easily manageable and can lead to failure.

- Privatizing public assets: An option that, according to some empirical studies, does not necessarily lead to an improvement in the service provided. This research deepens the idea that efficiency is not a determining factor, much less an atomically measurable one, which is affected by many other factors such as the market and competition, which are in turn macroeconomic composites. In general terms, privatization makes no sense depending on the service in question (judicial system, police, etc.), and its success is subject to multiple circumstances such as

regularization or deregulation, the specific service or entity to be privatized, and the political and social context of the country, among others.

Between these two classic models, there is another one that has begun to be applied: public-private collaboration, where the two worlds, private efficiency and public control, come together. Thus, this type of alliances must obey a clear normative regulation that facilitates the participation of the private sector in the design and implementation of digital transformation measures, while allowing the public administration to increase its efficiency and take advantage of the knowledge, experience, and innovation capacity of the private sector.

THE IMPERATIVE NEED FOR A STRONG, LEADING, EFFICIENT PUBLIC ADMINISTRATION IN THE PROCESS OF DIGITAL TRANSFORMATION PUSHES TOWARD THE USE OF COLLABORATIVE PROCESSES, BUT FOR THIS IT IS NECESSARY TO DETECT THE KEYS THAT GUARANTEE THE OPERATION OF SUCH A MODEL.

THE PROBLEM OF THE CLASSICAL MODEL

In the classic models, this process is followed to carry out these projects:

1. The administration tenders bidding documents.
2. Companies present their best offers. In order to be selected, they are likely to propose a reduced quotation.
3. After the award, the company puts its resources to work on the contracted projects.
4. The selected company starts the project with resources commensurate with the price offered and not the bid/desired price.

Beyond the possible contractual repercussions, the classic model is not capable of associating the two worlds: the need to have the best people because the management deserves it and can *versus* the reality called competition, where in order to win, it is mandatory to lower the price and therefore sacrifice the quality desired by the customer.

This model also lacks the characteristic of transferability, since if the project is successful, the service will not be operated/transferred to other organizations with the will of the private entity. In order to combine this classic model with guaranteeing measures that do not cast doubt on the viability of investments by the states in projects of this nature and the quality of the resources provided by the top talent, it is necessary to have regulatory standards that pursue noncompliance on the part of private companies and act as a watchdog of the investments. This is the success of a well-managed public-private partnership.

THE DIFFERENTIATING FACTORS OF A COLLABORATIVE MODEL

Greater collaborative value contribution

A strengthened public administration vis-à-vis the private sector

Definition of a regulatory framework based on the assumption of responsibilities by private companies and on the guiding role of public administrations

Better approach to the stages that make up digital transformation projects

Joint investment

Social demand

GREATER COLLABORATIVE VALUE CONTRIBUTION

The ultimate goal of the digital transformation of public administrations is to offer a better service to citizens. With this idea of service provision, which is the same as what is done in the private sector, it is important for the public sector to offer the necessary regulatory framework and tools so that society itself can collaborate in the digital transformation. Historically, collaboration with private entities has been developed through the publication of tenders and the receipt of bids; however, for many services, a closer working collaboration would be advisable where public procurement is not understood as an expense, but as an investment. Therefore, the regulation of all states must be clearly aligned with the idea of value for money. The economic crisis as a consequence of the 2020 pandemic is leading us toward a new economic management based on public procurement and public-private partnerships as a plan to generate value.

A STRENGTHENED PUBLIC ADMINISTRATION VIS-À-VIS THE PRIVATE SECTOR

The increasing dependence of the public administration on third-party private entities for the provision of certain public services has led to the search for agreements and alliances to define, develop, plan, implement, and evaluate collaborative strategies. The question that arises is to establish the role to be played by the public administration in this scenario. In this sense, within the framework of digital transformation, the state must include in its strategy the changes in the country's regulations and laws to define and regulate how it is going to

- exercise control in public-private interaction;
- ensure the participation of private entities in public services;
- search for the appropriate communication channels to ensure compliance with public and social values such as equality, responsibility, etc. without this being detrimental to competitive concurrence or implying the creation of monopolies.

DEFINITION OF A REGULATORY FRAMEWORK BASED ON THE ASSUMPTION OF RESPONSIBILITIES BY PRIVATE COMPANIES AND ON THE GUIDING ROLE OF PUBLIC ADMINISTRATIONS

- The absence of such a regulatory framework poses a serious risk for digital transformation projects, especially in the IT field, and may trigger undesired consequences for the parties involved in the process of implementing this type of action:
  - public administrations in charge of managing the resources made available by the state (material, economic, human)
  - project suppliers, usually represented by private companies.

BETTER APPROACH TO THE STAGES THAT MAKE UP DIGITAL TRANSFORMATION PROJECTS

- Unlike other areas, digital transformation usually encompasses in a single project three major stages that properly correspond to so many other subprojects, each with its own complete life cycle:
  - definition, specification, and design of what is to be built
  - construction and testing of the design
  - implementation and commissioning of what has been built
- Although there is a tradition of treating all the stages in a single project, it is advisable to treat each of them as a separate project in order to avoid the problems arising precisely from the fact of carrying them out together. These problems are centered on the difficulty or even impossibility of planning and defining the construction project when what is to be built has not been specified (designed). Therefore, it is essential to regulate, in a public-private collaboration regulation, what is referred to:
  - delivery of documentation.
  - it project management, within the scope of digital transformation, through public tenders and framework agreements.

This is undoubtedly a novel aspect, currently under study by a number of countries.

- the following is an example of the basic requirements that should be included in a standard of this nature so that they are reflected and complied with in the tenders and framework agreements drawn up by public administrations within the framework of public-private partnerships:

Control sheet for documentation of digital transformation actions (justification for exclusion):

Table of contents (required)

Memory (required)

- Introduction (required)
- Purpose of the project (required)
- Background (justification)
- Description of the current situation (recommended if it exists)
  - Description of the current environment (required)
  - Summary of identified deficiencies (required)
- Standards and references (required)
  - Legal provisions and standards applied (mandatory)
  - Bibliography (required)
  - Methods, tools, models, metrics and prototypes (required)
  - Methods and tools (required)
  - Models, metrics, and prototypes (mandatory)
  - Quality control mechanisms applied during the drafting of the project (mandatory)
  - Other references (optional)
- Definitions and abbreviations (recommended)
- Initial requirements (mandatory)
- Scope (mandatory)
- Hypotheses and restrictions (mandatory)
- Alternatives and feasibility study (mandatory)
- Description of the proposed solution (required)

- Risk analysis (mandatory)
- Project organization and management (mandatory)
  - Organization (required)
  - Project management (mandatory)
- Time planning (mandatory)
- Budget summary (required)
- Prioritization of basic documents (mandatory)
- Annexes (required)
  - Annex – Entry documentation (required)
  - Annex – System analysis and design (required)
  - Annex – Size and stress estimation (required)
  - Annex – Project Management Plans (mandatory)
    - Integration management (justify your exclusion)
    - Scope management (justify exclusion)
    - Deadline management (mandatory)
    - Quality management (mandatory)
    - Human resources management (mandatory)
    - Communications management (mandatory)
    - Risk management (mandatory)
    - Procurement management (justify exclusion)
    - *Stakeholder* management (justify exclusion)
  - Annex – Security plan (justify exclusion)
  - Other attachments (if deemed necessary) (optional)
  - Communications management (mandatory)
- System specifications (required)
- Budget (required)
- Studies with their own entity (optional)

JOINT INVESTMENT

- When there is joint investment, there is coresponsibility, the total financing of the administrations is avoided, and the private enterprise is given the opportunity to provide the appropriate means, reaching future collaboration agreements. At this point it should be noted that the dimension of the administration's responsibility for state competitiveness must be combined with the dimension of the concern for expenditure—and therefore optimization—that the private entity wishes to carry out (cogovernance based on codecision). With regulatory tools such as the one defined in the previous point, control and monitoring by public administrations acquire many more guarantees. Depending on the state of maturity of each country, the application of such a regulation should be studied.

SOCIAL DEMAND

- The idea of the collaborative model provides a better response to the constant growth of services demanded by citizens. In a public administration that is in the process of digital transformation, public-private collaboration must generate the necessary coordination and cooperation mechanisms with civil society in order to advance in this project, listening to and meeting the new demands and needs of twenty-first-century society.

    - *Example:* In Europe, due to the economic and social crisis caused by COVID-19, two economic plans have been launched through a new collaborative model of public and private services. In this way, it is hoped to achieve an adequate rebalancing of wealth and of rights and duties, and to advance in an open and participatory society in this type of model:

        - *Next Generation EU*, a new recovery instrument endowed with 750 billion euros
        - A reinforced long-term European budget for the period 2021–2027 (1.1 trillion euros)

ACHIEVEMENTS THAT CAN BE ATTAINED THROUGH PUBLIC-PRIVATE PARTNERSHIP

- Generation of new talent, knowledge, and value, both for the administration and for private entities. Given that a digitally transformed administration has new knowledge needs, such as specialists in cybersecurity, programming, etc., the state must bet on digital talent. Currently, this is found to a greater extent in the private sector, and it is therefore essential to ensure that the public administration has regulatory mechanisms for hiring that allow it to have this knowledge. At the same time, a commitment should be made to train public employees in the management of digital administration in order to reduce the talent gap between the public and private sectors.

- Faster and more efficient responses to society's demands.

    - *Example:* Given the recent health emergency situation and the need for the use of hotels for the sick, it would have been a disaster to wait for the bidding period for the rental of these spaces.

- Rationalization of public spending for cases in which investment is carried out jointly, since it implicitly results in better managed investments.

ONE OF THE FIELDS WHERE COLLABORATIVE MODELS HAVE BEEN SUCCESSFULLY APPLIED HAS BEEN IT, WHERE THERE IS A HUGE NUMBER OF PROJECTS TO BE DEVELOPED JOINTLY BETWEEN THE ADMINISTRATION AND PRIVATE[29] ENTITIES

BEFORE APPROACHING THIS MODEL...

When deciding to adopt the public-private collaboration model, it is first necessary to analyze the weaknesses found in the public administration, such as the lack of specific regulations or collaborative culture, since conventional models are still in place. To this end, it is necessary for the lead institutions of digital transformation to carry out training activities in this area and make the parties aware that joining forces is the way forward.

In a digital, agile, and transparent public administration, it is essential that public-private cooperation or partnership formulas have a legal framework that incorporates equally agile and transparent mechanisms. In most countries, however, these can only contract according to what is regulated in the public procurement regulations of their country; it is therefore essential to develop a regulatory framework that allows, without falling into legal uncertainty, the use of new digital capabilities and talents.

Often the public administration, because it is too bureaucratic or excessively bureaucratic, does not adapt to the needs of society in an agile way. However, this must change in a digital public administration, which must be flexible and adapt to new realities. Therefore, the lead institution must implement the necessary regulatory changes to provide its country with an agile model of public-private collaboration that is conducive to a fluid, fast, and simple relationship with the private sector.

29. It should be kept in mind that some of these projects—for example, those derived from disruptive technologies such as artificial intelligence—will have uncertain results.

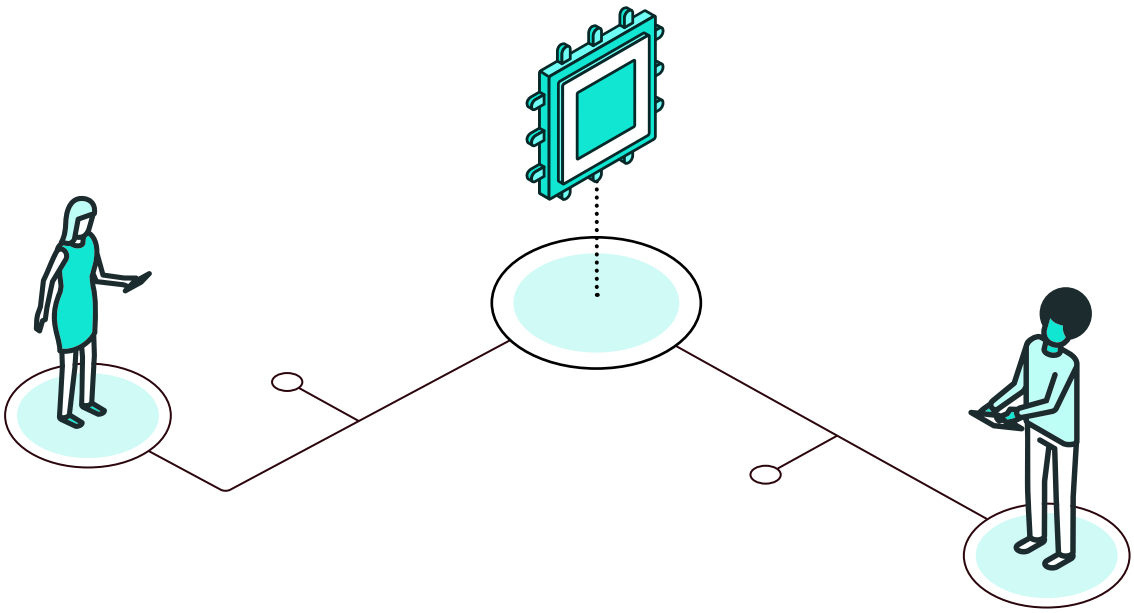
PPP APPROACHES MAY BE DEVELOPED TO ATTRACT PRIVATE FINANCING FOR THE EXECUTION OF PUBLIC CONTRACTS, OR AS A MEANS OF INNOVATION AND IMPROVEMENT OF PUBLIC SERVICES, OR A MIXTURE OF THESE PURPOSES.

BEYOND THE MERE ACQUISITION OF TECHNOLOGICAL TOOLS

In short, the digital transformation process is configured as a new form of organization and relationship of the public administration with citizens and private companies, and even with other administrations. In this context, it is essential to do the following:

- Create a new environment of competition and public-private collaboration, developing an appropriate legal and regulatory framework to promote this cooperation in all areas in order to adapt to the needs of a digital society.

- Create mechanisms for dialogue and participation between the different public administrations, the private sector, and society, in order to achieve a better articulation of public-private collaboration. This could be channeled through a set of instruments such as funds, pilot programs, tractor projects, and innovative purchasing, among others.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara is determined to shorten the deadlines of the public health service transformation plan by focusing on the citizens' healthcare priorities through various high-impact projects, including the outsourcing of nonhealth services (cleaning, security, food, laundry, or administration) and the modernization of the hospital network's electromedical equipment, whose useful life cycle has been radically reduced, leaving two-thirds of the equipment technologically obsolete.

The ministry's procurement officers, aware of the delays in deadlines and the difficulties that conventional procurement processes have been experiencing, have proposed to address its needs in an innovative way through the Public-Private Partnership (PPP), advising a proof of concept that will also serve to generate lessons learned. Initially, an agreement has been successfully formalized with a consortium of private-sector partners for the provision, modernization, and maintenance of the electromedical equipment in a reduced period of six months, an experience that will serve to launch other processes in which agility in contracting and attracting financial resources is sought.

Due to the COVID-19 pandemic, Sara needs to procure 10,000 ventilators by the end of the month, and the expectation is that the administration will have an additional 150,000 ventilators. One of the models that her country regulates is urgent procurement via sole source; however, a private entity has developed a model of ventilators that can be mass-produced and whose manufacturing costs are 40 percent lower than those of any other supplier. The company has 15,000 ventilators in stock to meet the initial demand, but to manufacture more ventilators, the manufacturing plant needs to be expanded. Sara does the calculations and concludes that if she buys only 75,000 respirators at the price agreed with the company, the state's investment in the new factory will have been profitable.

EXAMPLES

Click on each flag or icon to go deeper.

Peru

Ministry of Transportation and Communications (MTC), Red Dorsal Nacional de Fibra Óptica (RDNFO) (National Fiber Optic Backbone Network).

Spain

Madrid City Council. The Foro de Empresas por Madrid is a collaborative platform for project planning and development that allows the business community to contribute and contribute their knowledge, experiences, and technologies to advance the common good of all citizens.

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a public body that monitors compliance with public-private partnership and contracting regulations?
- Is there a national regulatory framework for PPPs? If so:
  - Does it contemplate common concessions to provide public services and perform public works where revenues come from user fees?
  - Does it contemplate administrative concessions in which the consideration for the services combines payments from the administration and user fees?

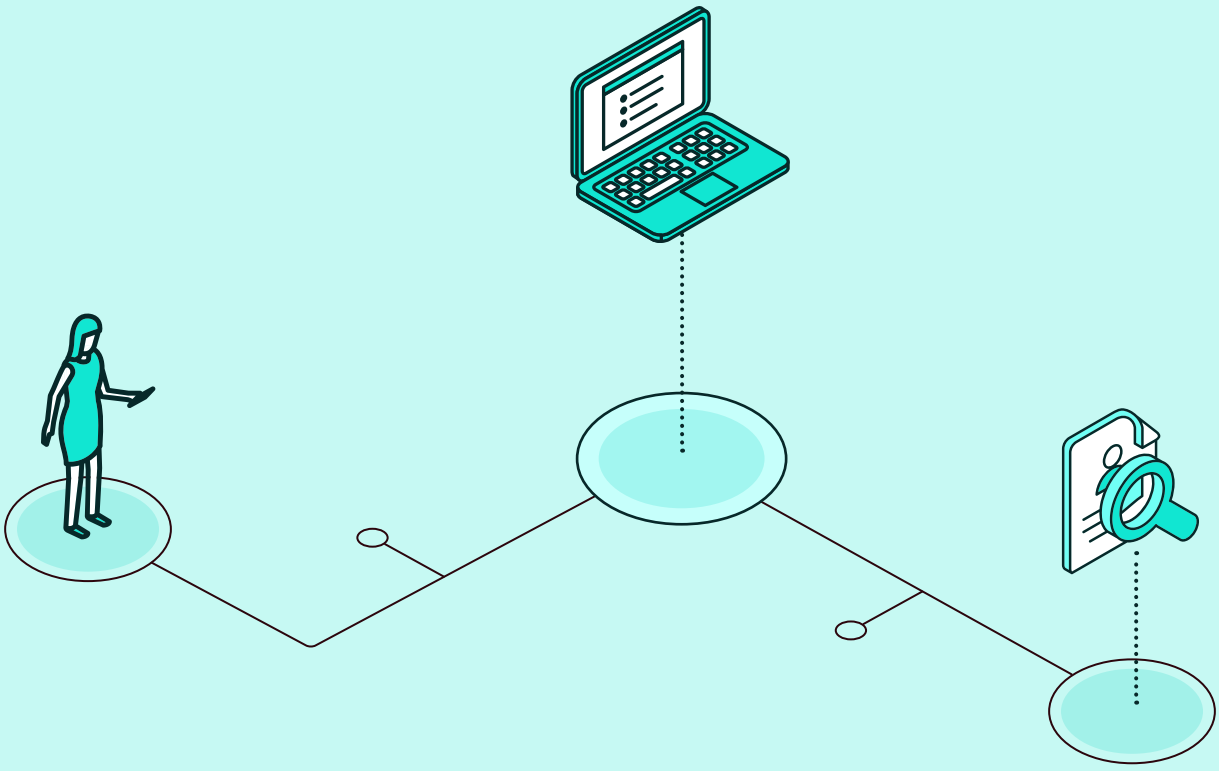
- Does it require prebid feasibility and PPP investment value estimation studies at the preproject level of detail?
- Does it contemplate and offer clear risk allocation principles and/or rules?

› Do you have an institutional framework at the national, state, or municipal level for PPP management?

- Is there an entity in charge of approving the results of technical feasibility studies and monitoring PPP contracts?
- Does it include the monitoring and control of the economic and financial equilibrium of PPP contracts?

› Are there any studies of good practices or lessons learned and/or interest groups on PPPs at the national or regional level?

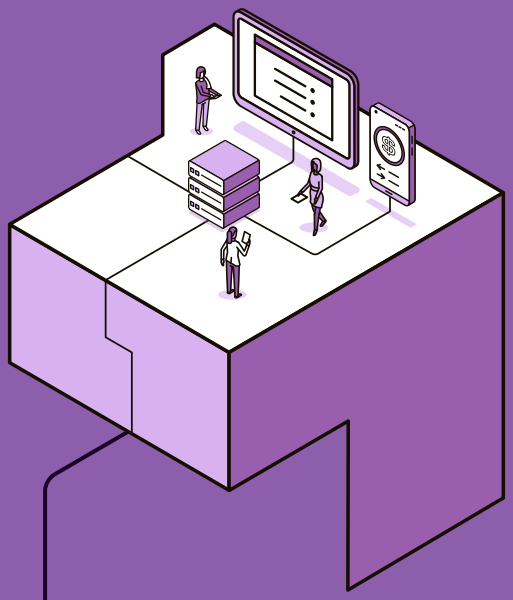
› Are there professional service experts and/or financial and insurance sector entities specialized in PPP contracts?

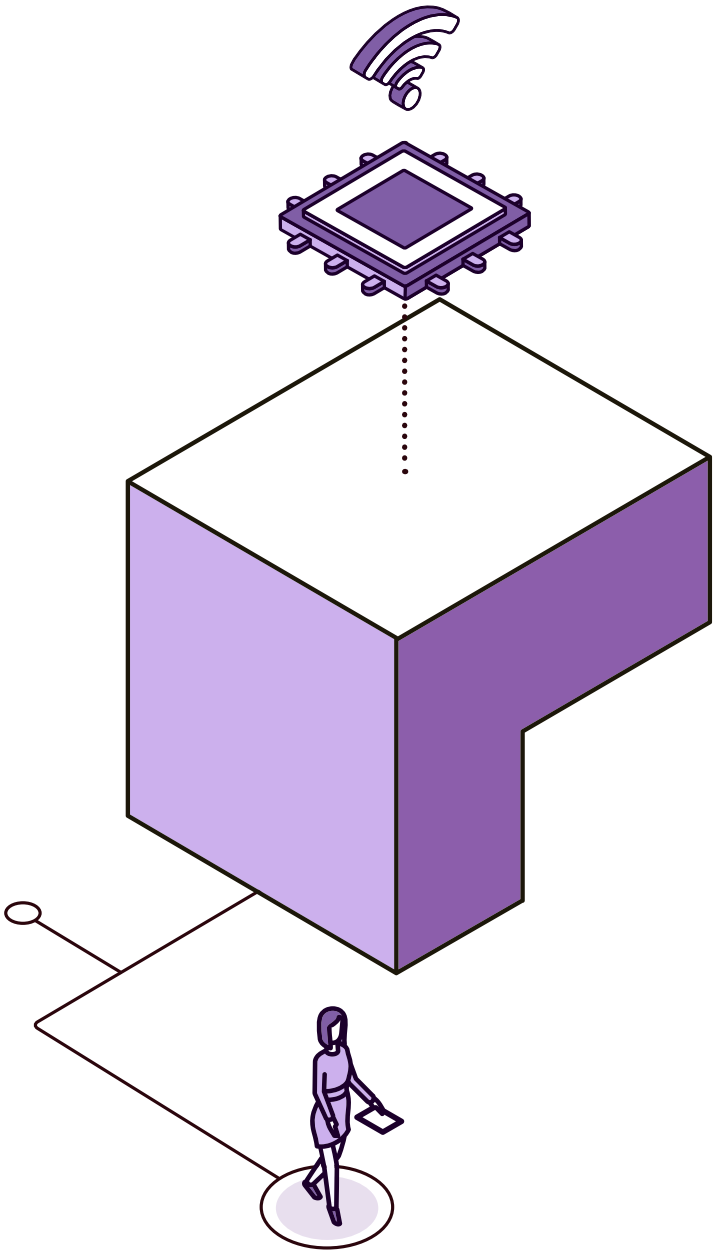


CHAPTER

04

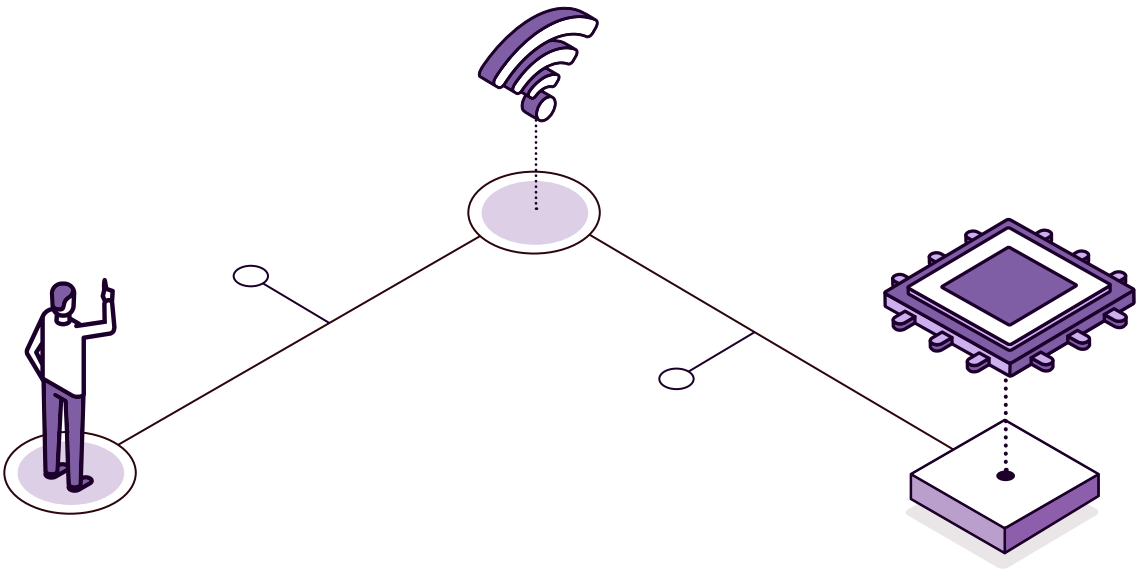
Infrastructure and technological tools





4.0

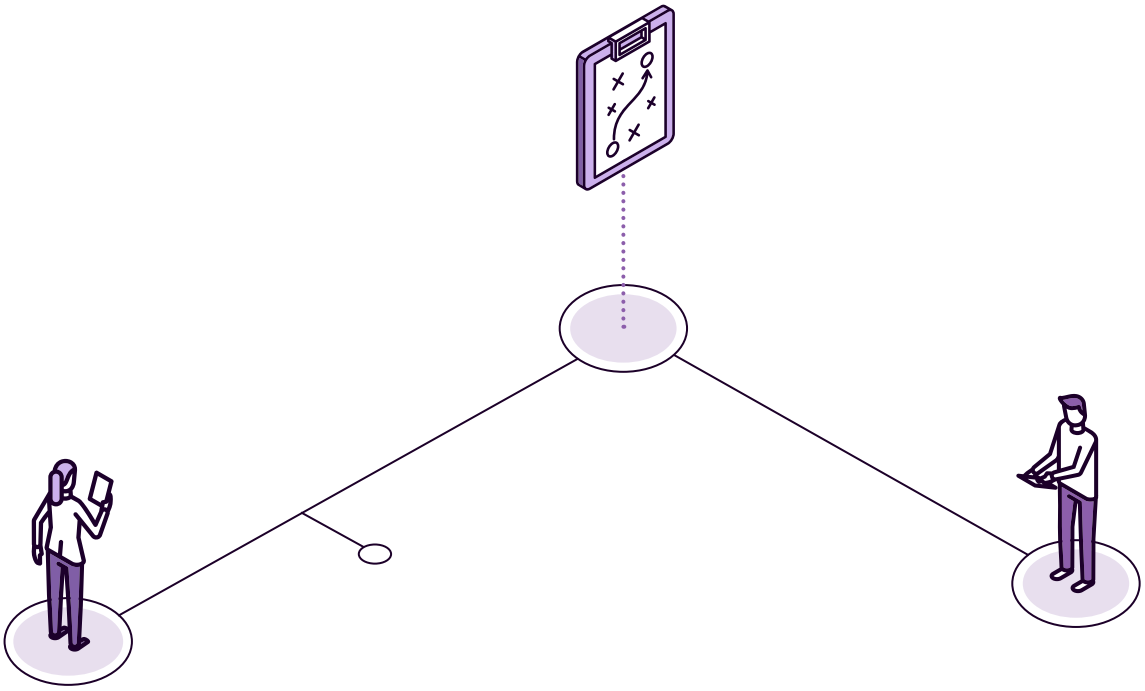
Introduction



Technology is undoubtedly one of the key elements of the current social paradigm; its presence has a direct influence on the life of societies and their members. In this sense, the leading role of technologies in information societies is the fundamental driver of structural change in society. Its influence can be seen both at the economic level, where it has revolutionized most of the productive processes, and at the social level, influencing practically all aspects of human life, especially those related to communication.

The technological implementation of document processes in public administration has led to a significant improvement in the response capacity: before, a procedure took days, it was subject to opening hours, and it was known when it started but not the status unless you went in person to ask, etc. In fact, there is no digital transformation without technology adoption.

Although there are many voices that claim that technology is only a means and not the end, this can be seen as partly true. The strategic objectives of digital transformation processes must always include the adoption of technology itself. This will contribute to the end thanks to its contribution to the transformation of the processes of the administration in its relations with citizens. A clear example of this can be seen in the most current digital transformation plans of certain countries, which usually include the deployment of 5G or the incorporation of artificial intelligence as a technology and not as an administrative process.



ICT INFRASTRUCTURE PLANNING AND MANAGEMENT

One of the great challenges that arise when incorporating technological solutions within an organization is which is the most convenient way to do it. There are a multitude of solutions on the market, and choosing the best one for the organization is not a simple task. Decisions such as where to store data or what elements should be provided to workers and headquarters so that work and processes are carried out efficiently require prior analysis if they are not to be turned against the organization in the future.

This planning, and subsequent management, is a difficult and complex job that requires the following:

- A very solid foundation in the application of fundamental concepts in areas such as computer science, management, and people skills.

- Special skills in understanding, for example, how networked systems are composed and structured, and what their strengths and weaknesses are. In information systems there are important *software* concerns such as reliability, availability, capacity, security, ease of use, effectiveness, and efficiency for intended purposes, all vital to any type of organization.

NEW OPPORTUNITIES IN LIGHT OF TECHNOLOGY

Technology makes it possible to simplify and automate administrative processes, achieving the efficiency and agility that today's society seeks in its public sector. This automation should be understood as a comprehensive redesign of services, taking advantage of the capabilities that new technologies allow, in order to implement new and better models of relationship with citizens, with greater efficiency.

Thus, the digital transformation of government is the strategic opportunity to do the following:

- Incorporate mature technologies as well as emerging technologies.
- Integrate a new logic for public services based on an updated operating model, aimed at making services more effective and able to capitalize on new opportunities for profitable growth.
- Provide all information on the operations, processes, and results of public administrations:
  - To citizens, for the sake of transparency.
  - To the private sector, with a view to promoting the reuse of public-sector information for the benefit of economic development.
- Develop data analysis and cross-cutting information capabilities through disruptive technologies (microservices, cloud services, AI, and supercomputing, among others), thus optimizing management and improving decision-making, independently of the administrative structure.

BENEFITS OF DIGITIZING PUBLIC SERVICES AND OMNICHANNEL PLATFORMS

- They make it possible to propose a more transparent government.
- They favor citizen participation in the definition and even in the design of public services, so that these are better adapted to the real needs of citizens in a new governance model.

IT IS ESSENTIAL TO DESIGN AN ACCESS, SECURITY, USABILITY, AND MOBILITY STRATEGY FOR END USERS, ACCORDING TO CURRENT NEEDS AND ADAPTED TO THE DIFFERENT GOVERNMENT PROFILES.

THE NEW JOB

The government's lead institution must lead the change from the traditional workplace to a mobility model that guarantees its security and makes use of technological tools at the horizontal level, which are made available to all ministerial departments in the vertical sectors, for the economically responsible provision of services. The current needs are not only for the development of certain functions but increasingly the use of collaborative tools that cover the different use cases that make up the digital work model in the government.

This commitment must be based on open system architectures that support a modular (technological components) and progressive design, under the requirements of interoperability, scalability, and portability, with high performance, quality, reliability, and consistency. This type of architectural stacks, based on interoperability components, allow vertical sectors to adopt the new digital approach in a gradual manner, adjusted to their needs and resources, and following a homogeneous technological reference framework.

This approach ensures :

- A robust digital transformation process.
- Interoperability with the rest of the actors that make up government institutions, public services, and other agencies involved, whatever their technological references in the vertical sector they represent.

FROM THE GLOBAL TO THE PARTICULAR

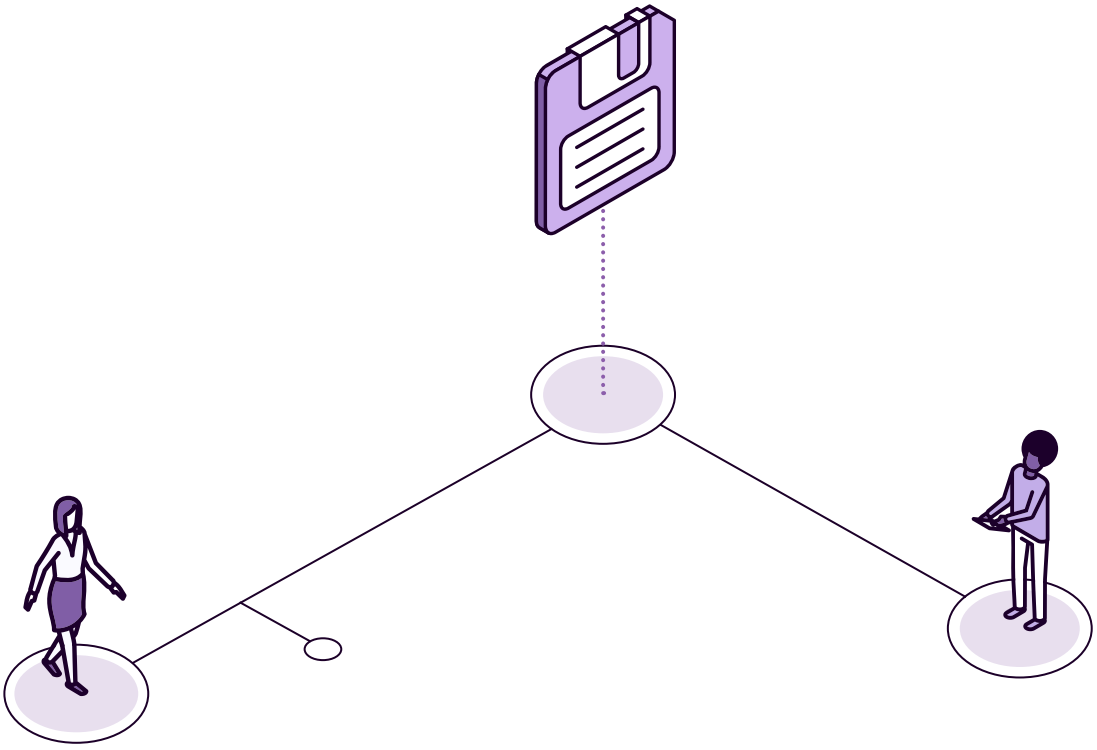
In the context of a digital transformation of the government, it is necessary to implement a global strategy that allows a rational use of available resources. At the same time, this must take into account the particularities of the different vertical sectors, in order to clearly differentiate the boundaries between the infrastructures and technological tools in common use, central or horizontal in nature, and those that, due to their particularity, must be designed and adapted by each vertical sector. This process will be guided by a series of action principles, both in its conception phase and in subsequent development, aimed at maximizing efficiency, the reuse of tools already available, and collaboration between different responsible departments and administrations, in order to achieve specific short-term objectives, concentrating efforts on a set of priority projects.

It is at this point that the lead institution must take the lead, implementing an appropriate management model adapted to the scope of the proposed strategy. A new, more rational, efficient and secure model for the provision of infrastructures and technological tools, based on transparency and data analytics from the design stage, must be implemented. The idea, therefore, is to have a series of common and shared tools of a mandatory nature to cover the common needs of all vertical sectors. In the same way, there would be

common infrastructures in the ICT field, as well as hosting in data centers.

KEY COMPONENTS FOR DEVELOPING AN OVERALL STRATEGY FOR TECHNOLOGY INFRASTRUCTURE AND TOOLS

- The infrastructures from the following points of view: Central or horizontal, Headquartered and Intelligent workstation.
- Interoperability, at all levels, as an essential technical element, and the need for technical guidelines and standards to standardize technological implementations.
- Digital identity management as a requirement, since it is the pillar on which much of the digital transformation is based.
- The digital signature as another of the main tools around which the common services revolve.
- Horizontal tools, such as electronic notifications, electronic registration, and consultation and verification of data held by public administrations.
- The development of administrative directories.

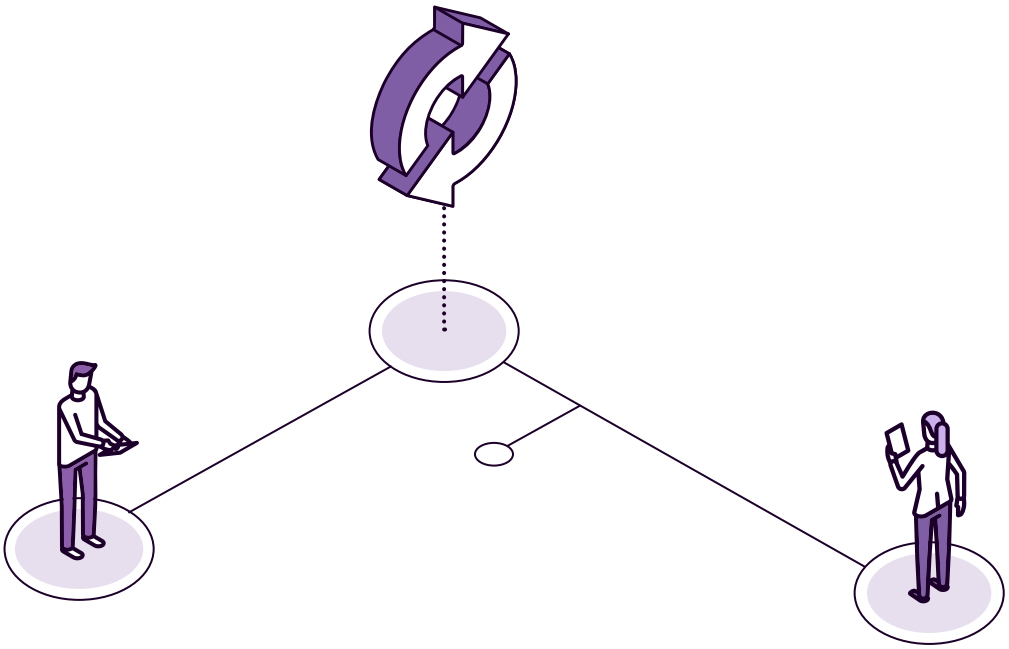


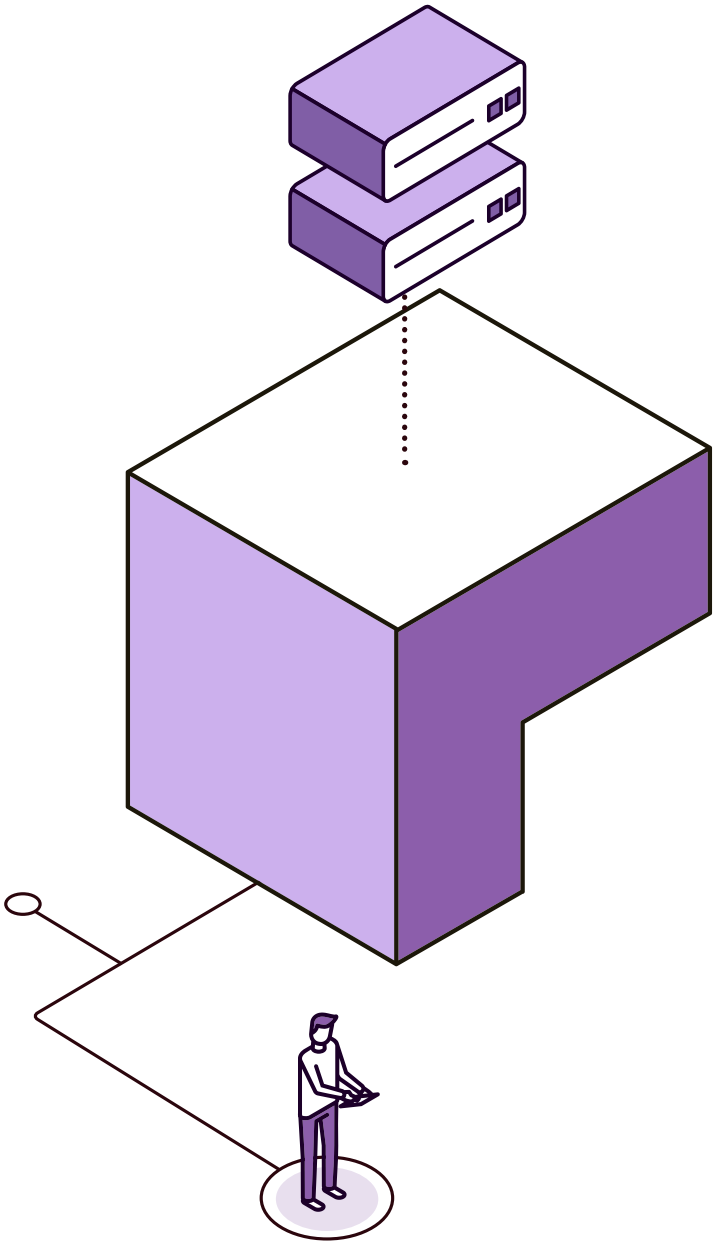
- The creation of a national digital archive.

- The unprecedented qualitative and quantitative leap that disruptive technologies represent: technological advances in hardware equipment, new application development paradigms, the emergence of artificial intelligence as a differentiating element, the new provision of technological services (*on-premise,* as well as the different *cloud* modalities), the Internet of Things, *big data*, to name a few, offer a variety of scenarios that adapt to practically all needs and starting situations to address this type of transformation project.

- Cybersecurity as a horizontal discipline covers all infrastructures and technological tools, so that it not only affects computer equipment, but also involves training for civil servants and raising public awareness. In this regard, it should be borne in mind that, as technology has evolved, so have the threats related to cybersecurity. While technology offers a wider range of services to citizens, making organizations more transparent and simpler, special and greater attention must be paid to systems in order to preserve data and prevent unauthorized access to them.

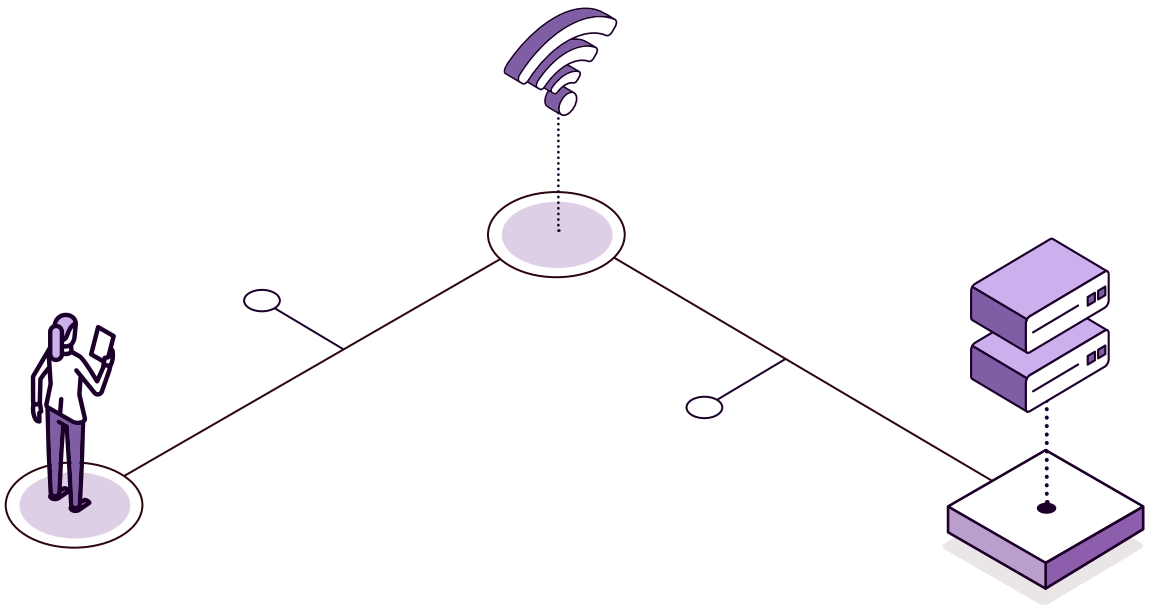
The digital transformation of government brings a world of opportunities and challenges for public administrations. This will involve updating the business operating model both horizontally and vertically, incorporating emerging technologies and turning them into a competitive advantage. To achieve this in a coordinated, efficient, secure, reliable, and transparent way, it is necessary to design this global strategy of infrastructure and technological tools.





4.1

Infrastructure



The implementation of ICTs in public administrations means that the volume of data handled within organizations and institutions will become unmanageable if the necessary tools are not available to manage it and make it accessible to employees and third parties quickly and securely. In addition, the fact that citizens today demand a more agile, closer, and more transparent administration, capable of meeting their demands in a much more efficient way, requires several indispensable elements:

1. Processing, automation, and storage capacity, either in the cloud or in the company's own data centers

2. Adequate technological services in offices and customer-service units

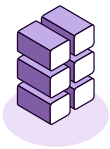
3. Digital workstations that allow public servants to incorporate into the systems—and therefore into the digital ecosystem—the relevant actions in each case.

LARGE VOLUMES OF DATA REQUIRE A PHYSICAL COMPUTING INFRASTRUCTURE THAT IS CAPABLE OF MANAGING THEM EFFICIENTLY, AS WELL AS GUARANTEEING THEIR SECURITY AND NOT LOSING THEM IN THE EVENT OF A DISASTER.

It is of utmost importance to do the following:

- Provide the necessary means to be able to structure the information and make it flow efficiently to its addressee.
- Ensure data integrity. Thanks to the technological evolution that has taken place in recent decades, it is now possible to achieve this goal through the use of devices and technologies that allow anyone to access information, regardless of their computer skills.

The following articles will review some of the concepts and tools that must be taken into account when making decisions aimed at helping organizations achieve their objectives and continue to improve day by day. In this way, a tour will be made of different basic elements in any organization that needs agility and efficiency when managing its processes:



Central or horizontal infrastructure, referring to the facilities that the lead institution makes available to the rest of the organizations.

Headquarters infrastructure, understood as a delocalized office and customer service.

User station infrastructure

Cloud

Finally, an alternative that has grown in recent years is addressed: cloud providers, looking at their advantages and, equally, their disadvantages in order to make the right decisions that will drive any organization to be a benchmark in terms of ICT efficiency and effectiveness.

4.1.1 CENTRAL INFRASTRUCTURE

The digital transformation of an organization would not be possible without the so-called data processing centers (DPC) or *datacenters*, essential infrastructures that allow achieving the objectives and requirements at the level of information storage and access. A definition of data center would be the location where the IT equipment necessary for processing the information of an organization, whether private or public, is located, without forgetting the services that allow the appropriate management, support, and maintenance.

> ***IN SHORT, A DATA CENTER IS A FACILITY THAT CENTRALIZES ICT EQUIPMENT, OPERATIONS, AND TECHNICAL EQUIPMENT FOR THE PURPOSE OF STORING, PROCESSING, AND DISSEMINATING AN ORGANIZATION'S DATA, INFORMATION, APPLICATIONS, AND SERVICES.***

In the face of a country's digital transformation, it is crucial that the lead institution in charge has a perfectly sized data center that centralizes computing and storage requirements at the government level, both for infrastructure and for common technological tools. In this way, all services that can be provided in a centralized manner would be housed in the lead institution's data center, with all the necessary security, operation, and maintenance measures.

It is even possible to contemplate the hosting of agency infrastructures with a reduced size, thus simplifying the data center network and optimizing the investment for its maintenance and operation. This scenario does not prevent each agency or ministerial department from having its own data center or a hybrid solution, where part of its services are on its premises, while others are consumed from the government data center managed by the lead institution.

The design of the lead institution's data center must have all the necessary control, monitoring, and operational measures to guarantee the service it provides, because an incident can have a direct impact on the other agencies. For this reason, such a design must have a backup data center that provides exactly the same services, with the same level of performance and security. In fact, the idea of having not only two data centers, but also a backup center in case of a contingency, should not be ruled out. Moreover, thanks to these replicated infrastructures, it would be possible to configure certain services in active-active mode, so as to be able to cope with higher levels of service availability.

For all these reasons, data centers or datacenters have become the brain of any organization that is committed to new technological advances, innovation, and flexibility to provide immediate answers to its needs.

DATA CENTERS UNDER A NEW APPROACH

Until now, data centers were rooms with extreme security measures and very strict Building Management Systems (BMS). Without losing this idea, the emergence of cloud services has meant a significant evolution in the design and distribution of an organization's computing and storage infrastructure, choosing between in-house resources and external providers.

Undoubtedly, any technology provider has multiple resources available to offer hosting and cloud services that could cover any need of the public sector. However, it should not be forgotten that there is particularly sensitive information (confidential information, personal information) that it is advisable to keep in the state's own facilities, under the supervision of the technical team of public employees. In this way, policies, procedures, and technical instructions that are mandatory in the public sector can be applied.

GUIDELINES FOR SETTING UP A DATA CENTER

When talking about a data center, it can be understood from two dimensions:

- **Continent:** The building, room, and facilities available to ensure the supply, availability, security, and adequate environment to house technological equipment.
- **Content:** Technological equipment of various characteristics, features, and performance that make up the complete technological infrastructure of the organization.

The design of a data center, from the point of view of the continent, has reference standards, which even allow its certification:

- ANSI/TIA-942
- TIER
- ISO/IEC 24764
- ANSI/BICSI-002

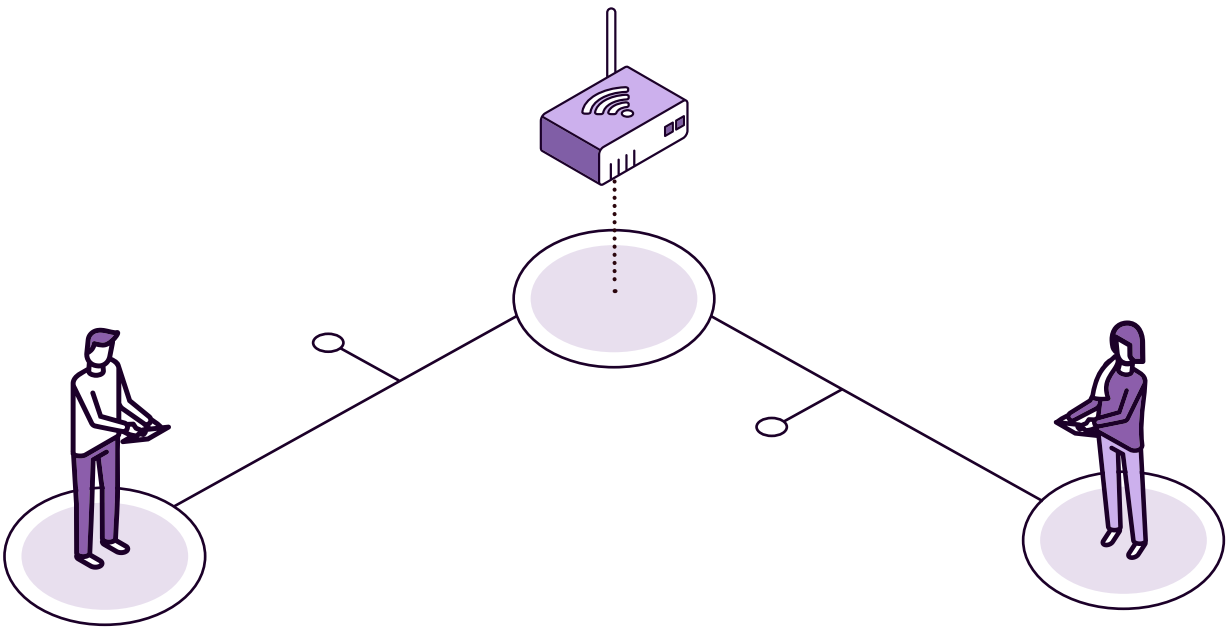
The first two are worth mentioning because of their wide dissemination:

- **TIA 942** *(American National Standards Institute – Telecommunications Industry Association)*: This standard, published in 2005, provides both recommendations and guidelines for the creation and subsequent maintenance of the data center. The purpose of this standard is

to provide a series of guidelines and directives for design and construction, and focuses on communications, such as distribution and cabling. In this sense, it defines specific parameters and values such as weights and floor loads, width and height of doors, separation distance between electrical and communications cabling, or even the distance between the site of the center and other sensitive installations.

- **TIER Classification:** This started in the 1960s and was created by the Uptime Institute, the body in charge of managing the different levels of the standard up to the present day. The four levels of this classification evaluate the performance of a data center according to the availability of the facilities or telecommunications required for the operation of a particular organization. Thus, each of the four levels defines criteria for maintenance, energy, cooling, and failure capabilities.

As explained above, the design of the data center has to be adapted to the requirements of the organization and the planned growth strategy. In this case, the lead institution has to take into account the current and future provisioning needs. It is therefore necessary to have a strategy with a provisioning plan that foresees a location with possibilities for expansion and growth in terms of equipment, cooling, power supply, footprint, etc. The preparation of this plan is an exercise of coordination between the lead institution and the sectorial departments in which, starting from the current situation ("*as is*"), an adequate medium-term projection can be made (*"to be"*), considering all the needs that the execution of the sectorial strategies may require.



MAIN ELEMENTS OF A DATA CENTER

- **The facility itself or the usable space available for IT equipment.** Providing twenty-four-hour access to information makes data centers some of the most energy-intensive facilities in the world. This must be considered in the design to optimize space and environmental control, seeking to keep equipment within specific temperature/humidity ranges. Island or cube data center designs are now available that manage cooling in a more energy sustainable manner.

- **Facilities or equipment that helps to securely maintain the highest possible availability.** Some components for the support infrastructure include the following:

  - Medium to low voltage transformers
  - Ups (uninterruptible power supply systems)
  - Generating sets
  - Air conditioners for computer rooms (CRAC)
  - Heating, ventilation and air conditioning (HVAC) systems
  - Exhaust systems
  - Detection systems.
  - Physical security systems: biometric and video surveillance
  - Environmental management systems and fire detection and extinguishing systems

- **The equipment itself,** such as chassis, equipment, and *software* for IT operations and data and application storage. These may include the following:

  - Network electronics equipment
  - Perimeter security devices
  - Cabins and storage networks
  - Physical or virtual servers

- Specific equipment for database optimization
- Elements of backups and tapes for their realization
- Armored and fireproof cabinets for storing backup copies, if so determined by the operating procedure.

- **Technical operation team,** which monitors all control indicators of the facility and performs preventive, proactive, and reactive management and maintenance to ensure the correct operation of infrastructure and IT equipment twenty-four hours a day. These operators rely on BMS (*building management systems*) monitoring systems, which collect all the events of the facility as a continent or container. The monitoring of the data center becomes a part of the management and monitoring of the overall security of the building (intelligent or not). Additionally, it can take over the monitoring of the infrastructure or content.

- A room manual with all operating procedures correctly detailed to react to any eventuality.

Defining the minimum requirements of a data center, according to the above elements, will depend to a large extent on the business scope. In short, the organization's requirements condition the design of a data center, based on its prioritization and security and availability needs. In the case of digital government, the scenario is the provision of public services twenty-four hours a day, 365 days a year, so having a data center with high levels of availability is a priority.

As mentioned above, the data center becomes one of the neuralgic points of the digital transformation, so it is necessary, at the organizational level, to have a structure that assumes responsibility for its management and the technical team in charge of its operation. In this regard, the lead institution must incorporate trained personnel dedicated exclusively to it, so that adequate coordination procedures can be established for the support and attention of the sectoral departments.

Going into a little more detail regarding the elements that would form part of the "content" or equipment of the technological infrastructure, it is worth highlighting issues such as virtualization, disruptive servers, and storage solutions.

VIRTUALIZATION

One of the technologies that have revolutionized the configuration of data center infrastructure, especially from a management point of view, is virtualization. In fact, this alternative offers opportunities for improving the agility, flexibility, and overall performance of the data center, as well as for efficient management of its footprint (physical space). This technology generally uses virtualization software together with computing equipment based on physical on-premise blade servers, which have large processing and memory capacities.

Among the countless benefits of virtualization, the following are worth mentioning:

- **Speed and flexibility:** The allocation of physical resources according to the demand of the applications will be much simpler using virtualization (i.e., it is possible to allocate more or fewer resources without having to modify the physical structure of the data center to the applications or processes that need them quickly and efficiently).

- **Isolation:** Virtualization will allow systems to be isolated, ensuring that the failure of one system will not affect the others.

- **Portability:** Having virtualized applications and data will allow their portability to new machines or even to other data centers, regardless of whether they are in the cloud or in-house installations.

- **Reduction in operating costs:** It is always faster and less expensive for the technical team to set up new virtual servers than physical servers.

- **Reduced infrastructure and real estate requirements:** Organizations running virtualization reduce the need for physical space required when launching new services.

- **Data center disaster recovery:** This technology allows environments to be recovered quickly and immediately from available images and backup systems.

While a few years ago we only talked about virtualizing physical servers, today it is possible to classify virtualization into five areas:

- Desks or workstations

- Servers or processing

- Storage

- Applications

- Communications networks

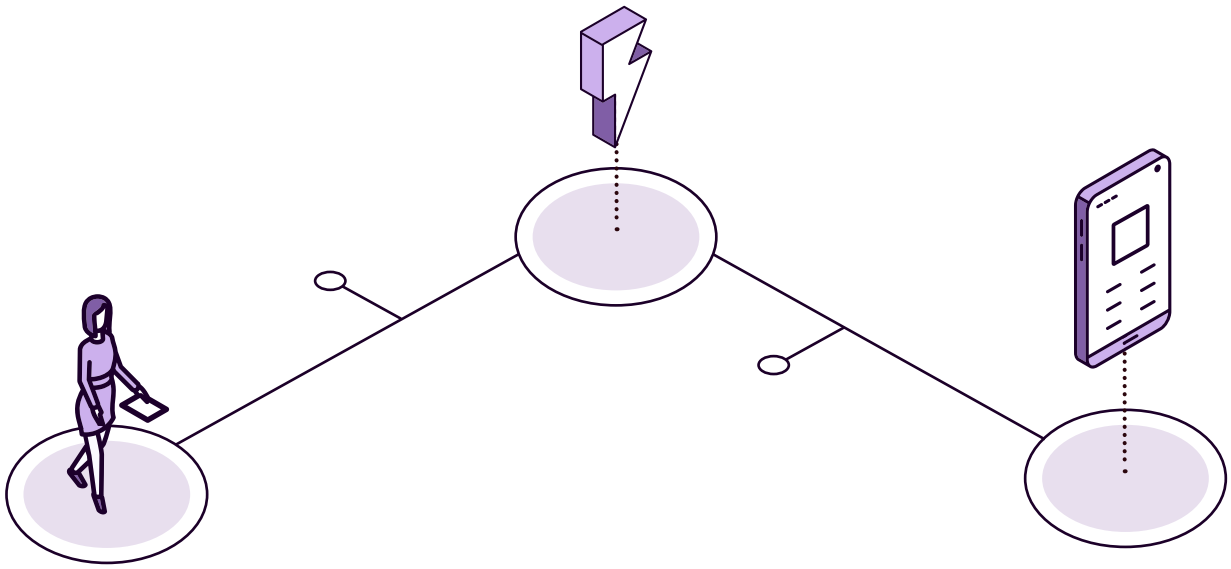
HYPERCONVERGENCE

Without undermining the above, it is worth mentioning that the technological revolution that revolves around storage and processing solutions involves several alternatives to virtualization to be considered; among them are hyperconvergence or quantum computing solutions.

Hyperconvergence simplifies traditional IT management by bundling data center services such as network electronics, physical and virtual servers, and storage. It is a software-supported infrastructure that makes the management of the system's hardware infrastructure independent, so that the entire architectural stack underneath can be managed as if it were a single component thanks to the higher-level management software (hypervisor). This makes it possible to isolate the connectivity, storage, and processing spaces, eliminating dependencies between them and improving management efficiency.

The main benefits of hypercorvency include improved availability and scalability of the solution, although the future will be written by quantum servers, which at the moment have promising projections in proof-of-concept tests in the laboratories of large manufacturers.

THE MAIN BENEFITS OF HYPERCORVENCY INCLUDE IMPROVED AVAILABILITY AND SCALABILITY OF THE SOLUTION, ALTHOUGH THE FUTURE WILL BE WRITTEN BY QUANTUM SERVERS, WHICH AT THE MOMENT HAVE PROMISING PROJECTIONS IN PROOF-OF-CONCEPT TESTS IN THE LABORATORIES OF LARGE MANUFACTURERS.



STORAGE SOLUTIONS

As in other fields, technology is making advances in storage solutions, especially in terms of reducing the storage footprint and implementing functionalities related to document management, protection against cyberattacks, and free backup. These solutions optimize the type of disk used to facilitate access to information according to the frequency of use and provide the most appropriate model according to the required storage format: file/file, block, and object.

There are already resources designed to host and optimize database performance, which solve problems with legacy applications or very heavy queries. These facilities not only optimize the execution of queries but also incorporate online backups with very efficient recovery times, improving them if necessary.

Finally, everything related to the software needed to be able to offer applications to end users and citizens requires architectural stacks made up of operating systems, database management solutions, middleware software, and an endless list of alternatives that offer functionalities such as content managers, document managers, web portals, office tools, collaboration and coordination solutions, and management and decision-making tools, among others.

APPLICATION DEVELOPMENT HAS EVOLVED FROM CLIENT-SERVER SOLUTIONS, IN THREE-TIER MODELS, TO CONTAINERIZED APPLICATIONS BASED ON MICROSERVICES, WITH AN AGILE PROGRAMMING PARADIGM AND CONTINUOUS INTEGRATION BETWEEN DIFFERENT ENVIRONMENTS.

THE CLOUD AS A SERVICE ALTERNATIVE: SOME CONSIDERATIONS

Having briefly outlined the main elements that would make up a proprietary data center, it is important to mention a service that has grown a lot in recent times in organizations: cloud infrastructures. More and more organizations are deciding to move all these components and facilities to third-party infrastructures. In this way, the data center infrastructure has moved from local equipment to a virtualized infrastructure that supports the management of all computing, processing, and storage capabilities in multicloud environments that are contracted to a service provider.

The main advantage of the cloud is the decrease in costs, since the use of third-party data centers makes it possible to delegate these costs, including the obsolescence of the machines (i.e., the servers are rented to a third party, who would be responsible for ensuring that they work properly and always offer the latest-generation machines). A priori, it may seem that there are only advantages to using this type of installation, but it is also true that this option has other disadvantages, such as the fact that the data would be "physically held" by an external provider.

This approach can be taken into account when questioning the location of the infrastructure by any organization, but in the context of the public sector, the need to protect information must always be taken into account. Current procurement laws allow this type of service with all the necessary legal confidentiality clauses, although it is recommended to have an "on-premise" copy (on the premises of the public body) for security reasons. In the case of contracting this type of services, it is necessary to have a data return plan for when the contractual relationship is terminated.

The possibility of having a private cloud in public administrations means the optimization of resources and the homogenization of solutions, so that both technical specialization and the provision of management and support services are centralized, improving security and efficiency. The lead institution can consider having this type of cloud services to offer them to sectorial departments, with all the legal guarantees required by the data being hosted.

All of the above must be supported by the aforementioned organizational structure, as well as the corresponding operating procedures and technical instructions that enable the management and coordination of the data centers, whether they have their own, have cloud services, or opt for a hybrid solution. It is not just a matter of having a data center room manual; it is necessary to have capacity, maintenance, contingency, and disaster recovery plans.

FOR THE LEAD INSTITUTION AND THE SECTORAL DEPARTMENTS, THINKING ABOUT CENTRAL INFRASTRUCTURES BECOMES NOT ONLY A STRATEGIC EXERCISE, BUT AN EXERCISE IN GOVERNANCE AS A WHOLE.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara is driving the digital transformation within her ministry. Currently there are many departments that still work on paper, and she needs to digitize all that information so that it is accessible from any office. On the other hand, she is concerned about the possibility that a failure in one of the computer systems in one of the offices could paralyze their activity, and information from a file could be lost, since there are no backup copies. Sara's first objective will be to take the necessary actions to ensure that the information of its premises and offices is stored centrally and that it can work efficiently, regardless of the office in which its public employees are located.

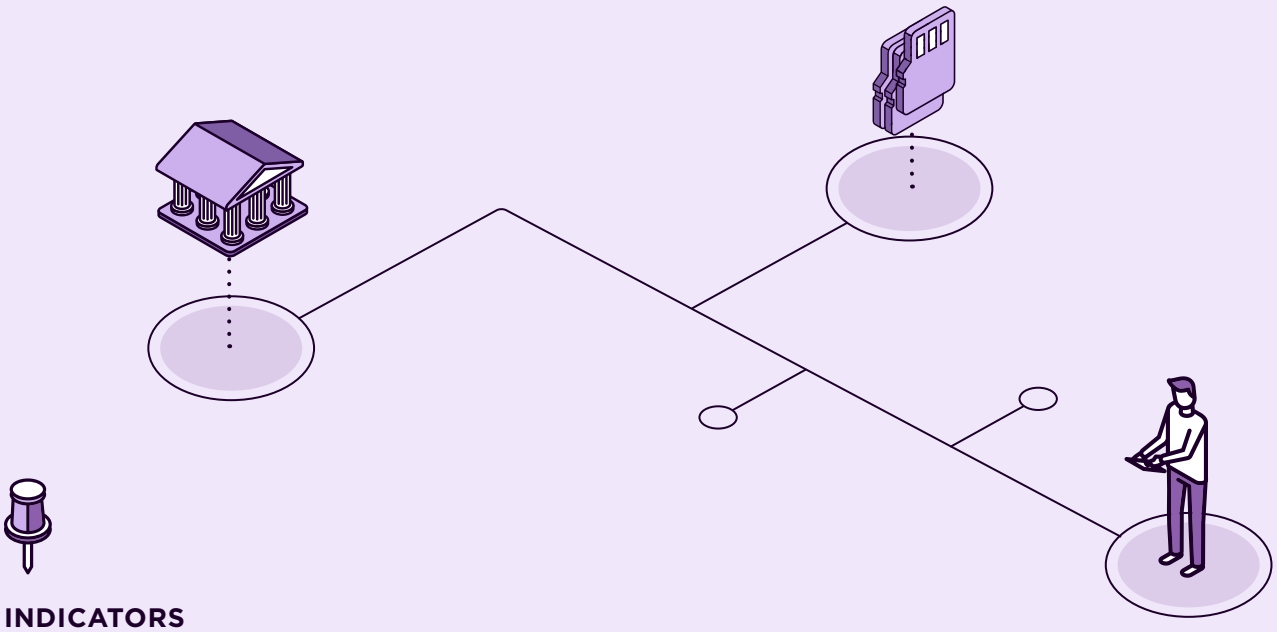
EXAMPLES

Click on each flag or icon to go deeper.

Paraguay
Data Center: study and design

Colombia
Ministry of Education. Data Center uses

Dominican Republic
Data Center



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

Is there a centralized *data center* for the entire state?

- Does it have sufficient infrastructure to provide the necessary data efficiently and quickly to employees?
- If tomorrow there was a computer failure or fire in a data center, how long would it take to recover the data and get employees back to work?
- If you wanted to migrate applications and data to another *data center,* how long would it take? Could you migrate all applications at once?
- Do you have any cloud services available?
- Does the central *data center* have a backup center to ensure high availability?
- Are there sector *data centers*, and are they coordinated and connected to the central data center?

4.1.2 HEADQUARTERS INFRASTRUCTURE

The way in which public services have been provided over the years has been drastically modified by the digital transformation of public administrations. Before, any procedure had to be done in person at a counter, providing endless documents and waiting in a long queue, while today many procedures can be carried out online.

ICTs have brought about a significant change in all sectors, and it is the public sector that has had the most direct impact on citizens. Internet, social networks, 5G technology, *smartphones*, and audiovisual systems are the basis of the relationship and communication model from the technological point of view in society, and of this society with the public administration. Thus, from the moment a citizen has to carry out a procedure, he or she is surrounded by a whole series of technological services that the state has made available to adapt to his or her needs and resources. Thus, it is possible to carry out procedures by telephone, in person, or totally online through the web portals of public administrations. All these channels can even be opened simultaneously, so it is possible to start a procedure using one communication channel and check its status or finalize it using a different one.

This new context means that the headquarters, offices, and offices of public administrations are also immersed in a process of digital transformation, as they have to incorporate infrastructures that help to provide quality public services efficiently and safely but above all are adapted to the digital society that is becoming more and more prevalent. Therefore, nowadays, when a citizen enters a public building, he is surrounded by media and audiovisual systems that allow him to communicate information in a massive and unattended way, which contributes to a better communication and, above all, to the automation and simplification of the public information process.

Thus, before physically going to a public administration's customer service office, it is certain that the citizen has telephoned or consulted the agency's web portal, either to carry out the procedure online or to consult where the nearest office is located, if it has not been possible to carry it out digitally. This is where the citizen has a first channel of information and bidirectional communication with the public administration. It is even likely that they have interacted with a virtual assistant, based on AI, which has directed them in the relationship of the procedure in question.

If you finally have to go to the physical office of the agency, it is essential to have the appropriate means to help and guide citizens to the correct location where they can be properly served to carry out their management. Having intelligent screens with clear and concise information indicating which procedures are carried out at each window, as well as ticket dispensers and shift managers, will facilitate the organizational work and increase the productivity of this office. This increases the satisfaction of the citizen, who has been able to carry out the appropriate procedure in a simple and agile manner.

For this purpose, technological solutions used in citizen services are being considered:

- Information booth (kiosks or totems)
- Shift dispensers
- Information screens integrated with content management systems
- Digitization and cataloging systems
- Solutions for collecting handwritten signatures
- Recording and videoconferencing solutions

Generally, technological solutions provide information on administrative procedures, warn of the next shift according to the organization's appointment system, and facilitate the dissemination of organizational, informative, awareness-raising, or simply useful information for the citizen. In any case, it is a matter of finding the right technology to implement the organization's information and communication strategy, adapting to the different citizen profiles, according to their needs and capabilities, and using all the communication channels that today's world has to offer.

All this equipment distributed in the public offices must have an organizational team in charge of its management, maintenance, and support, as well as those responsible for the edition, approval, and publication of the contents—in other words, two technical teams: one responsible for the IT equipment and the other responsible for the management and implementation of the communication plan.

STAND-ALONE PROCESSING THROUGH KIOSKS

Among the technological elements that allow a citizen to carry out different queries or procedures autonomously and independently at the headquarters, there are kiosks, totems, or automated information booths, where users can use touch screens to carry out most of their transactions or obtain the information they need quickly and efficiently. The use of this particular resource has become widespread in recent years, and it is even becoming increasingly common to find biometric identification totems, which are able to identify a person reliably by different methods, such as fingerprint or iris reading together with an ID card or similar. Thus, it is possible to offer completely personalized and highly sensitive services, since the totem in question could ensure that the individual is who he or she claims to be.

Such services already include access to information, notifications, or even specific files. In addition, through standardized forms, citizens can submit written submissions on their own procedures. These systems save time for the citizen, as well as provide more satisfaction, since they do not have to wait to carry out their procedures and, on the other hand, they save time for the organization's employee, who can devote himself to other tasks that cannot be automated.

In addition, this type of device is particularly useful when implementing systems for evaluating the quality of services and the degree of user satisfaction with them. In this way, in an unattended, voluntary, and nonintrusive way, it is possible to have an assessment of the provision of services and the acceptance of the implementation of new initiatives.

Both in the case of information screens and multimedia kiosks, it is possible to have solutions and infrastructures managed centrally by the lead institution. In this way, by providing the devices, sites, and content management consoles, any sectoral institution can take charge of the configuration and management of its devices and information. Therefore, each unit would only have to install the equipment in the *sites* and manage the applications of each vertical sector, as well as proceed with the information and communication of its administrative procedures.

Recently, it has become increasingly common to see in certain offices staff helping citizens to encourage them to use this type of semiautomatic technology. In this way, people receive help, personal attention is decongested, and, at the same time, citizens are trained in these disciplines, creating over time a certain base of digital culture.

IT CORNERS

In certain sectors, all the technological equipment of an informative and self-management nature described here is complemented by information points, understood as much smaller spaces aimed at solving technological problems, rather than exclusively providing information. These are known as *IT corners*, and they provide quality support fully adapted to the digital transformation.

For the public sector, this type of support represents a considerable improvement in the face of a digital transformation process, since concern for the digital divide, change management, and digital training is also part of public services. It is not possible to implement a process of this technological depth without support and awareness focused on the citizen.

CURRENT PUBLIC ADMINISTRATION MODERNIZATION POLICIES ALWAYS PLACE THE CITIZEN AT THE CENTER OF PUBLIC SERVICES.

RECORDING AND VIDEOCONFERENCING SOLUTIONS

Depending on the services provided by the headquarters, for more specific sectors and from a point of view more oriented to administrative procedures in the medium and long term, another example of technological infrastructure advancement arises: the audiovisual means of management and production. These are required, for example, in a courtroom where trial hearings are held, or in the press rooms of ministries and public agencies, which broadcast and distribute the signal to the media. In these cases the need is completely different from that of the front office, and probably in this type of environment it is necessary that the systems allow not only the recording of the hearing, but also its subsequent reproduction by the administration of justice.

In such situations, systems such as digital cameras, microphones, institutional signal production and distribution equipment, and even live broadcasting of hearings when they are public are used. All of them are solutions that allow to provide a public service adapted to the citizen or to a particular group, incorporating the technology that best suits each case.

It is possible to offer this type of technology using centralized solutions by the lead institution, because the functionalities are similar, and the management and operation are practically identical. This provides a business case for a more responsible investment based on economy of scale.

Up to this point, a brief description has been made of the headquarters infrastructure that has a more direct interaction and visualization with citizens. Now, if we were to focus on a more professional internal scope, we should mention two technologies that allow collaboration and communication between professionals: the counter workstation equipment, to digitize the paper that reaches the public administration, and virtual meetings or videoconferences.

DIGITIZATION OF DOCUMENTS

In those public offices where there is face-to-face attention to citizens, and which therefore receive documents from them, scanning and digitization systems must be provided. The aim is to eliminate the use of paper and to ensure that all documentation is digitized for its incorporation into digital files.

The digitization and cataloging process solves the problem of paper being digitized at an early point in the process, which has advantages such as the following:

- An electronic document is created, thus ensuring its integrity and traceability.
- Evidence of the presentation is created in the input/output register.
- It avoids the obligation for the citizen to have electronic means to communicate with the administration, converting citizens' documents into electronic documents.

Opting for this alternative means including, of course, optical character recognition, which will make the document data available in a structured form, so that working with them will be faster and more efficient than if these documents were simply images. All this information can be incorporated with the acceptance and signature of the citizen, who will use digital ink tools to introduce his handwritten signature into the system, as well as other auxiliary devices such as code readers.

VIRTUAL COMMUNICATION AND INTERACTION AS A COORDINATION MECHANISM

With regard to virtual communication and interaction tools, it is necessary to give as an example the change brought about by the incorporation of videoconferencing in the public sector. Until relatively recently, only the meeting rooms of private companies had end points (televisions together with an audio-video signal decoder) and microphones to carry out this type of meeting; today, market solutions have jumped to the end user's workstation, and even beyond, by offering this same functionality in all types of mobile terminals. Thus, videoconferencing has become commonplace and accessible to the vast majority of people thanks to its usability and simplicity.

Videoconferencing systems have made it possible to bring the communication, collaboration, and coordination process closer in multiple scenarios and administrative procedures:

- Continuing with the example of the courtroom, it is now possible to testify without having to travel to the courtroom, from the place where the witnesses and investigated persons are located.
- It is possible to make medical consultations.
- Online training has been improved, allowing access to virtual classes that are recorded and whose subsequent playback allows reinforcement of knowledge.
- Virtual job interviews.

- Government meetings, sectoral committees, institutional meetings, among others.
- The relationship model between the lead institution and the sectoral institutions is based on videoconference meetings.
- Costly meetings, which involved travel and subsistence expenses, as well as the time required for travel, have been optimized, as they can be held online with all the guarantees of security.

OTHER TECHNOLOGICAL SUPPORT ALTERNATIVES AT HEADQUARTERS

Finally, thanks to technological progress in recent decades and the introduction of ICT in public administrations, there is a wide variety of elements that provide flexible and effective solutions to solve each of the problems that can be found in administrative procedures. These solutions range from simple appointment dispensers to facial recognition systems that, supported by artificial intelligence, allow automatic recognition of people, with a probability of success of 100 percent.

The main advantages of having these types of elements are the following:

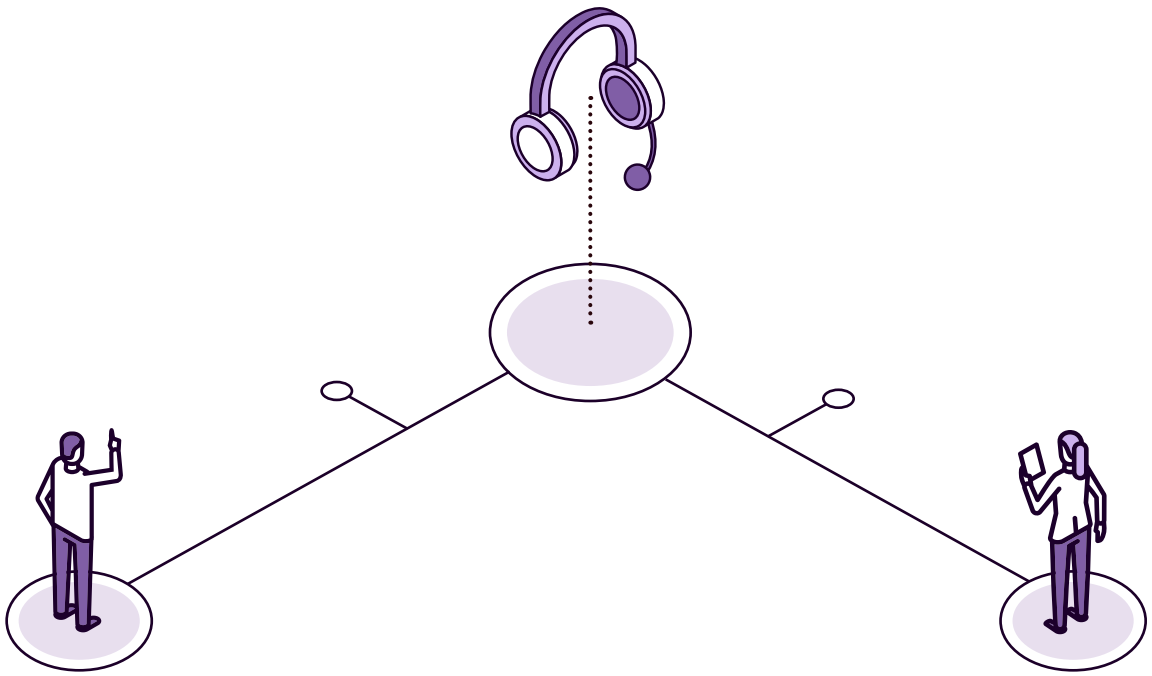
- They drastically reduce the workload and time of all officials involved.
- They improve productivity and quality of public services.
- They make it possible to provide a closer service, guided and focused on the citizen, whatever his needs may be.
- They make it easier to implement a communication plan automatically, disseminating content on the agreed dates, news, awareness campaigns, events, and initiatives to be publicized, etc. This improves the information process offered to all the actors involved: citizens, civil servants, etc.

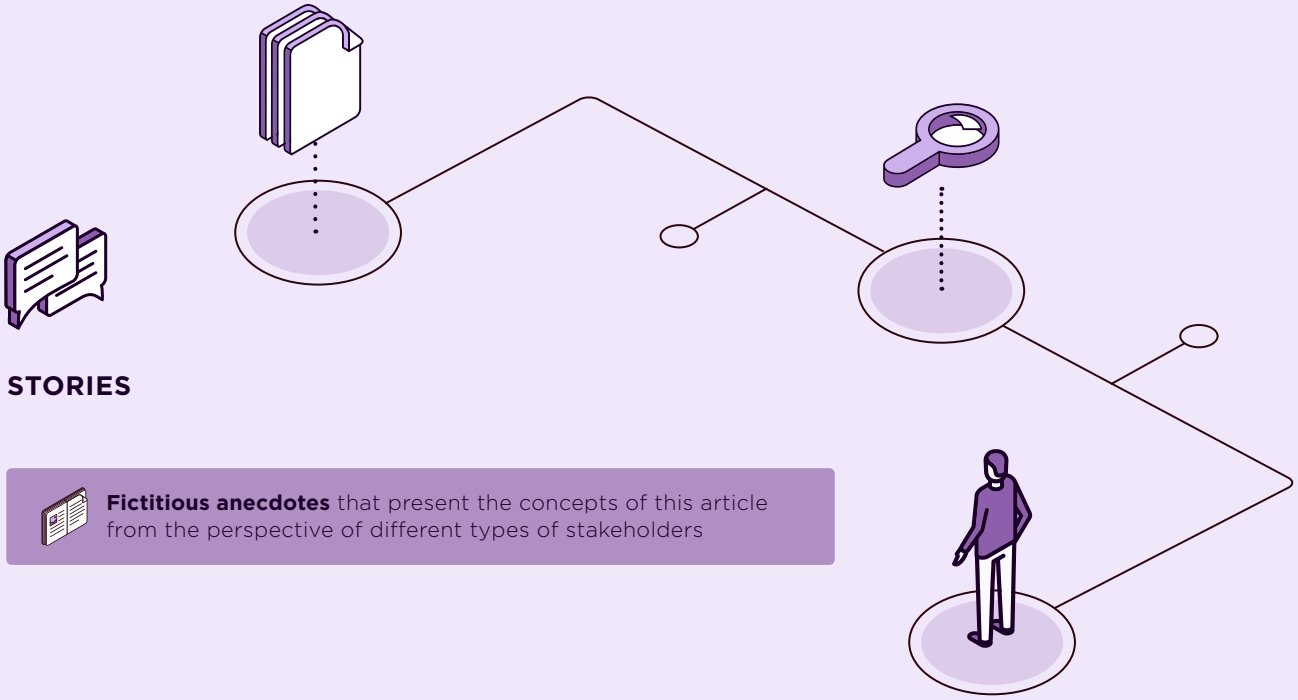
IN THE CONTEXT OF PUBLIC ADMINISTRATION, INTEGRATED SOLUTIONS TAKE ON GREATER INTEREST, GIVEN THE COMMITMENT TO EFFICIENCY, EFFECTIVENESS, QUALITY OF SERVICE, AND ECONOMIC RATIONALIZATION.

All of this equipment distributed in the public offices must have two technical teams:

- An organizational one in charge of IT equipment management, maintenance, and support
- Another person responsible for editing, approving, and publishing content (i.e., managing and implementing the communication plan)

In general terms, it can be concluded that, depending on the area in which they are working and the administrative procedures that support their public service, it is necessary to provide the headquarters with some means or others that help to efficiently manage the different problems that arise in their day-to-day work. In order to carry out a correct and planned needs analysis, the lead institution can have a media plan with the devices, tools, and solutions it provides centrally to the sectoral agencies and ministerial departments. For their part, the sectoral institutions will draw up a media plan adapted to their headquarters, which will be based on that of the lead institution. This tool should contain the necessary means that a "typical" headquarters must use, and each of these means must be associated with a business process, indicating what problem it solves and for whom.





STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Mayor's advisor
Daniel

In Daniel's town hall, citizens are allowed to carry out formalities related to their country's taxes. Every day his office receives hundreds of visits from citizens who come to carry out different types of procedures. Unfortunately, the municipality cannot attend to them all due to the amount of time spent explaining them. On the other hand, the number of interruptions caused by citizens who go to the wrong counter is enormous. At the same time, there are other types of citizens who hand in documents that are simply photocopied and stored in the system, without being able to be cata-logued correctly, since this would increase the time of attention per citizen, so that not all of them could be attended to, generating a long delay at the office. Daniel has decided to install systems to guide citizens in the correct completion of the procedures, as well as an appointment dispenser and a kiosk that guides people and indicates the necessary documentation to be provided. This has reduced the number of unsuccessful procedures at the head office by 80 percent.

EXAMPLES

Click on each flag or icon to go deeper.

Spain

Salas de Vista (SV)

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Do the citizen service areas located in the different offices have the necessary means to automate processes that can be carried out without human intervention?
- Are there audiovisual elements that inform citizens about the correct way to carry out the procedures?
- Is there a system for managing appointments and printing out appointments?
- Can citizens carry out procedures that do not require human intervention automatically, themselves, at totems or similar?
- Are there any information, assistance or guidance points when using kiosks or ticket vending machines at the administrative headquarters?

4.1.3 USER STATION INFRASTRUCTURE

People often make the mistake of believing that a desk, a computer, and a few other accessories are all it takes to have an adequate workspace, but nothing could be further from the truth. In some cases it may be that a table and a computer is enough to perform the task; however, it must be taken into account that, in general, public employees spend about forty hours a week in the workplace, so they must be more than comfortable areas and have the elements that allow them to work efficiently.

Public administrations, like all other organizations, are gradually joining the technological evolution of the workplace, deploying solutions that enable functional, collaborative, delocalized, and mobile work—in other words, an intelligent workplace.

Within the digital transformation of government, it is necessary to have an axis that takes into account a concrete measure for the digital workplace. It is here again where the lead institution plays a predominant and centralized managerial role, as it has to lead the strategy of defining, acquiring, configuring, managing, and supporting the workplace. This strategy implies having a technical team whose role is focused on the intelligent workplace. This team will be in charge of the policies, procedures, technical instructions and tools that will support the end users. To this end, it is necessary to focus on the definition of the workstation based on a classification of profiles, roles, and responsibilities, and thus design the workstation according to the needs of each profile, in order to make a more responsible investment.

IT IS ABOUT MAKING AVAILABLE TO PUBLIC EMPLOYEES WHAT THEY NEED TO DELIVER THEIR SERVICES IN THE MOST EFFICIENT WAY.

New office tools and other technological solutions enable secure access to the workplace by implementing additional authentication factors via other devices, such as cell phones. Thus, information can be shared securely in the cloud within the work team, and functions such as collaboration, coordination, task sharing, and planning can be performed remotely without any problems: virtual meetings are the order of the day. All this must go hand in hand with cybersecurity measures that facilitate mobility and device management, so that not only responsible access to information is guaranteed, but also the location of the device and remote destruction in the event of theft. The information on the mobility equipment can be constantly encrypted.

Focusing on the activity to be performed by public employees and making available to them equipment and technological tools that allow them to perform their work comfortably and efficiently, more than an option, becomes an obligation if we want an organization capable of working efficiently and sustainably. Again, a governance model between the lead institution and the rest of the sectoral institutions is necessary to consider all the particularities of the vertical sectors but, above all, to identify all the aspects common to the implementation of a digital workplace based on centralized procedures.

Therefore, when considering technological tools, it is not only necessary to think about physical devices in the workplace or office automation and collaboration tools, but also about digital training and the incorporation of new skills for employees. Technological advances in recent decades have completely redefined work procedures.

CHARACTERISTICS ASSOCIATED WITH THE NEW DIGITAL WORKPLACE

- **Improved efficiency in work performance:** Normally, this type of advantage is achieved by simplifying processes and developing tools that allow the automation of repetitive processes in which user interaction is not necessary, or at least not throughout the entire process.

- **Increased cybersecurity:** To ensure impenetrable workplaces, in view of the increasingly sensitive information they have to manage.

- **Collaborative environments:** Nowadays it is possible that within an organization with a large number of employees, all of them are connected to each other, regardless of the internal hierarchy. This connection makes it possible for them to collaborate on projects, share information, etc. Providing the organization with tools that allow the rapid dissemination of information necessary for the work is possible today using the tools that technology puts within our reach.

- **The need for digital skills:** The use of all the technological means available to work teams requires the incorporation of new skills that were unknown until now. It is necessary that officials have digital training that allows them to use all the technological tools in an efficient way, taking advantage of the functionalities they offer. Failing this, it will be necessary to carry out digital training programs.

- **Coresponsibility and sustainability:** The provision of computer equipment, office application licenses, mobile devices, as well as other technological tools, implies a responsibility on the part of the organization and a coresponsibility on the part of the employee regarding the care, maintenance, and correct use of these resources. In the same way, it is essential to think about sustainability when using these means and to avoid that their misuse can have a negative environmental impact (for example: turning off the equipment when it is not being used to reduce the energy consumed and, therefore, the level of CO2 emitted).

- **Mobility and relocation of the workstation:** The equipment allows the workstation to be moved from one place to another easily and lightly. A public employee can be at his desk, have a virtual meeting, or attend a face-to-face meeting in another room by bringing his own equipment to take notes or share documentation.

- **New ways of working:** The new mobile devices, together with the benefits of office automation and telecommunications solutions, make it possible to consider teleworking as an alternative to the physical workplace in the office, and as a driver of inclusion and work-life balance.

The above points make it clear that ICT has given rise to the birth of the "virtual office," capable of moving with the worker wherever he or she goes, and is having a strong impact on the distribution of physical space in the company. As a result, despite having followed parallel paths in the past, space and technology are tending to converge as two completely interdependent dimensions of the same reality: the work environment and the associated workstation, nowadays the intelligent workstation. This has reached such a point that it can be established as a general "rule" that, with some exceptions, the greater the requirements of technological resources for collaboration and mobility of a worker (virtual office), the lesser the need for "owned" or exclusively occupied space (physical office).

MOBILE WORKSTATIONS

Public employees need to have digital workstations that make it easy to work anywhere. However, these interfaces are not always the most comfortable or ergonomic. For this type of problem, the most common solution is often the use of *dock stations at workstations*. These devices make it possible to use a mobility device as if it were a desktop computer, with the possibility of having screens of better resolution and size, in addition to other types of devices, such as printers, cryptographic card readers, or scanners, simply with a single connection and without having to connect one by one each time you arrive at the office. Once the user has finished his working day, he can take his mobility device—and thus his entire workstation—home with him in case he wants to do some business or simply work from home the next day.

VIRTUAL PRIVATE NETWORKS

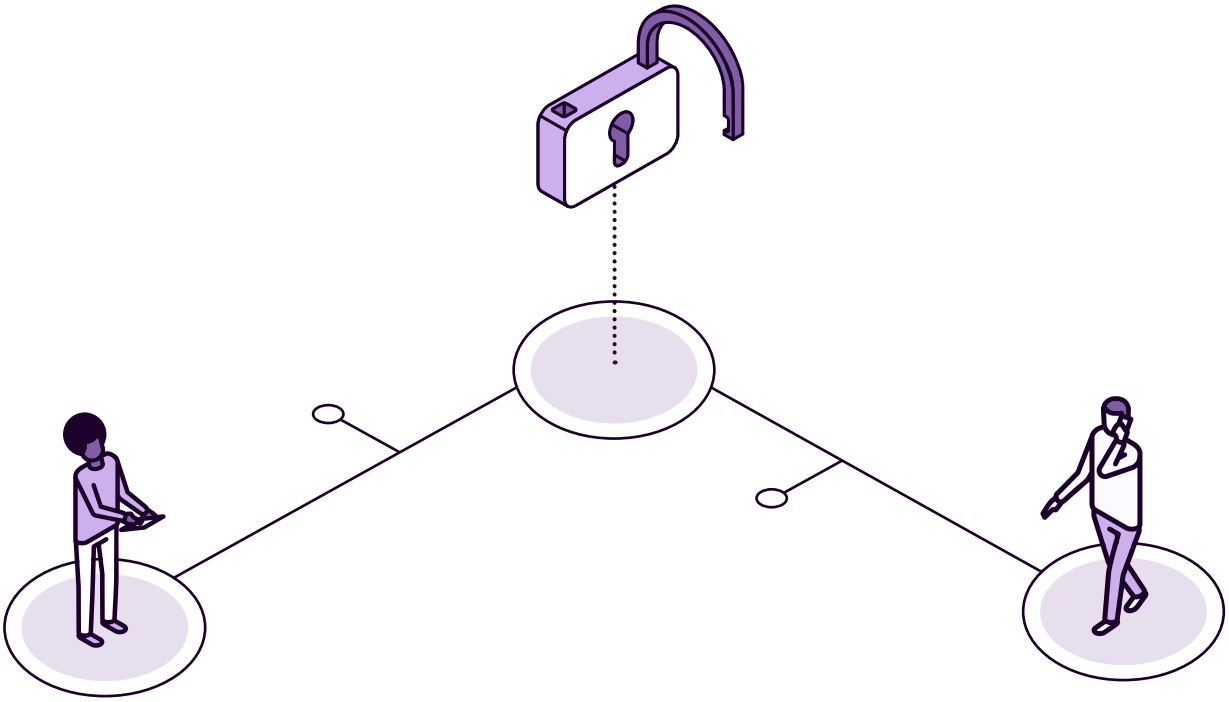
It is not only necessary to have mobility equipment, but also a central infrastructure that allows connectivity from anywhere to the organization's work environments. As a first alternative, virtual private networks (VPNs) allow an employee to connect from home without any problems and work with the same workstation as at their physical headquarters, ensuring that internet traffic is carried out safely and securely, just as if they were connected to the local network of their workstation. A VPN provides the employee with a secure network connectivity from their workstation at home to the office communications network.

VIRTUALIZATION

In the same way, other technological alternatives are the virtualization solutions of the workstation, either by remote desktop or virtual workstation. This option provides access to the workstation, with all the applications and permissions, from any device—for example, a personal computer at home—with all the associated security measures. In this way, the user connects from home to a secure workstation made available by the organization, which could be his own computer in his office or a virtual desktop deployed in the organization's infrastructure. This solution can be combined with a VPN (i.e., this remote desktop or virtual workstation could be accessed through a private network, which provides much more security).

BYOD: BRING YOUR OWN DEVICE

Virtualization opens up another possibility that is spreading in many organizations: the so-called BYOD model (i.e., "bring your own device"). Until a few years ago, it was common for companies to be technologically better equipped than users. For example, many people did not have a computer at home but did have one at the office, and it was common for those who had a laptop or cell phone to have these devices because they had been provided by their company. However, advances in technology and its consumption have reversed this trend: today, it is more common for users to have more advanced, productive, and efficient technology than that provided by the institution or company itself.



BYOD consists of allowing the employees of an organization to bring their computer equipment (tablets, *laptops*) and work with them within the organization itself, connecting them to the network and accessing its resources. This model can also be incorporated in the public sector, as it has the following advantages:

- Increased productivity and satisfaction level
- Reduction of the learning curve
- Reduction of acquisition and maintenance costs of the workstations
- Immediate implementation of the telework model

However, this type of solution has a number of drawbacks associated with it that should not be underestimated, as they can cause serious damage to the organization if not managed correctly:

- The security of the private network may be compromised, as users' devices may contain *malware* and infect the organization's network when they connect to it.
- The organization's information can be compromised in the event that a user loses a device containing work data and there is no solution that allows for its remote deletion, or simply if it is not properly protected by encryption or some other type of mechanism.
- Possible increase in the cost of support and maintenance departments, as there may be compatibility issues between some user devices and certain applications.

In order to try to solve this problem, there are a number of programs called MDM (*mobile device management*), which allow to perform certain tasks on these terminals remotely, such as the following:

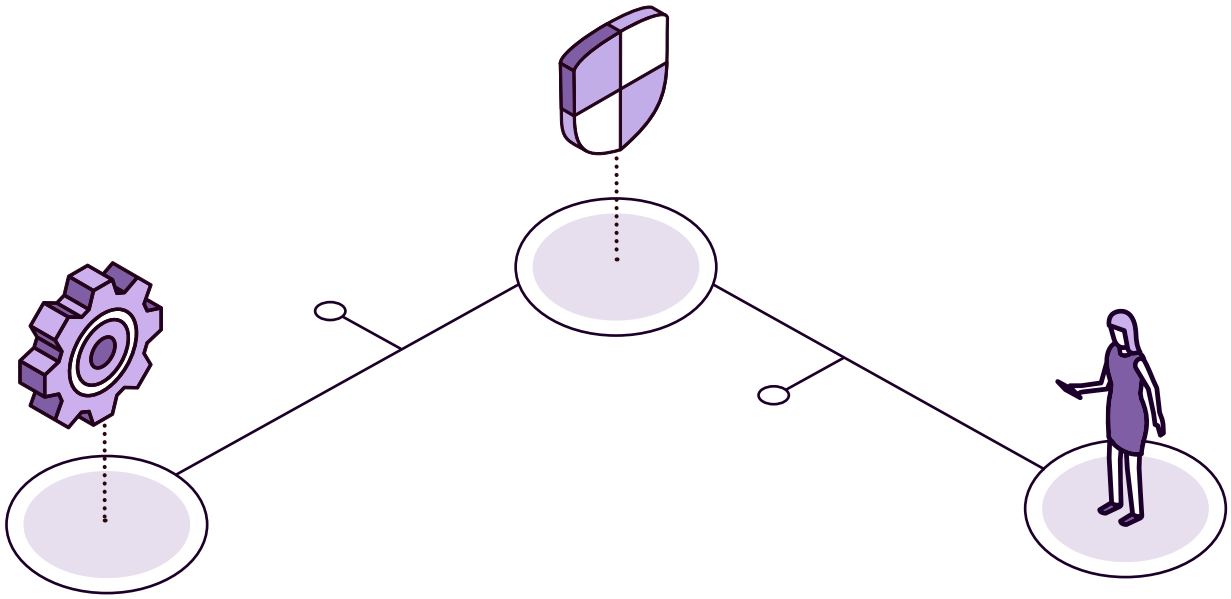
- Massive and remote installation of applications, such as antivirus, to ensure information security
- Control of certain applications that may or may not be used
- Physical location of the device
- Locking device functions
- Remote data deletion

In other words, this type of MDM application will provide the essential functionality to ensure the security of the organization's data.

In summary, there are a number of criteria that must be taken into account to ensure security if you decide to opt for BYOD:

- Corporate network access and services must be guaranteed and therefore protected.
- An additional layer of security must be in place for all devices connecting to the network.
- The communication of these devices with the organization's network must be encrypted on a mandatory basis to ensure security, so employees must be trained or given guidelines on how to use the corporate network with their devices in a secure manner.

The above is a picture of the new intelligent workplace, on which the digital transformation of government must work to make it available to its civil servants. The renewal of the public sector workplace is an issue that cannot be postponed, although it requires considerable investment and a commitment to incorporate digital capabilities and awareness of the use of confidential information, personal data, and cybersecurity in general.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Mayor's advisor

Daniel

Daniel works every day in his office at city hall on his own personal device because he has chosen to do so. The IT department provides him with access to a virtual workstation at city hall, where he performs his professional tasks. Thus, his workstation is a "window" to his own laptop. As it is his personal device, it allows him to perform other tasks in his private life in his free time and on his commute to work. This gives him a lot of flexibility with just one device, with the weight and transportation advantages that come with it. In addition, the municipality saves on hardware made available to employees who choose this option.

EXAMPLES

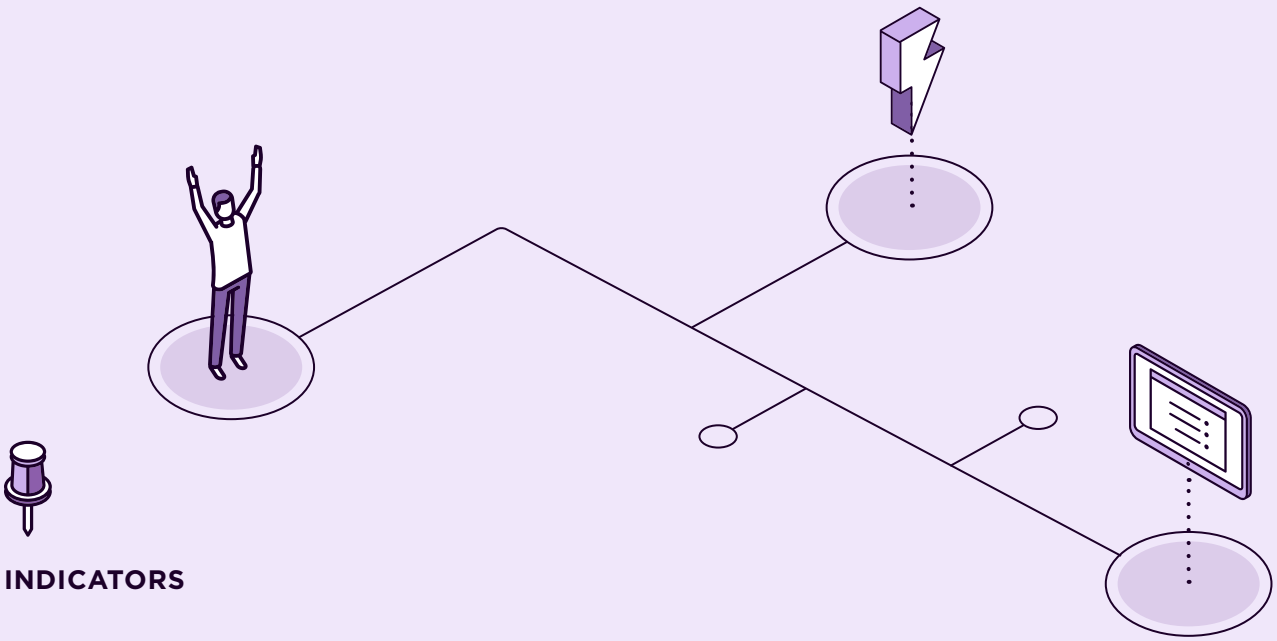
Click on each flag or icon to go deeper.

European Union

Digital Workplace Strategy

Singapore

Digital Workplacel



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Do the organization's users have the necessary elements to carry out their work efficiently? Do they have a workstation with a personal computer and auxiliary devices? Do they have office automation tools? Do they have a videoconferencing solution at their disposal?
- What percentage of the organization's users can access the organization's data from off site, if necessary? About 25 percent? 50 percent? More than 75 percent? 100 percent?
- What percentage can access your corporate mail from outside the organization? About 25 percent? 50 percent? More than 75 percent? 100 percent?
- What percentage has the possibility of teleworking from home? About 25 percent? 50 percent? More than 75 percent? 100 percent?
- Have employees received training on new workplace tools?
- If an employee were to lose a device belonging to the organization, would it be possible to locate it or implement the relevant mechanisms to ensure that the information it contains is not exposed?

4.1.4 CLOUD

Cloud technology is basically the provision of an organization's ICT needs from a separate entity. The type of provision will depend on the type of need; the most common is ICT infrastructure (servers, information storage, communications), an area in which there is a strong market. Likewise, when talking about the cloud, it is often related to this need, which is called infrastructure as a service (IaaS).

However, in addition to the infrastructure, it is possible to include services and improvements that extend the functionality; for example, having the database in the cloud, which includes the base *software* licenses, those of the database itself, the associated support and maintenance services, etc. In this case, we speak of platform as a service (PaaS); the agency's ICT services have certain packaged services, provided externally to the agency, for its ICT development.

Finally, there is the possibility that what is offered externally is the complete service itself, according to the needs of the organization; for example, the office automation system, electronic mail, etc. These are the usual services, but more specific services or *software*, such as municipal management systems, accounting management systems, etc., can also be provided.

This type of approach to ICT service delivery is increasingly used in both the public and private sectors, and today it is no longer an emerging technology, but rather an option to be considered in practice for all government ICT projects.

Cloud technology can be either public or private:

- **Public:** This is the cloud offered by companies to any public, be it the government, other companies, or citizens. This type of cloud has the well-known global North American providers (Amazon, Microsoft through Azure, Google, etc.) and from other countries, especially China, as well as more local solutions, usually associated with the telecommunications companies that provide the service to a country.

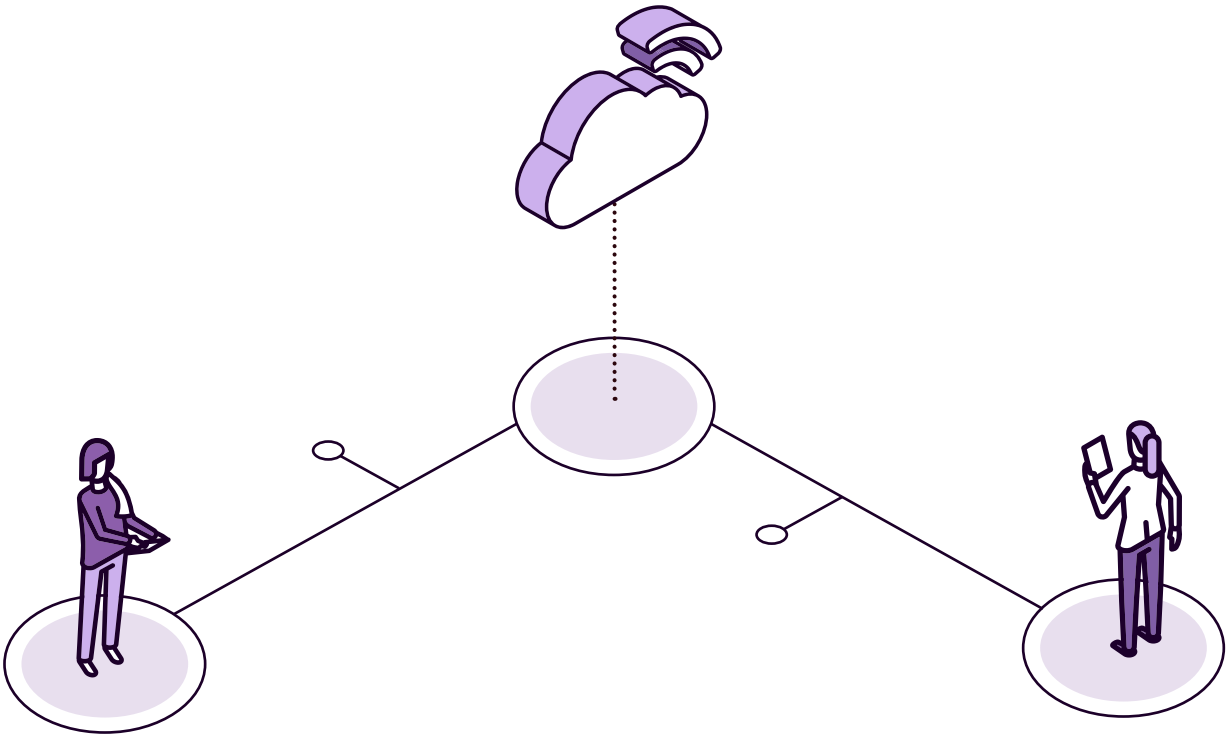
- **Private:** In this case, the characteristics of cloud systems are maintained (on-demand services, great elasticity in the face of increases or decreases in computing or storage needs, pay-per-use, self-service, speed in the deployment of new servers or projects, etc.), but it is the organization or institution itself that provides the cloud for itself. In this way, technology or banking companies and governments have their own cloud infrastructure for their own use, but with this technology.

This section considers these solutions, which lead governments to create a private cloud to offer services through it to their own agencies or other public institutions. For this purpose, the focus will be on infrastructure, platform, and application cloud services. There are other services that can be offered following the cloud philosophy, such as communications or cybersecurity, which are discussed in other sections. The following three sections will present the classic classification of cloud services:

Infrastructure as a service (IaaS)

Platform as a service (PaaS)

Software as a service (SaaS)



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara is driving digital services in the ministry, and she is able to do it thanks to cloud services. If she had to contract out the infrastructure or information systems, or if she couldn't leverage e-ID services in the cloud, this digitization drive would be much more expensive, time consuming, and complex, as the ministry would have to have all the technology—from data processing centers to digital services—autonomously and independently.

Mayor's advisor
Daniel

Daniel fully understands that until now municipalities like his were lagging behind in offering digital services; in the absence of a cloud strategy, they had to build a data processing center, buy servers and other hardware, purchase expensive software licenses, or have specialized technicians in all areas, which was clearly impossible. Thanks to the cloud strategy, now everything you need you get as a service, so now your municipality can provide digital services of the same quality as the capital of the country or the national government.

4.1.4.1. GOVERNMENT PRIVATE CLOUD: INFRAESTRUCTURE AS A SERVICE (IAAS) FOR AGENCIES

Although shared data processing centers and IaaS are not equivalent, in this section they are presented together because both are aimed at improving the provision of ICT infrastructure to a unit that requires it, without requiring the latter to make the heavy investments necessary to make it available.

The provision by a centralized unit of data processing center (DPC) services, the data center in its most basic form (in this case, one could not strictly speak of IaaS cloud service, but rather of *housing or hosting*[30]), covers one of the great needs of IT departments. Since data processing centers are expensive and complex infrastructures, requiring a huge initial investment and a large economy of scale, it is more interesting to build one or several large centers to be used by several administrative units or even several institutions. This saves each one from having to carry out civil works, maintain the security of the center, make investments to prevent the center from ceasing to provide service in the event of any eventuality, etc.

The next phase is to offer infrastructure as a service.[31] In this case, in addition to avoiding the need for the consumer agency to have a secure, refrigerated physical space with uninterruptible power supply systems and generators to ensure continuity in the event of power interruptions, etc., computing capacity, storage, and other infrastructure services are provided directly from a private government cloud. In other words, the consumer does not have to buy servers, disks, storage systems, etc.; he uses what he needs as a service, whether it is offered by the government or by a company.

The traditional approach, where each unit creates its own data processing center and provides services to itself,[32] not only does not have the economic advantages that are achieved with DPC consolidation, but—especially except for very large or very specific organizations (defense, internal revenue service, or social security)—the service provided by a government private cloud is of a higher quality and has many advantages for the ICT units compared to a decentralized option.

---

30. See https://en.wikipedia.org/wiki/Web_hosting_service.
31. See https://en.wikipedia.org/wiki/Infrastructure_as_a_service.
32. From Wikipedia: *data center o data centre.* Is a building, a dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems. (Available in https://https://en.wikipedia.org/wiki/Data_center).

There are many reasons for this. The first is economies of scale: in the DPC ICT infrastructure, centralized purchasing capacity allows for significant savings in the purchase of servers, storage, internal DPC communications, security equipment, etc., as well as associated software. The same is true for the data center itself: the requirements of a government data center are very stringent and costly, requiring redundancy in power supply and uninterruptible power supply systems, strong access control and physical security, secured buildings, etc. These costs mean that the data centers of small agencies do not meet the characteristics and international classifications necessary to ensure the continuity of services for critical government issues.[33] All the advantages of the cloud are achieved with this approach.

› *Example:* If the government provides this service, and a ministry has to, for example, set up a new project, it does not have to worry about tendering or stockpiling servers, disk arrays, etc., or even expanding or creating its own DPC but can use the services of the government cloud. Thus, you immediately have the necessary infrastructure for your project and at a minimal cost to the government, compared to the option of the ministry buying the necessary infrastructure on its own.

TYPICAL STEPS TO IMPLEMENT A CLOUD PROJECT

1. As a preliminary consideration for this project, take cybersecurity guidelines into special account, since it is essential that these guidelines are complied with by the infrastructure providing the services.

2. Prepare a study of the plant and inventory of the resources currently available to each of the governing bodies, and determine the growth forecast that exists.

3. At the same time, carry out a study of the characteristics of the current data centers. Ideally, with the necessary investment, one of them could be upgraded to become the data center or one of the data centers serving the government's cloud:

    - If there are viable data centers, agreements will have to be reached to change their ownership or enter into a usage agreement, so that there are no problems in relation to the data center that will provide the service to any government body.

    - If no viable data center can be found, it will be necessary to study the costs and possibilities for setting up a government data center, with the idea that it will provide its service to all agencies.

---

33. See https://en.wikipedia.org/wiki/Data_center#Data_center_levels_and_tiers.

These options, of course, do not have to be 100 percent public; they can be supported in whole or in part. The data center can be located in a facility already created and, with the necessary features, in an enterprise, or even in a public cloud (in general, this option will not be for all services—only some where there are no security, data protection, or regulatory issues). In this way, the private cloud of the public entity behind closed doors is really a hybrid cloud.

4. Include the agreements or the way in which the consumption of services will be regulated by the different agencies, and the mode of economic relationship between the consumer and the service provider.

5. Ensure that harmful incentives are not generated (e.g., consumption cannot be costless for agencies because they will not make good use of the resources) and that the advantages of speed in providing services and deploying the infrastructure that agencies need are not lost.

THE IAAS OFFERED BY THE LEAD INSTITUTION IS THE BASIC PILLAR ON WHICH TO BUILD SERVICES, SO IT HAS MORE USES THAN PRECONDITIONS. EVEN SO, SOME OF THESE USES MUST BE CONSIDERED IN ORDER TO FACILITATE AND EXPLOIT IAAS TO THE MAXIMUM IN THE ORGANIZATIONS.

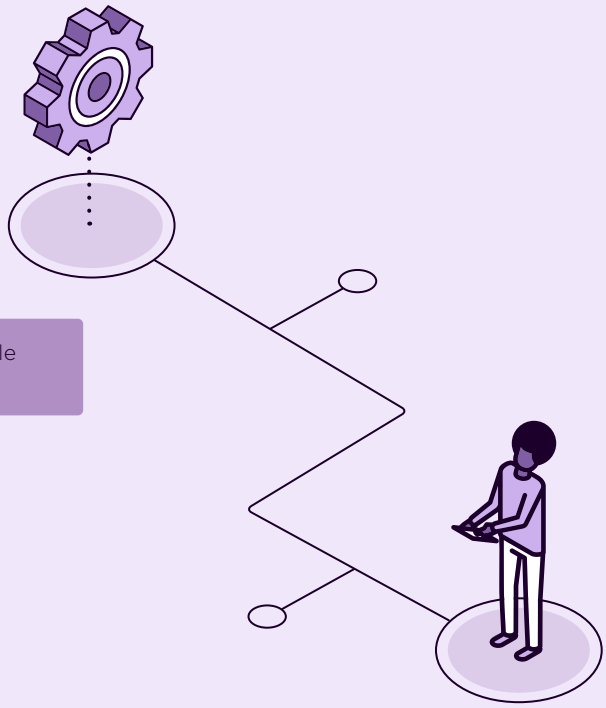
RELATIONSHIP WITH OTHER MODULES

The idea is to offer this service to public entities, not as IaaS per se, but to facilitate its consumption; therefore, the system will be related and will benefit from certain modules like any other system:

- The directory of administrative units, to associate the infrastructure to the user entity
- The identification and electronic signature system for, for example, signing the start-up of servers or storage, which have a cost on the part of the institution or organization requesting it
- The system of roles and registration of officials, to ensure that the signatory is the one who can request what he/she is asking for.

Having IaaS benefits all services. Potentially, all technological services can be mounted, with considerable advantages compared to ad hoc infrastructure, on the state's IaaS system.

STORIES



Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Like the rest of her counterparts in other ministries, Sara has a data processing center at the ministry's headquarters that used to occupy an entire floor in one of the best areas of the city. She would like to be able to take advantage of this space to improve services to citizens. In addition, the center does not provide her with adequate security conditions (double power supply, fire protection systems, uninterruptible power supply). Fortunately, the national digital government office is offering you infrastructure as a service (IaaS). Thanks to it, you will be able to scale easily, and you will have more peace of mind, as the service is more secure and will reduce costs.

Mayor's advisor
Daniel

Daniel needs servers and data storage for the new digital citizen service project. Thanks to his country's cloud strategy, he can have them immediately available, and he gets significant savings, as his municipality does not have to buy them.

EXAMPLES

Click on each flag or icon to go deeper.

Canada

Case of DPC consolidation in Canada

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a centralized DPC with hosting/housing services for other agencies?
- Is there such a thing as a government private cloud? If so:
  - Do you have virtual servers, and is there a capacity plan to estimate the growth of processing needs?
  - What is your net storage volume, and is there a capacity plan to estimate storage growth?
  - How many user organizations do you have?
  - Are there subnational governments that are users?

4.1.4.2. GOVERNMENT PRIVATE CLOUD: PLATFORM AS A SERVICE (PAAS) FOR AGENCIES

Platform services (PaaS) refer to the provision by a centralized ICT services unit of necessary modules or services that are more complex than the infrastructure itself (i.e., it is more than just servers, communications, and storage), but have no end value on their own, as they have to be combined and extended with others or have to be worked on to have real functionality for the end user.

The platform is considered to be a service; therefore, it covers all the intermediate level between the infrastructure and the final applications that serve officials or citizens. This includes, by way of example, databases, authentication systems, messaging, etc. These services are usually provided from the government's private cloud to the different ICT units of ministries and public agencies, and even to other entities. The provider of this service is usually the governing body of the digital government itself, a public company, or the public telecommunications company.

It should be noted that even if a cloud infrastructure service (LaaS) is not available, cloud platform services (PaaS) can be provided to other units. Logically, the existence of PaaS on top of a government IaaS multiplies the synergies of both projects, since the cloud platform service benefits from all the advantages of IaaS (elasticity of demand, rapid deployment if necessary, cost reduction, and economies of scale).

The approach of providing more packaged or advanced, higher value-added services directly from a centralized agency to users represents a significant improvement and greater cost savings than offering infrastructure alone. This is because not only the costs associated with the infrastructure are shared, but also those of the software required for the infrastructure to function (operating system licenses, antivirus, database licenses or application development environments, etc.), as well as those corresponding to the technical assistance that enables the system to function,[34] costs that in many cases significantly exceed the infrastructure costs themselves.

34. For a database system to work, for example, it is necessary to perform different configurations, maintenance of operating system versions, and the application of patches, as security problems are found, review of space consumption on the server, adjustments when necessary and a long etcetera. PaaS makes it possible to contract the database service (or development environments, software testing, messaging, etc.) and forget about all this, since it is the provider who takes care of all these tasks to keep the system running.

However, although cost savings in many cases is the main reason for promoting this type of project, it should be emphasized that, as in the previous case, the important thing is that with a small fraction of the cost a significantly greater result can be achieved than what the organization could obtain by its own means. This is especially relevant for small and medium-sized organizations.

ADVANTAGES OF PAAS FOR SMALL ORGANIZATIONS

- They may have technical capabilities that would be impossible to imagine if they had to manage on their own. This is common, for example, when providing database services as a platform.
- They benefit from the technical staff that handles database administration tasks, which is specialized and highly experienced, instead of having to hire staff on their own, something they often cannot achieve due to volume.

THE PLATFORM AS A PUBLIC SERVICE REPRESENTS A SIGNIFICANT IMPROVEMENT BOTH IN COST SAVINGS, AS IT CLEARLY EXCEEDS THE SAVINGS OF IAAS, AND IN QUALITY OF SERVICE.

Another reason why these services are needed from a public perspective is that, unlike IaaS, there is not as much of a private market. While in the case of IaaS there are multiple options at the international level, and there are usually options in the local market as well, at least in countries that handle large volumes of business, for PaaS there are not so many options for service provision by companies. For example, large proprietary database vendors often have cloud services, but it is not as common in other areas, such as backup management, development or test environment management, load testing systems, documentation, deployments, collaborative development, etc.

WHAT TO CONSIDER BEFORE TURNING TO PAAS?

- What agreements are needed or the way in which the consumption of services by the different agencies will be regulated.
- The mode of economic consideration.

- A way in which:
  - Bureaucratic burdens are not increased;
  - No detrimental incentives are generated (consumption cannot be free for organisms, because they would not make good use of resources);
  - The advantages of speed in providing the services that agencies need—one of the great benefits of these projects—are embraced.
- What types of platforms will be deployed as services, from databases to application development environments, from mobile services to load testing or attack systems.
- Cybersecurity guidelines, since it is essential that the platform providing the services complies with these guidelines.

As far as possible, the idea is to generate added value on the services; to this end, services can be added on top of the infrastructure itself and, in this way, provide a service as a platform that is more useful to the institutions.

- *Example:* It is more useful to provide not only a server as infrastructure (IaaS), but also the technical services of configuration, support, and maintenance. Thus, by adding the layer of technical support services and specialized personnel, all IaaS services can be offered not only as infrastructure, but also as a platform, which saves costs for agencies and significantly improves the service received.

When the system is set up, and in general the more it is used, the more savings and benefits it will produce, so it will be necessary to go through the different units to integrate them with this type of system, so that they are incorporated into the project, and the company's own resources, both personnel and financial, are freed up for the provision of these services.

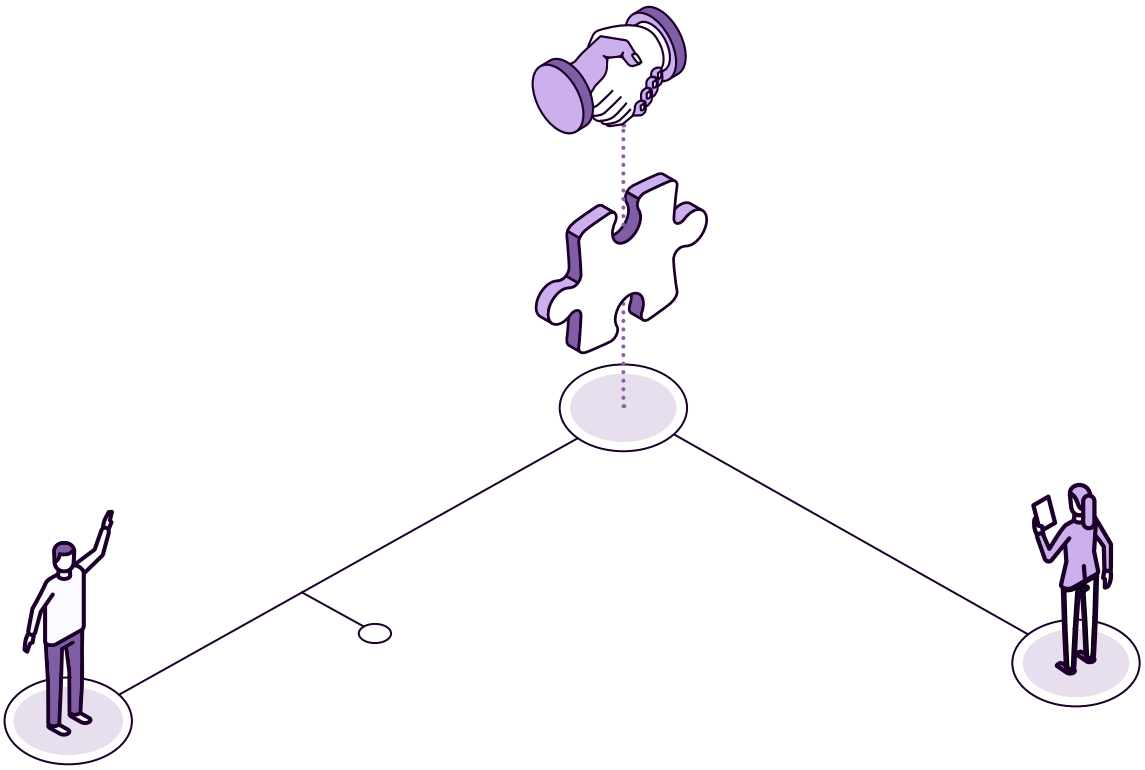
The PaaS offered by the lead institution can be built on top of the IaaS, if available. As in the case of IaaS, some common services must be considered to facilitate and exploit PaaS to the maximum in the administration.

RELATIONSHIP WITH OTHER MODULES

The idea is that this service will be offered to administrations, so—not as a PaaS per se, but to facilitate its consumption—the system will be linked and will benefit like any other system from certain modules—for example,

- The directory of administrative units, to associate the platform to the user institution;
- The electronic identification and signature system—for example, to sign the start-up of the platform, which has a cost for the entity requesting it;
- The system of roles and registration of officials, to ensure that the signatory is the one who can ask for what he/she asks for.

HAVING PAAS BENEFITS ALL SERVICES, AS POTENTIALLY ALL OF THEM CAN BE MOUNTED ON TOP OF THE STATE'S IAAS SYSTEM.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

The Ministry of Health works with database technology from a specific manufacturer, which makes it difficult to carry out IT projects using other database technologies. Thanks to the digital government database platform as a service (PaaS) to which Sara is now attached, she only has to use what she needs as a service, without having to purchase licenses, have database administrators, etc. In fact, it is so cheap for her that she is thinking of migrating all her databases to the digital government service.

Mayor's advisor
Daniel

Daniel has limited resources in his municipality for the provision of services. Although they had professional servers and systems for the environments that provide services to citizens, the development of projects was done by external technical teams, which made it difficult to share information, and sometimes even led to the loss of documents or developments when a technician left. Thanks to the platform for application development and testing of digital government, today his municipality no longer depends on the teams of technicians, but there is a professional and shared application development environment, and the performance and security tests that this allows have greatly improved the quality of digital services of the municipality.

EXAMPLES

Click on each flag or icon to go deeper.

Spain

Cybersecurity as a platform

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a platform as cloud services in the country? If so, are the following platforms offered as services?
  - Databases
  - Application development environments
  - Mobile services
  - Load test systems
  - Attack testing systems
- Is it connected to the identification and digital signature system?
- Do more than half of the central government institutions use the platforms as a service?

4.1.4.3. GOVERNMENT PRIVATE CLOUD: *SOFTWARE* AS A SERVICE (SAAS) FOR AGENCIES

SaaS consists of the provision of complete ICT applications or services from a lead institution, or under its control, to other public entities (or companies, in the case that it is appropriate—for example, to use the electronic identification system for a signature procedure). This *software* can be:

- General or common, such as email or office software;
- Specific—for example, a citizen relations management system for a municipality.

The idea is to include SaaS for public agencies, in a general way, with the condition that although it has a specific purpose, it is usable by multiple public entities, and therefore it is considered a common service.

In cases where the *software* is generic, there are usually companies that offer these services to public entities. However, as the organization focuses on more specific needs, the market shrinks, so that sometimes only the provision of *software* from an agency can cover the needs of citizen services of some entities or agencies.

- *Example:* Email is a generic service, and therefore many companies offer it in the cloud. Therefore, the lead institution may not provide it and may rely on the market, since it is needed by public entities, but also by companies, and it is generic (email has no limiting particularities). On the other hand, the state's interoperability platform is something very specific to public entities and can hardly be provided by anyone other than the lead institution.

IAAS, PAAS, AND SAAS: FROM LOWER TO HIGHER VALUE ADDED AND COMPLEXITY

Platform as a service is a significant improvement over infrastructure as a service for the effectiveness and efficiency of public services, and PaaS offers packaged services, which eliminates the administrative burdens of IaaS. However, as discussed in the case of PaaS, the ICT need of a public entity is the internal service to its civil servants or the direct service to citizens and businesses—that is, full end service (administrative processing or communications with the citizen, for example). Therefore, even better than having the pieces to put it together (processing capacity, databases, etc.—i.e., PaaS), the most effective option is often that, directly, an institution can obtain from another the complete service it needs for its internal operation or to provide services to citizens. This may be the case of directly obtaining the citizen folder or interoperability service.

This is especially important in small or underresourced units. A ministry should have no problem creating ICT projects to provide services to its officials or to citizens and businesses. On the other hand, a small municipality, for example, may not have the necessary resources available.

Thus, different forms of cloud technology help small entities at different levels:

- **IaaS** eliminates the need for physical infrastructure (data processing centers, systems technicians, servers, storage, communications, etc.).

- **PaaS** leaves aside the higher value-added needs that IaaS still requires from the user entity (database technicians, database licenses, development environment licenses and technicians, etc.).

- **SaaS** is in some cases the only option for certain organizations to offer advanced value-added services, thanks to the fact that another entity or company offers the complete applications they need. In this way, the organization will not even need developers, ICT project managers, user support systems, etc., because all this will be offered directly as a final service. Therefore, this modality is even more important than the previous ones.

Given the greater complexity of SaaS, except for common software (email, office automation, customer management, accounting), in many cases the market does not cover all the needs of institutions. In this case, it is essential that—if we want to eliminate the digital divide in the country, so that the more distant entities with fewer resources or less ICT capacity provide the same services and functionalities as the larger ones—someone is responsible for offering this software as a service to these small agencies.

STANDARDIZATION AND COMMON OPERATION AS AN ADVANTAGE OF SAAS

Consider the creation of a software as a service so that any citizen, through the internet, can send official documents to any institution or organization. The advantage in this case is not only that it is developed once and used thousands of times (cost savings) or that small municipalities that could not even dream of this service can offer it to citizens; it also lies in the fact that the system is common to the entire public service. Thus, if a civil servant changes from one unit to another, for example, he uses the same system for this task, and what is even more important: a citizen does not have to use and learn different systems depending on the unit he is related to. The system is common and works equivalently for all entities. This includes that, by default, all documents, certifications, and other such materials that depend on the use of the same software will be in a single format and compatible with the computer systems of the rest of the country.

WHAT TO CONSIDER BEFORE OPTING FOR A SAAS?

- **The unit that will be in charge of providing this *software* to the rest of the agencies or entities.** Digital government usually has a leading role in this task, but it is not surprising that other specific units offer SaaS within their competencies.

  - *Examples:*

    - If there is one unit responsible for procurement, it can offer e-procurement as software as a service to all interested entities.

    - If there is a person in charge of accounting and economic control in the state, he/she can offer the software that facilitates this type of control to all public institutions.

- **Which are the most interesting projects to offer this type of services.** Usually, through coordination forums with other public entities, it is possible to detect the needs of the different agencies, prioritize them, and, from the digital government or the competent body, create a SaaS project to meet the detected need.

- **An agile management for the incorporation of public entities to these services.** In fact, it is usually important that in PaaS or IaaS there is a system that covers the legal and management aspects to start the services, as it happens that in infrastructure or platform the number of user institutions is usually smaller, and due to its characteristics, there is usually more specialized staff (use by ICT teams, use by medium or large entities in general). On the contrary, in the case of SaaS, the organizations or institutions can be thousands (for example, all municipalities), and the users can also include personnel who are not accustomed either to technologies or to this type of project. Therefore, here it is even more important that the legal and technical system for joining, registration, use, and management of the system is very simple and easy.

  - *Example:* In a country there are usually hundreds or thousands of municipalities. If the lead institution offers a new service (an electronic payment gateway, for example, or any other common service mentioned in this document) to all municipalities on a massive scale (because, from the point of view of use, it has this capacity), some of the problems will be the following:

    - The management of thousands of agreements.

    - Obtaining the signature of the competent person in the municipality (the mayor, for example).

    - The desire to adhere to the system.

- Registration of the municipality's employees who will be able to use the platform.
- Consideration of the charges and income that this generates.
- Yes, the system allows massive use, but a paper process must be carried out to join, register, manage users, etc.

These drawbacks will increase management costs (if there are thousands of municipalities, the governing body will spend all day doing administrative procedures). On the other hand, everything can be done automatically:

- There is a user and membership management system.
- The mayors are identified in the system.
- The system is integrated with electronic identification and signature.

- **Some kind of support or training so that civil servants and citizens do not have problems using the service.** Again: a database will be used by specialized ICT personnel, but a software for dealing with a public entity can be used by any citizen, even those with digital literacy problems, and any civil servant, even those reluctant to use technology or those working in small units, with little training of their own. It is therefore important that, when considering this type of project, manuals, training, and issues related to user service for these systems should be kept in mind.

- **Cybersecurity guidelines,** since it is essential that the platform providing the services complies with such guidelines.

THE SAAS OFFERED BY THE LEAD INSTITUTION CAN BE BUILT ON TOP OF IAAS AND PAAS, IF AVAILABLE.

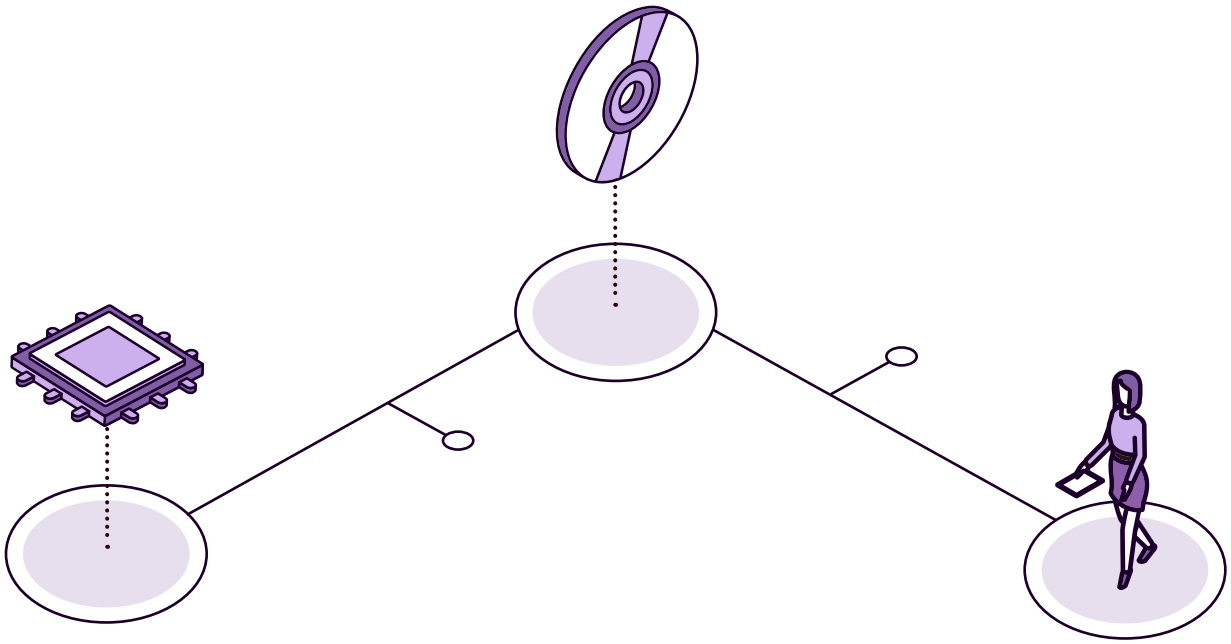
As in the other cases of cloud services, there are some common services to consider in order to facilitate and exploit SaaS to the maximum in public entities.

RELATIONSHIP WITH OTHER MODULES

The idea is that this service will be offered to the agencies; thus, in order to facilitate its consumption, the system will be linked and will benefit like any other system from certain modules, such as:

- The directory of administrative units, to associate the service to the user institution;
- The electronic identification and signature system, for example, to sign the start-up of a certain service, which has a cost on the part of the entity requesting it;
- The system of roles and registration of officials, to ensure that the signatory is the one who can actually request what he/she is asking for.

Potentially, all the technological services listed in this document can be offered as SaaS by the lead institution. This will allow those entities that due to their size and lack of personnel cannot offer advanced ICT services to serve citizens without discrimination based on their capabilities, since each and every one of the services listed in the document (from citizen folder to payment gateway, from communications with citizens to document entry on their part) are provided by a public entity, based on software as a service provided by another agency or a company, integrated with the country's systems.



STORIES

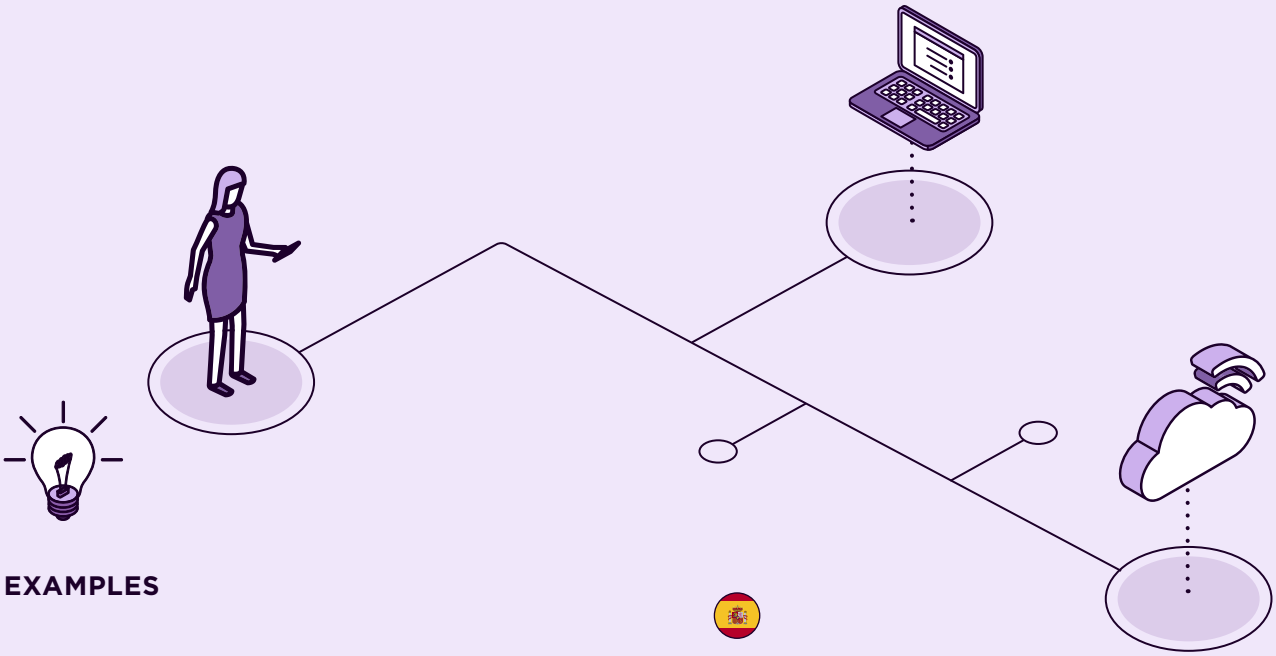
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Before starting any project, Sara always reviews the government's catalog of digital services. So, when the need for electronic identification was identified, she saw that there was a country service that covered it. When she wanted to eliminate paper signatures in her ministry, she noticed that there was the electronic signature service. Thanks to these cloud services (SaaS), his ministry did not have to develop the tools to cover them, since they had immediate access to them, with proven, scalable applications and at a much lower cost than any other option.

Mayor's advisor
Daniel

Daniel understands the importance of software as a service for his municipality. Without it, he would not be able to provide the digital services he offers to citizens—on the one hand, because he does not have the technical capacity to do so and, on the other hand, it would not be feasible for him to do so, even if he had the money and capabilities to do so. For example, it would hardly be able to implement an electronic identification and signature system if this country service did not exist, or it would not be able to interoperate with the rest of the country.



EXAMPLES

Click on each flag or icon to go deeper.

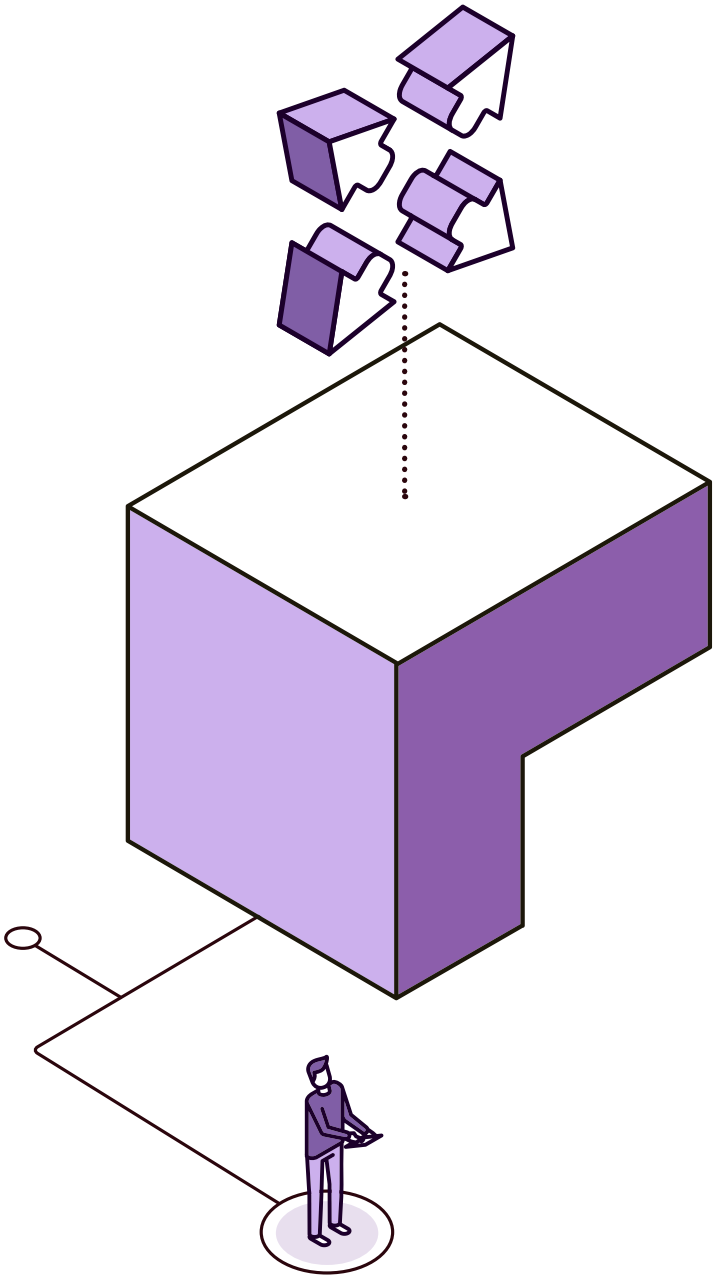
Spain

Catalog of cloud services

INDICATORS

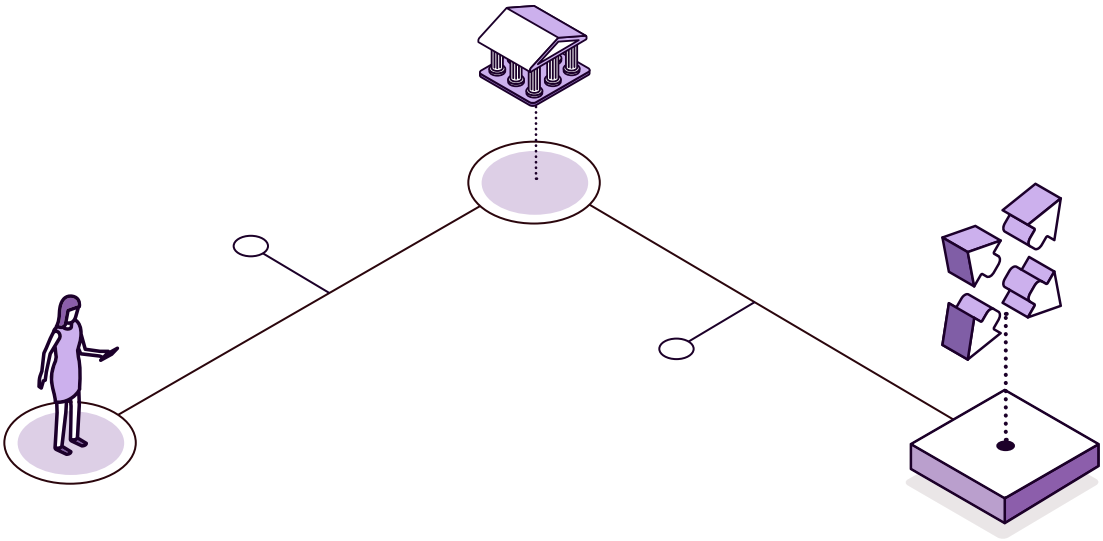
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Does software as a service exist from any government agency? If so:
  - Is it integrated with the digital identity and signature?
  - Do more than half of the central government institutions use *software* as a service?
- Is there a software-as-a-service catalog?



4.2

Interoperability



In many governments, the manual exchange of information represents the following:

- One of the main activities of many public officials
- A major cost center
- A cause of delays
- A source of errors and confusion
- Ultimately, a root cause of inefficiency and ineffectiveness

Digital transformation offers solutions to these problems through a series of tools that standardize, regulate, and automate the exchange of information of all kinds: data, documents, and entire files. This standardized, regulated, and sometimes automated exchange of information by technological means is what is known as interoperability.

It is precisely here where the technical regulations relating to electronic files, electronic documents, and so on become particularly relevant, because they are the path to success on the road to interoperability. The semantic definition of the structures of administrative information is what will really allow this kind of data to be successfully exchanged between organizations.

THE FOUR LEVELS OF INTEROPERABILITY[35]

As mentioned in the interoperability section of the regulatory framework, it is absolutely necessary for interoperability to be worked on at four levels: legal, organizational, semantic, and technical. It would be impossible for organizations to manage the generation of point-to-point connections individually without standards and definitions for the exchange of information. A "tower of Babel" would be built little by little, which would become unmanageable in the medium term, from the point of view of maintenance and evolution, in addition to the inefficiencies that could be generated.

- **Legal:** Ensures that organizations operating under different legal frameworks do not have impediments to interoperate (e.g., restrictions on the use or storage of data, obligation to use specific technologies, and conflicting requirements for similar business processes). This is particularly relevant in the case of cross-border interoperability, as it exists in the European Union.

- **Organizational:** Aligns and documents in a common way the business processes, including the information potentially exchanged between organizations, to visualize the role of this information in the negotiations between the entities participating in the interoperability and to clarify the relationships between service providers and consumers.

- **Semantics:** Ensures that the format and meaning of the information exchanged are uniform throughout the interoperability system. Key tools for achieving semantic interoperability include controlled vocabularies, code lists, and standard data structures.

- **Technical:** Covers the applications and infrastructures that connect systems and services, including interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols.

Precisely to solve the potential problem of the proliferation of a multitude of bilateral and nonstandardized connections, a technical regulation of electronic administration is generated, as described in the section on cross-cutting technical regulations of the regulatory framework. Regulations regarding electronic files, electronic documents, exchange of records, and notifications, among other aspects, will ensure the creation of a successful ecosystem of standardized interoperability, with transparent and simple management rules for all organizations. Thus, publishing or consuming information should become a simple procedure that virtually any agency can perform.

35. Based on the European Interoperability Framework. See https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

THE CENTRAL PLATFORM AS THE BASIS FOR INTEROPERABILITY

An interoperability system can help generate an ecosystem of exchanges that eliminates inefficiencies in a country. Entities are connected to a central platform, through which they can consult the information of other entities that are also connected to it. Normally, in this area, the leading entity of the digital transformation of each country should be responsible for the following:

- Starting up the main interoperability node to be able to start generating connections from there.

- Generating the first versions of the platform's information exchange protocol, based on the cross-cutting technical standards that have been approved. Usually, these first versions of the exchange standard are discussed and finally agreed upon by the governance technical working groups, since it is very common for different organizations to have different needs when it comes to resolving information exchanges.

TYPES OF INFORMATION EXCHANGE

- **Synchronous:** In the same process as the request, the request is resolved, and the transferring agency returns the data and information requested in the request.

- **Asynchronous push:** The requestor launches the exchange request and does not wait for any response. In the request process, he has indicated the way to send the information, usually a URL, and when the information is ready, the sender sends it to him in an automated way.

- **Asynchronous pull:** In this case it is the requester who recurrently "asks" the interoperability platform for the response to a request to be ready. When it is ready, it withdraws the information it was waiting for and terminates the exchange. Normally, the approximate waiting times for queries, as well as the intervals, are established by the sender of the information, in order to avoid unnecessary saturation of the services.

Of course, the combinations of these types, as well as what is the responsibility of the interconnected nodes or the centralized platform, is manifold, and will be architectural decisions of each implementation.

- *Example:* It may be decided that the service that handles information result queries in asynchronous schemes will be handled by the central platform or by each issuer. This will depend exclusively on the architecture and implementation decisions of each state.

OTHER INTEROPERABILITY PLATFORM FUNCTIONALITIES

In addition to the information exchanges themselves, the interoperability platform should be responsible for some other functionalities, such as the following:

- **Security and access control:** The platform must guarantee an adequate level of secure connections to ensure that information exchanges are carried out properly.
- **Traceability:** The platform is responsible for keeping a log of connections and exchanges made, mainly for auditing purposes and also for possible resolution of security incidents.
- **Monitoring and statistics:** Not only technical, but also functional. Data mining and analysis can definitely help to improve the platform's performance, as well as to identify possible new types of exchanges.

IN A BROAD SENSE, THE NATIONAL INTEROPERABILITY SYSTEM IS COMPOSED OF ALL SYSTEMS THAT ALLOW THE EXCHANGE OF INFORMATION IN A SECURE AND TRACEABLE MANNER FOR ADMINISTRATIVE MANAGEMENT WHEN NECESSARY.

It should be noted that the national interoperability system is a key element in achieving automated or proactive processing, so it is important to define it in a way that favors these types of processing. Of course, this system should be used to exchange any type of data, documents, or files between institutions.

SOME NECESSARY DISTINCTIONS WITH RESPECT TO INTEROPERABILITY

- **It is not the same as the open data system; often it is just the opposite:** Through the interoperability system, data are exchanged within the public administration that, by their nature, cannot be open, but are nonetheless necessary to facilitate procedures for citizens and businesses, and to enable the government's internal administrative processes.

- **Interoperating does not mean integrating information:** When interoperating, databases and information do not move from the entity where they are, citizen profiles are not created, and information is not integrated. If in order for entity A to access the data of another entity B a common database is created, we are not talking about interoperability, but about data integration, which is a separate issue.[36] On the other hand, interoperability can be understood as a system of specific queries, which maintains the data at all times in the body that must keep them; there is no creation of centralized databases. The consultation of information is specific; for a given procedure or action, this is traceable; and the privacy of the citizen is ensured.

Following the general line of implementation in the different countries, this section focuses on the system of interoperability of data, documents, and files that institutions exchange when they are in information systems oriented, in general, to limited data or data sets (such as "social security number," "birth certificate," or "criminal record information"). These usually have a common and defined structure (all certificates or data sets have the same fields, for example) and it is normal that they can be generated automatically (through queries to information systems).

Regulations increasingly state that public entities cannot ask citizens for documents that are already in the possession of these bodies or are generated by them, which means that one institution has to request the documents in question from another, and the latter must provide them. To solve this problem when data is not open, it is necessary to integrate the information in common databases that are accessible to several agencies, or to be able to interoperate between the different entities to obtain them.

Thus, in short, the interoperability system resolves the issue of exchange, not integration: it is a matter of an entity A being able to access the data that an entity B needs and has (note that "has" is indicated, not "generates") in order to carry out a procedure X for a citizen C.

BILATERAL RELATIONSHIPS VS. THE ADVANTAGE OF AN INTEROPERABILITY NODE

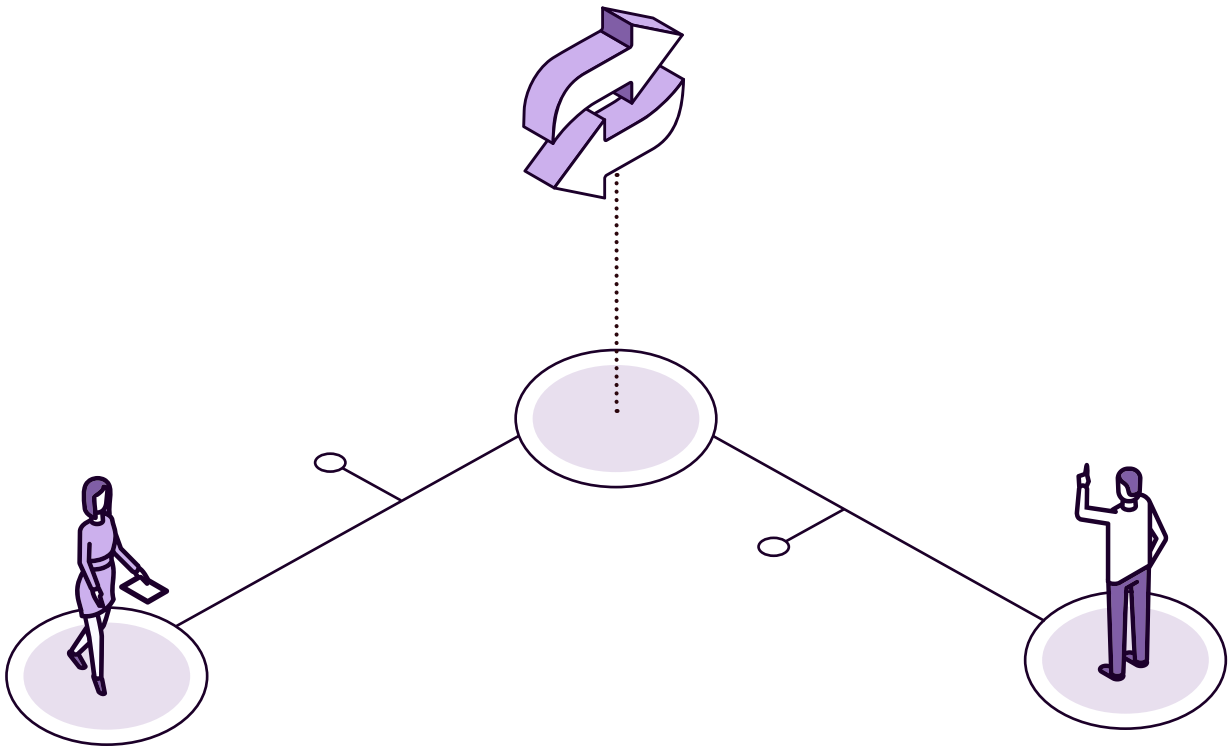
As data exchange is a real general need, many institutions have entered into bilateral agreements and exchange data of the same type between them, but this is not a system of interoperability, nor is it sustainable. Bilateral relationships and the specific API (*application program interface*) mean that as the number of actors increases, the complexity of the system increases: if there are two actors,

36. Care must be taken with the moral, competency, and data protection implications of integrating information, as this can create profiles of citizens and can be very dangerous in terms of civil rights or privacy. It should be emphasized that if you want to have a centralized database, integrating information from multiple sources, this does not have to be done through an interoperability system. In fact, interoperability systems guarantee citizens' rights in terms of data protection and privacy.

only one bilateral relationship is needed, but if there are 10, then 90 relationships are needed for all to relate to all; if there are 100, 990 relationships; and so on.

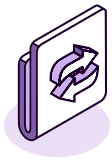
With interoperability systems, only one relationship between the agency and the interoperability node is needed: if there are one hundred agencies, there are one hundred connections between them and the node. Moreover, under this scheme, if agency X has to change its interface (e.g., due to technological change), the rest of the entities do not have to apply this change, but only the agency-interoperability node relationship is adjusted. In contrast, when the relationships are bilateral, the change of one of the one hundred ecosystem actors implies that the other ninety-nine have to adapt their interfaces, when they may lack the financial resources or capabilities to do so at that time, and then in some cases the information exchange may cease to function. Thus, the bilateral system without an interoperability node is not sustainable.

The bilateral approach can be taken by large entities for large volumes, but even in this case they would benefit from a country interoperability system. This avoids specific developments and systems and allows efficient management of data exchange between institutions.



THE TECHNOLOGICAL CHALLENGES OF INFORMATION EXCHANGE

It should be pointed out that the interoperability system has certain complexities that must be taken into account and that are not obvious in principle in order to solve a simple problem: the exchange of information. In this regard, the following stand out:



The exchange of electronic administrative records

Automated processing and metadata management

The volume of information

Signature systems for large documents

The exchange of electronic administrative records

This will be necessary as long as there is an ecosystem in which public administrations operate through an interoperable electronic file. This state and situation is more advanced than the exchange of general documentation and is very much oriented toward automated processing and through a metadata file. For the proper functioning of a complex electronic file exchange system—understood as the set of documents that make up a procedure, which can range from dozens to thousands, all of them metadata and with information that allows their automatic management—it is necessary to have this type of standardization for the management of information in the country, or at least in all public entities.

If there is no electronic record model, or if it only exists internally within an agency, or if records are handled bilaterally, there is no point in creating a general system that allows electronic records to be exchanged between any public entities (and the private sector). However, once this is stan-

dardized, having a system that allows exchange without losing the structure, metadata, etc., and then the file is even automatically processed by the recipient, is a common service of great value to the country.

In general, the regulated administrative procedure generates specific files, in which all related information is integrated, such as the following:

- A citizen's initial request
- Your entry record
- The requirement
- The response to the injunction
- Supporting documentation
- The certificates or data, probably collected through the brokerage platform or the documentation exchange system, and incorporated into the file
- Internal reports generated
- Resolutions, notifications, and a possible long etc.

All of them together form the electronic file, which sometimes needs to be exchanged between public entities and, in any case, made available to the citizen. The complexity in this state makes the usual documentation exchange systems useless (for example, a file can have up to hundreds of thousands of documents, all related), and the maximum benefits can be obtained when exploiting the file and document metadata model, which enables automated processing.

- *Example:*

1. A court requests a procurement file from an entity.
2. If a file exchange system is available, the entity will send the document electronically, in a secure manner, obtaining confirmation of arrival, all by electronic means.
3. The court will include the administrative procurement file in the court file as evidence.

4. If the court is only interested in checking the notification of the award, it will navigate through the document tree and directly select—or even the target information system will automatically process—the date of the award.

Automated processing and metadata management

It is essential that none of the file metadata is lost when the file is exchanged. Similarly, it is essential to ensure the flexibility of the system (e.g., only a certain subset of documents in the file may be of interest; therefore, the system should allow for such transfers), while maintaining the integrity and security that certain documents are indeed those that belong to the file in question.

The volume of information

Complex electronic files can contain tens of thousands of documents, some of them of significant size. This is why it is common to have to have systems that allow document management as a reference; in other words, it is like putting a link to a cloud storage repository, instead of sending the document by mail. This is due to the technological difficulty of transmitting large documents through conventional systems, something that can be solved by providing the reference to the document for download through a system specifically designed for managing large files. When this is done, especially in the public sector, document repository systems can be created that are secure, are capable of storing documentation indefinitely, and have a commitment to availability at all times.

This option is useful in the case of public entities or private repositories recognized by them, which have to comply with well-defined rules. Thus, the document is not transmitted as such, it is not held at the destination; what is obtained is only a link with which the document can be accessed, but it is not stored in the information system. This favors data or single document policies (“only once”) and prevents all administrations from having to make copies of the documents that make up a file, since they do not store it in duplicate, but only keep the reference to a trusted repository.

Signature systems for large documents

Traditional electronic signature systems usually have to store documents in their memory. However, if the documents are very large, or the equipment is large, or the system fails, specific electronic signature systems are needed. This is also true for referenced documents: it is necessary to have a system that can process the signature (and often recognize its validity and data before accessing the document), all in an interoperable way, with all institutions (and the private sector) using the same standard, which must have the requirement of being able to be managed automatically.

In this case of file exchange, the interoperability platform works as an orchestrator model, without the documents and files all physically passing through the central system, since, as the volume to be exchanged is so large, direct exchange is usually more effective than triangular exchange, always through a central point that can collapse. Moreover, intermediation platforms (called interoperability platforms in some countries) are not oriented to the exchange of any document. Of course, if the intermediation platform supports it, it is possible to take advantage of this function, but in general a generic system for secure information exchange is needed, for unstructured documents, between any public agency.

Public entities, when working with data, documents, and information, need them to perform their work, but such inputs are not always generated within the entity and are not always available through the platform. Similarly, some communications or issues go beyond the scope of the platform.

- *Example:* An institution has to send an official invitation to a manager of another unit for an event, or a regulatory body has to send an audit report. These types of exchanges are not usually included in the interoperability platform, but they tend to be very frequent. Therefore, in a digital administration environment, where there is no paper movement at all, there needs to be an information system that allows any document, even a scanned one, to be exchanged with any institution. Since it is an official exchange, this information system must comply with the corresponding security and traceability measures so that the status of the document sent is known at all times, given that the information being transmitted is being sent through it, and an official certification of the arrival at the destination must also be issued.

In these environments, the transaction and traceability, as well as the certifications of system events (arrival at destination, rejection at destination, forwarding), must have the necessary legal validity of an administrative procedure. This implies that the material must contain a digital signature and that the person responsible for confirming receipt, rejection, or forwarding must be identified (digital identification).

Note that it is not indicated that the exchange of documents as such has to be done from the centralized node, nor that they have to pass through it; in fact, one option may be that the central node orchestrates the system, but that the exchange as such is done between the origin and destination directly. Here there is a substantial difference with the general interoperability platform, since this one is oriented to data or certificates, and these are generally of a very limited size, hundreds of kilobytes, while in this other case a work project or the complete video of the recording of a trial, for example, can be exchanged. This means that if everything has to go through a central node, the system is heavily dependent on it and has to be very scalable. Exchanging documents directly between source and destination also favors privacy or confidentiality, but in return the orchestration of the system becomes more complex, because traceability and reliability of the exchanges are essential. In any case, it is important, as far as possible, to ensure the general encryption of communications and documents.

The system must work automatically, so it must have the necessary interfaces so that the information and document management systems of the different entities connect to it automatically. However, as this generally cannot be taken for granted (especially for small institutions, where the implementation of general automation is complicated), there should be a web interface, a cloud service, so that those who lack a strong infrastructure and ICT capabilities have access to the system, since a key to its success is to eliminate paper-based exchange in each and every public entity.

COMMON SERVICE MODEL

As already mentioned, the bilateral model is not scalable (if one thousand institutions have to relate to each other, there would be a million bilateral relationships), so it is advisable to implement a common service model, where interoperability management is performed once and that all entities can reuse. To this end, at least the following elements will have to be considered:

- **Transversal technical normative definition of**
  - How the country's interoperability works.
  - How an entity is enabled to interoperate with others.

- How an entity can consume data.
- What is the legal instrument covering such consumption or relationship;
- What are the obligations to be fulfilled, etc.

- **Data governance and system certificates.** A system must be in place to match demand and supply.
  - *Example:* If A needs a piece of data from B, the latter will not have to carry out manual processes to provide it. Therefore, it will be necessary to negotiate so that A asks B for a reasonable piece of information, and so that B can provide A with a useful piece of information.

This is particularly relevant when the data are of the same type but are provided by different entities. Therefore, the quality of the data that entities make available to others to interoperate must be guaranteed, as well as the quality of their technical infrastructure, to ensure that the service they provide is optimal and, for example, they can interoperate 24-7 delivering quality data. This is why, in some countries, the digital transformation lead entity, in collaboration with a working group (data governance committee), defines the conditions and certifies that, for example, entity B is a "secure data source" for certain specific data.

- **Interoperability platform:** Whether through a service bus, web services, REST API, or any other technology, the important thing is that there is an information system that allows the exchange of data, certificates, or documents from A to B in a common way, so that public institutions do not have to set up systems bilaterally.

- **Centralized traceability system:** Regardless of the previous model (it can even be distributed among nodes), it is essential to have a centralized traceability system, in which the only data stored is the entity that requests it, the entity that offers it, for which procedure or file of said procedure, by which official or information system the data is requested, and on what date and time. Apart from having to store this information in case it is needed in the event of possible future conflicts, it is interesting to make it public for the citizen through the single point of access system, so that he can see all the exchanges of his information that are being carried out by public entities and, if any transaction does not match a legitimate exchange, he can complain to the body responsible for controlling the protection of citizens' data.

- **Definition of system tasks:** It is essential to know whether the interoperability system exchanges data, files (which can be videos, graphics, text files, etc.), or both.

- **Ability to exchange data with metadata.** Independently of what is stated in the previous section, there must be the possibility of exchanging data with metadata, so as to allow automatic and proactive processing. The objective is that when the information that is exchanged reaches the destination agency, it does not have to be read or processed manually but can be processed by a computer that automatically makes decisions based on what is reported.

SUGGESTED PREREQUISITES FOR INTEROPERABILITY

Like most information systems, interoperability systems can operate in isolation, but they are greatly enhanced if there are certain common services or elements that appear in this framework. Ideally, these elements should be preexisting in order to make the interoperability system as efficient as possible. Some of the most relevant ones are highlighted:

- **Directory of public entities and companies:** Interoperability is based on the fact that a unit A requests sensitive information from a unit B within the scope of data protection, and that it is not public. Therefore, it is important to have the A and B units univocally identified, determined, without any doubt, to avoid uncontrolled access and information leaks. In this sense, there must be a common directory, with the units with unique, updated codes, which consumes the interoperability platform, to facilitate the exchange of information.

- **Procedure catalog:** To ensure traceability, and to ensure that it is always possible to know for what purpose a piece of data has been requested or transferred, it is advisable to indicate the procedure for which it is requested. The existence of a register of procedures, with a unique code that is always updated, is the best way to identify the purpose for which data is being requested. Moreover, the catalog of procedures can be the key to authorize or not a query allowed on the platform. Thus, if a code, a regulation, and a process where the required data are defined appear in the record of the procedure, the interoperability platform consults this record and sees if the consultation of the data is legal or enabled for a given procedure, which makes the management of authorizations and data protection much simpler.

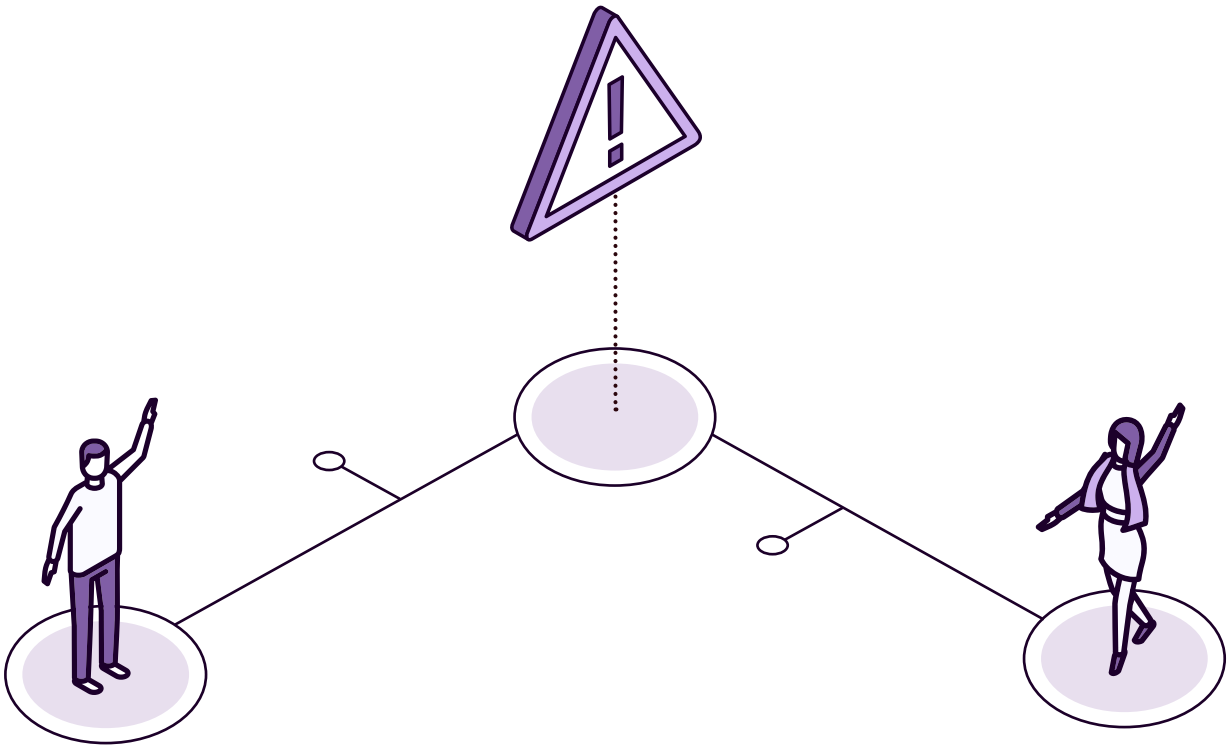
- **Data exchange register:** For the sake of transparency, and to avoid possible unauthorized queries, it is very efficient to publish any data exchange of a citizen through the interoperability platform in the citizen folder. In this way, the citizen can easily check, through the platform, which entities have consumed his data and, if necessary, detect any irregularities.

- **Registration of officials:** Although the interoperability platform is especially oriented to automated processing, so that the information systems consult the data they need when carrying out the administrative procedure, it is common for there to also be manual access for

authorized officials to access the information on the platform. The existence of a register of officials with their respective access profiles greatly facilitates the management of access to the platform. In this way, there is no need to create a database of officials with access, which runs the risk of becoming outdated.

- **Tailored data demand and supply:** Both the forums with the private sector (if it is good practice that they can access the platform's data with the appropriate controls) and the committees or working groups of the different public entities are essential to detect what data is needed, who has it and should introduce it into the platform, and standardize the data models to be included in it.

- **Cybersecurity and emergency and early response operations center:** These spaces are especially necessary for this type of information system, due to the multiple accesses that take place from different entities and because of the privacy of citizens' data.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo is going to build a new house and is overwhelmed by the paperwork to get the license from the municipality. He does not understand how he is asked for so many documents and certificates, for which he has to go many times to different public offices. If his municipality could obtain this information directly, not only would he save himself a lot of time, but so would the various entities that have to issue and receive the certificates.

Mayor's advisor
Daniel

Daniel does his business in his town hall, and, as it is small, he still does it on paper. He would love for someone to provide him with a system like that of the large public entities in which he has acquaintances, who tell him that they do not have to ask the citizen for the information; they consult it directly through the intermediary system.

Entrepreneur
Ana

Ana works for a large microchip company and wants to open two new factories. It is a problem for her to manage the building permits with the public authorities. As they have numerous documents, many of them huge, she has no choice but to print and move sometimes dozens of boxes of documentation between the different entities that are responsible for carrying out authorizations to carry out a work of that magnitude.

Vice minister of health
Sara

Sara sends other public entities the documentation they need by email, but she has always doubted the effectiveness of the system. When she sends an email to a person, it can happen that they are on vacation and do not receive the information in time. In this case, he has no confirmation that the information has arrived and is correct. You would like to have a secure information exchange system, which also leaves traceability of the status of transactions.

EXAMPLES

Click on each flag or icon to go deeper.

Uruguay
Digital Proceeding

Spain
Catalog of data and services.

Estonia
Interoperability services

Spain
Infrastructure and systems of Electronic Documentation.

European Union
European Interoperability Framework

Uruguay
Interoperability Platform

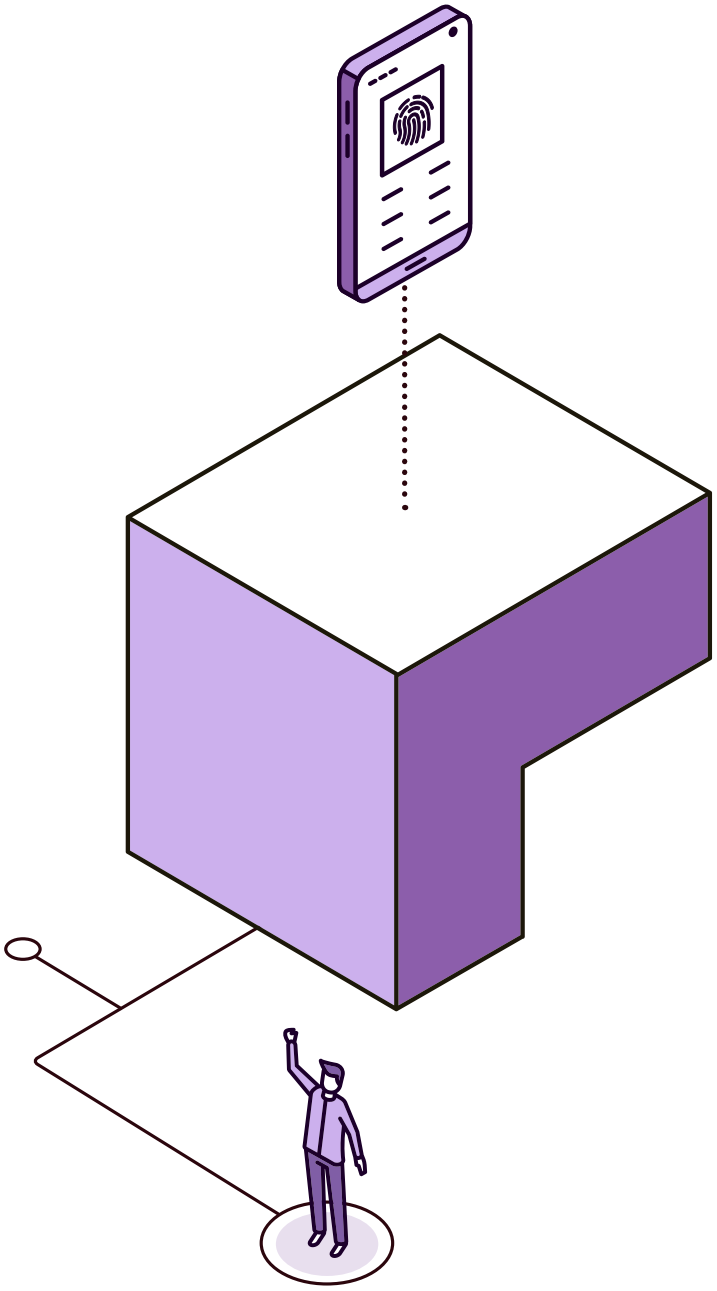
Brazil
Electronic Information System (SEI)

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

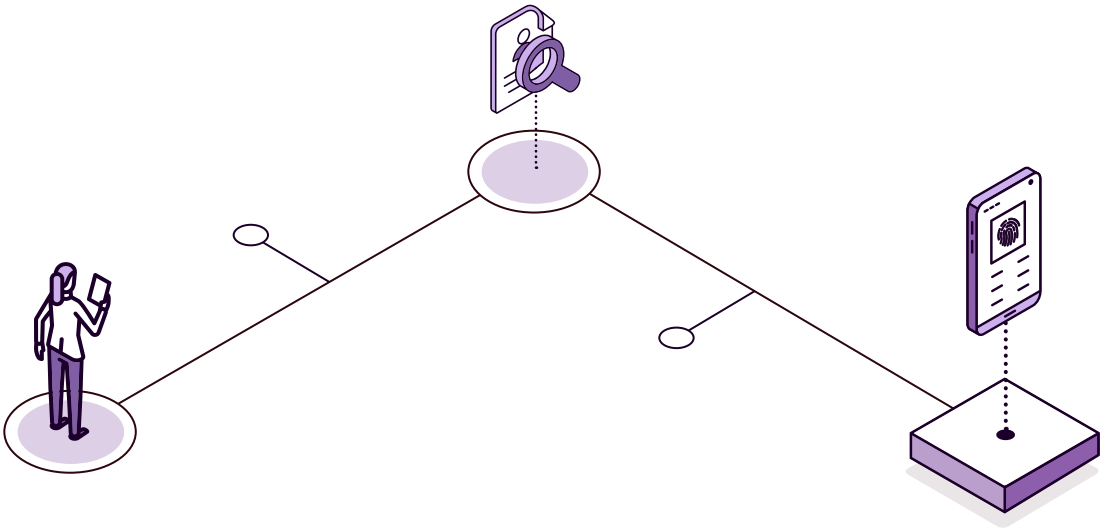
- Is there a national interoperability system?
- Is there a governance scheme for the national interoperability system?
    - The governance framework refers to decisions on the interoperability framework, institutional arrangements, organizational structures, roles and responsibilities, policies, agreements, and other aspects to ensure and monitor interoperability in the national context.
- Are more than half of the public entities of the central government integrated into the interoperability system?
- Is there an electronic file exchange system?
- Are more than half of the public entities of the central government integrated into the electronic file system?
- Are all public entities of the central government integrated into the interoperability system?
- Are more than half of the municipalities integrated into the interoperability system?
- Are all municipalities integrated into the interoperability system?
- Is the judicial branch integrated into the interoperability system?
- Is there a data catalog of the nation?
- Does the interoperability system exchange documents?
- Does the interoperability system exchange data?

- If yes, are these data standardized to allow automatic processing?
- Are the following types of data and certificates integrated in the system?
  - Personal and basic identification data:
    - Digital identity
    - Address
    - Date of birth, marriage, and death (civil registry data)
  - Economic, financial, and tax data
  - Employment data
  - Health data
  - In general, data from other areas and competencies of the national government.
- Is the use of the interoperability platform in the central government widespread? With few exceptions, is no data requested from the citizen that the government already possesses?
- Is the use of the interoperability platform at all levels of government, including municipalities, widespread? With few exceptions, is no data requested from the citizen that the government already possesses?
- Are data from the interoperability platform in some cases processed automatically?
- Is the data from the interoperability platform processed automatically in most cases?
- Is the interoperability platform bidirectional? That is, agency A requests a piece of data and gets it from agency B, and agency B produces a piece of data and proactively sends it to agency A.



4.3

Digital identity



When performing acts before public entities, it is necessary for the citizen to identify himself in order to know that it is really him and that he can act in relation to a given procedure, as it happens in the analog or paper context. As in the paper world, businesses often require proof of identity to complete a transaction. For agreements between individuals with legal validity it is the same: identity must be verified. As a consequence, in the digital world, systems must be in place that allow a citizen to identify himself/herself by non-face-to-face means (web, applications, cell phone, etc.). Thus, technological tools that facilitate identification are necessary, as well as a legal framework that allows citizens, companies, and entities to operate with clear and stable legal criteria.

ID IS NOT ONLY A MUST-HAVE TOOL FOR DIGITAL GOVERNMENT, BUT ALSO FOR THE DIGITAL TRANSFORMATION OF THE COUNTRY, AS IT SERVES PURPOSES THAT EXTEND BEYOND GOVERNMENT.

Digital identity (ID) is the common service that allows any public institution—and, desirably, the private sector—to easily identify citizens in the digital environment in a unique, unequivocal, and universal way, at the national level, for all public and private purposes. This identification system may have different levels or forms of use, but it must in any case ensure the possibility of secure use from mobile devices, which are becoming increasingly widespread.

This component includes not only the common ID service as such (which includes its procedures for citizen registration, citizen service, information systems, etc.), but also the system that allows the citizen, once identified, to navigate from one environment to another using the *single sign* on modality—in other words, without being asked to log in again and again, which is particularly annoying. What is particularly important to bear in mind is that the protection of personal data must be taken into account.

Given the need for identification for any procedure, an electronic identification system is required in all cases. Therefore, a tool that provides a common identification service to all public entities, for all procedures, is especially necessary. If this is not done, each digitization process will require the creation of an *ad hoc* identification system, which will generate duplication and high costs, since it will be necessary to consider the identification of citizens and the supporting system hundreds or thousands of times.

REASONS TO HAVE A UNIQUE DIGITAL IDENTIFICATION SYSTEM FOR THE COUNTRY

- **The provision of digital public services**: As already mentioned, the need for digital identification is clear for any procedure. If the agency providing the services does not have to be responsible for developing the system, it can focus on the provision of the service itself, which will make it available more quickly, since the identification module already has it solved. This results in ease of maintenance and improved quality of service, among other things.

- **It makes it easier for all or almost all citizens to be registered in a single registry:** This implies benefits for a body which, however small it may be, would only have to deal with very specific procedures and would have a system that makes it possible to identify the group of citizens of interest to it for the procedure, since all citizens are registered in the general system.

- **Perception and citizen service:** People find it incomprehensible, chaotic, and complicated to have to have different users, passwords (each with its own specific rules), two-factor authentication systems, etc. for each procedure they have to deal with, whether public or private. On the contrary, what they would like is to have a digital ID, under their complete control, that can be used for any type of service, regardless of the provider. Note here that it is not specified that they are public service providers; this could also be useful (and would be desirable) in the private sector.

For all of the above reasons, a digital identification system is fundamental for the development of the country's digital transformation.

ID SYSTEM AS A LINK BETWEEN LEGAL AND DIGITAL IDENTIFICATION

With a view to digital identification, an important precondition, which goes beyond the field of digital transformation as such, is that the country has a foundational/legal identification system that makes it possible to identify each and every citizen unambiguously and unequivocally, assigning a unique code. Logically, this is much easier in those countries that have a trusted universal ID (provided by the civil registry, the police or the authority designated for this purpose in each country). In the case where this is not feasible, because such a universal country ID does not exist, the creation of the ID should include the principles and good practices of well-formed universal identities.

The ID system will be the one that links the foundational/legal identification with a citizen's use of digital media. In general, it would be interesting if, through international standardization and electronic signature possibilities, the national ID system could obtain the citizen's identity through electronic certificates that follow international standards. Therefore, the national identity system will allow, based on a certificate issued by any of the certification service providers authorized in the country (which may also be international, to facilitate cross-border processing), to extract the citizen's identification and code, check the validity of the certificate, and provide this information, together with the necessary metadata (apart from the code, name and surname, other data of interest in the certificate, security level, etc.) to the service provider so that it can identify the citizen with whom it is interacting by digital means.

It should be noted that digital certificates[37] have problems such as the following:.

- Cost
- Difficulty in being used by people without a good level of digital literacy
- Expiration
- Lack of adaptation for use on mobile devices or tablets.

37. A digital certificate or electronic certificate is a computer file electronically signed by a certification service provider, considered by other entities as an authority for this type of content, which links signature verification data to a signatory, so that only that signatory can sign, and this confirms the signatory's identity. In addition, it has a data structure containing information about the entity.

These drawbacks mean that the system must, or should, be supplemented with the following:

- Non-certificate-based identification. In this case, the choice is usually mobile phone-based identification via a chip, an operator, or the sending of a second authentication factor, in order to achieve high levels of security and temporary passwords. This is due to the fact that the cell phone is now widely used by the entire population, and, on the other hand, it provides higher levels of security than other systems.

- A basic general username and password system, with or without a second authentication factor (to email, for example).

In any case, the important thing is that the national digital identification system should have a very user-friendly system (usability must be a priority), even if a lower security category has to be created, valid for the vast majority of public entity procedures, but perhaps not for some particularly critical or sensitive ones.

KEY FACTORS FOR ID ADOPTION

- **Governance and management of the national ID system:** Apart from the IT system as such, governance is required to enable it to evolve and adapt to the needs of all public entities (including the national and all subnational levels). Otherwise, there is a risk that some of them will set up a parallel system, thus losing the advantages of the aforementioned single system.

- **Publicizing the system:** It is necessary to have a personal and office team to help people register and learn about the digital identification system. Ideally, all public entities should participate in this, in order to reach all citizens.

- **Taking advantage of already-established systems:** In the event that there is already a widely used identification system created by some organization (usually the tax collection or social services entity), the possibility of using it as a base and expanding it to become a general system for the nation should be considered, instead of implementing a new one and this organization having to stop using its own and switch to the new one (which can create tensions in that unit).

- **Telephone identification:** It would be interesting if the state's identification information system were also available through the telephone system. This is especially useful for some institutions, as well as necessary for a multichannel service strategy, since for some information services, and for almost all transactional procedures over the telephone, it is necessary to have the citizen identified in this way. In two-factor systems with mobile notification, this is relatively simple and security levels are maintained.

- *Example:*

1. The citizen identifies herself by typing her ID number.

2. A numerical code is sent to her cell phone, which she dials or says over the phone, and she is logged into the system with a secure ID.

   If there is no mobile backup system, it is also feasible to ask for the document number and expiration date, or other known information. This is not as reliable as the cell phone backup, but it is sufficient for many procedures.

SOME SYSTEMS THAT THE LEAD INSTITUTION SHOULD STUDY BEFORE UNDERTAKING ANY ID EFFORT

- FIDO: https://fidoalliance.org/
- SAML: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
- Shibboleth: https://www.shibboleth.net/
- OpenID: http://openid.net/
- OAUTH: https://oauth.net/2/
- Liberty Alliance: http://www.projectliberty.org/
- CardSpace: https://msdn.microsoft.com/en-us/library/aa480189.aspx
- Kantara: https://kantarainitiative.org/

For example, the European Union has chosen SAML as the basis for its own interoperability protocol, which gives states the freedom to define their own identity management model. What is relevant is that the identity model adopted allows nationals of one state or continent to carry out formalities in another.

INTERNATIONAL ID INTEROPERABILITY

It is often the case that each country, or sometimes even a community of nations, has a different method of identification. In order to create an interoperability network based on identification, the

lead institutions must pool standards that make cross-border communication possible, and to this end convergence or interoperability nodes must be defined. These are mainly software components and are responsible for carrying out cross-border authentication.

The architecture of these interoperability nodes is based on standards for easy communication and integration with the middleware of the member states that make up the network. The steps to carry out the deployment and support of the aforementioned architecture are as follows:

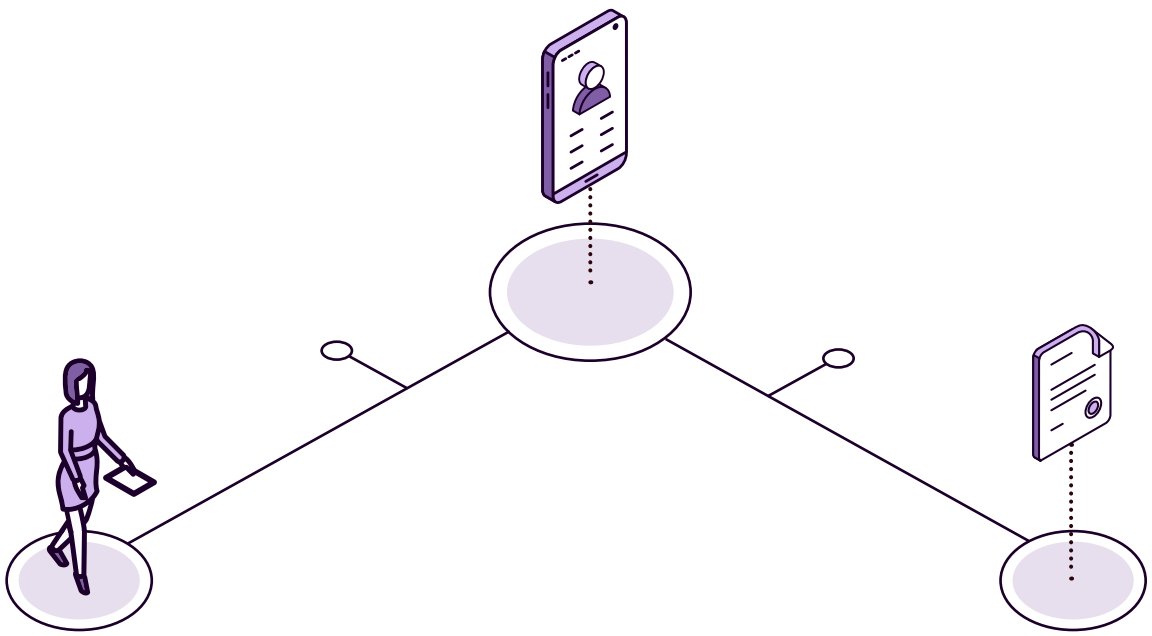
1. Definition of both syntactic and semantic interoperability standards, in addition to the communication protocol

2. Development and implementation of the relevant environments, including testing

3. Homologation of middleware systems based on established protocols and procedures (subnodes)

4. System certification

Whenever an adaptive or evolutionary maintenance occurs, an impact analysis should be carried out on the rest of the nodes or subnodes. In the area of collaboration, it is proposed that the lead institutions promote technology transfer between subnodes, so that solutions are reusable for other sectoral institutions and countries.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo tries to identify himself to an organization with which he only does one procedure a year, but he can't remember his username and password. What bothers him a lot is having to use a different ID with each public entity. Alicia, his sister, has a cryptographic electronic certificate because it is very useful for her work; however, no one else in the family has one, due to the complexity and cost involved. Alicia would like there to be an identification system in her country that would allow her brother to make transactions with public entities as easily as she does with her bank, which has a simple and reliable identification system. Every time she has to make an important transfer, she simply has to enter a password that is sent to her cell phone, which gives her a lot of confidence.

Mayor's advisor
Daniel

Daniel is the mayor's advisor and wants to put a municipal service on the internet, but he does not have the financial resources to install a system to identify citizens on the network, so unfortunately he has not been able to provide the service in a comfortable way to the inhabitants of the municipality for years. He would love to have a free identification service, and he alone would have to improve his service.

EXAMPLES

Click on each flag or icon to go deeper.

Uruguay
Digital Identification

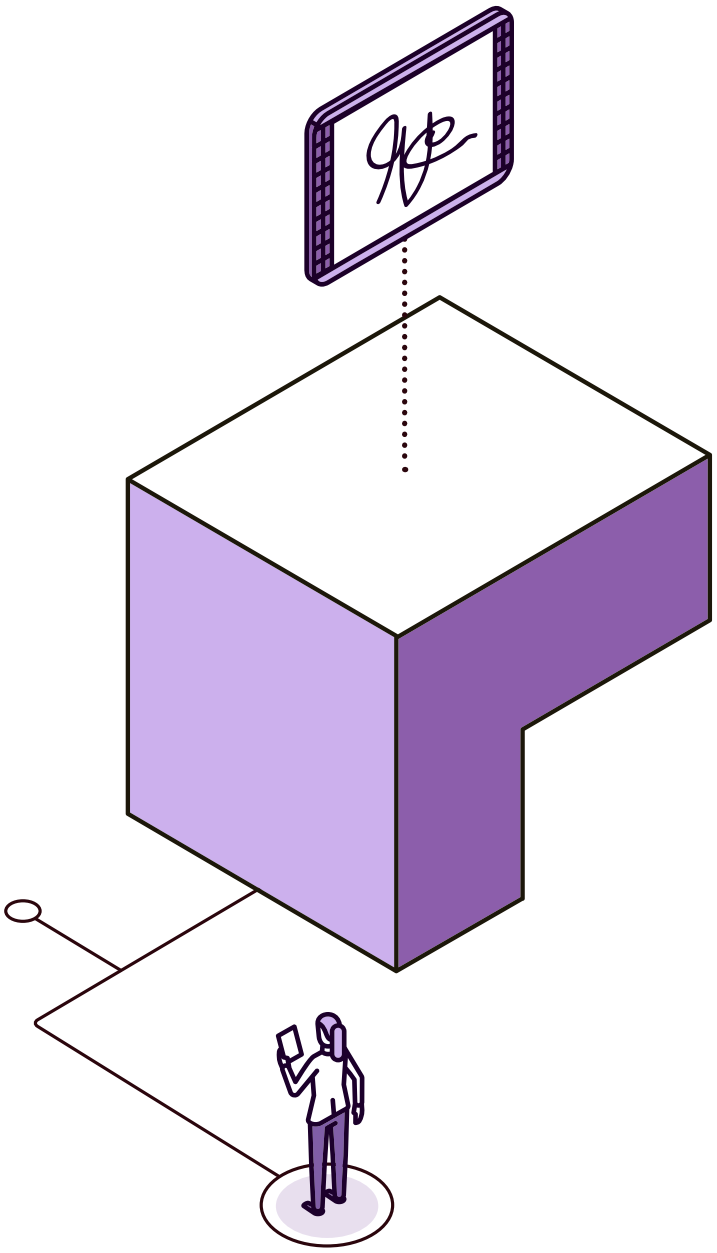
Chile
Authentication service

Spain
Electronic Identity for the Administration

INDICATORS

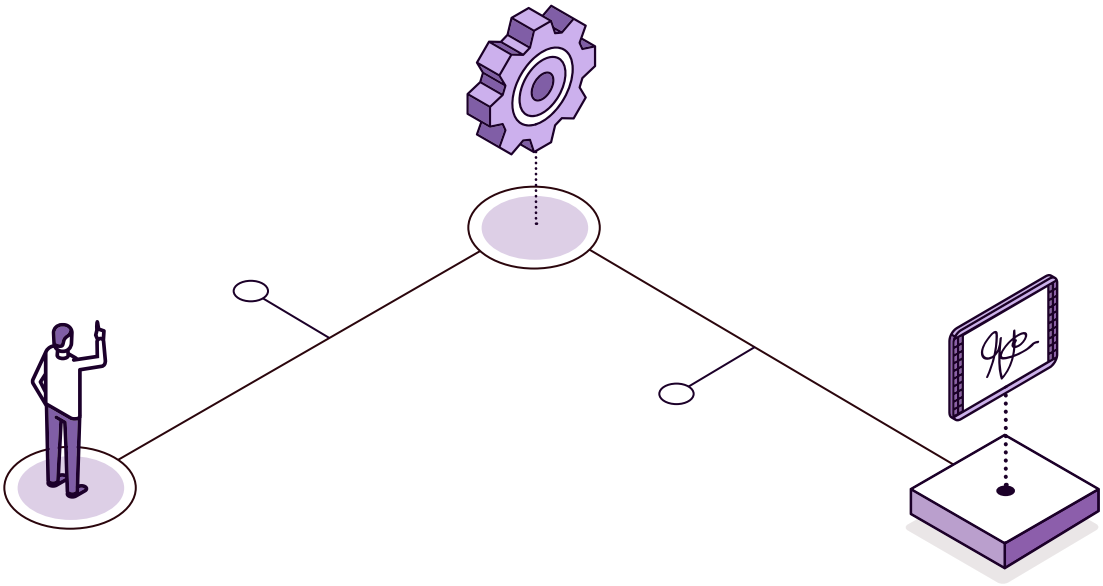
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a digital ID in the country? If so:
  - Is it unique (i.e., no two government entities issue digital IDs)?
  - Is it for universal use (i.e., for any identification purpose in the public or private sphere)?
  - Do you have the possibility of different levels of security to adapt to procedures of different levels of sensitivity?
  - Can it be accessed via cell phone?
  - Is there a possibility of telephone identification?
  - Is it mandatory to use it through a card reader or any other external device?
- Is a single key/single *sign on* system in place?



4.4

Digital signature



In the act of signing, a person accepts and validates the content of a message, and in the case of an electronic message, the signature is called electronic. From a technical point of view, the electronic signature and seal are formed by a cryptographic value resulting from a special mathematical operation between the private key held by the signatory and the result of a summary function applied to the document, together with the certificate containing the public key that allows the signature or seal to be verified. Frequently, it accompanies the document, and in the case of some document formats such as PDF, there are functionalities in the software that allow it to be displayed.

All organizations need the implementation of the signature, as well as the time-stamping systems that ensure and record the date and time when the will is expressed, in order to carry out their procedures. In short, the electronic signature is another of the modules that all institutions need, and it is therefore a particular priority to be part of the common services of the digital administration of any nation.

IT IS NECESSARY TO TAKE INTO ACCOUNT THE DIFFERENT SUBJECTS THAT CAN MAKE SIGNATURES: ON THE ONE HAND THERE WILL BE CITIZENS, INDIVIDUALS, BUT ON THE OTHER HAND IT IS NECESSARY TO CONSIDER THE SIGNATURE MADE BY COMPANIES AND PUBLIC ENTITIES.

CERTIFICATION SERVICE PROVIDERS

One of the most widespread and proven systems is the electronic signature based on cryptographic electronic certificates in the *public key infrastructure* (PKI). The first certificate-based signature scheme is called CBS (*certificate-based signature*), and its signature process requires the private key and the updated certificate, while the public key is needed for verification. In this type of system, the holder acquires the electronic certificate from the so-called certification service providers, which can range from the lead institution to private organizations.

The framework for the provision of certification services contemplates the existence of a supervisory body to which applications are submitted to initiate the qualified trust service. Associated with this body is the TSL trusted list publishing entity.

IN MANY STATES IT IS THE SUPERVISORY BODY ITSELF THAT PUBLISHES THE TSL TRUST LISTS.

Trusted service providers (TSPs) wishing to provide qualified services must pass an audit covering the services implemented. The qualified services of the eIDAS Regulation for Europe serve as an example (the technical standards used in their assessment are indicated in parentheses):

- Service for issuing qualified electronic signature certificates (EN 319 411-1 and EN 319 411-2)
- Service for issuing qualified electronic certificates of electronic seal (EN 319 411-1 and EN 319 411-2)
- Service for issuing qualified electronic certificates for website authentication (EN 319 411-1 and EN 319 411-2)
- Service for issuing qualified electronic time stamps (EN 319 421)
- Qualified electronic certified delivery service (EN 319 521)
- Qualified electronic signature validation service (TS 119 441)

- Qualified electronic seal validation service (TS 119 441)
- Qualified electronic signature preservation service (TS 119 511)
- Qualified electronic seal preservation service (TS 119 511).

In the European case, the PSCs must go through a three-stage approval process:

1. **Preparation:** The CSP designs, configures, implements, tests, and deploys in preproduction the qualified trust services it intends to provide, in accordance with the requirements set by legislation or the lead institution. In parallel, the CSP establishes the relevant documentation that will demonstrate its conformity with the requirements. A conformity assessment body assesses the conformity of the CSP and the qualified trust service it intends to provide with the requirements. The conformity assessment report must demonstrate conformity.

2. **Initial verification of compliance:** The so-called conformity assessment body (CAB) verifies whether or not the CSP and the qualified trust service it intends to provide meet the requirements of the regulation in order to be granted qualified status. It may rely on the information provided under the notification procedure, including the conformity assessment report, but it also has the right to request further information and may take a duly justified decision that goes against the conformity assessment report. After positive verification that the CSP and the qualified trust service it intends to offer meet the requirements, the CSP/trust service is granted qualified status and the body in charge of the national trusted list is informed for the purpose of updating the national trusted list.

3. **Publication of qualified status on the national trust list,** following notification that the PSC offers a qualified trust service.

In addition, biannually, the relevant documentation must be resubmitted for reapproval, by means of a technical report, corrective action plan for nonconformities (if any), insurance, etc.

INFORMATION AND TRUST SERVICE TOOLS REQUIRED IN THE USE OF DIGITAL SIGNATURE

In either case, the lead institution shall promote and/or make available to interested parties and agents easy and transparent access to the following:

Information system for the verification of credentials

Modules for agencies to manage, process, and validate electronic signatures

Programs or systems to make signing easier for citizens

Electronic signature system in the cloud

Time stamping systems

Electronic sealing systems or electronic signatures of legal entities

Accessible system for publishing and searching for a trusted service provider

Information system for the verification of credentials

› This is essential, because although cryptographic electronic certificates are relatively standardized in their technical aspects, the same is not true of their semantic aspects. Issues such as the way in which first and last names are encoded (In a single field? Two? Three? Four?), unique identifiers, or the type of certificates depend on each provider. On the other hand, if there are international agreements, you will not only work with certificates from your country, but from many others. This means that digital public service providers (a municipality, a ministry, etc.)

need an information system that acts as a centralizer and homogenizer: the so-called neutral point, which allows them to consult this system with a certificate, which can be any certificate, and always receive a homogeneous response. It is the neutral point that is responsible for standardizing the information, regardless of the type, country, and semantics of the certificate.

In case the neutral point does not exist, these are some solutions:

- Use a single PKI, which eliminates the market and forces the creation of a monopoly. In addition, there is no cross-border interoperability, since certificates from other countries, even if they follow the same technical standard, have different semantics (based on the language used, for example).

- Each entity, each public service, would have to check the validity with each issuer of electronic certificates, national and international, and independently process the response, which is not sustainable and requires advanced technical knowledge of digital signature. If there is no monopoly in the issuance of certificates in the country, the existence of a neutral point of validation of electronic signatures and certificates is usually a must. This information system will also have an interface for citizens in general, where they can check the validity of certificates and signatures issued by institutions, in addition to the system that allows confirming the validity to public entities.

Modules for agencies to manage, process, and validate electronic signatures

- Certificate-based signatures require libraries and modules to enable their processing, implementation, and management. Electronic signatures and their products require software to function. It does not make sense for each agency to develop, acquire, or have to incorporate these common modules independently, so it is a good practice to facilitate their use if these modules are provided free of charge to all public entities and are very easy to use. The idea is that they should have the necessary software and be able to integrate the electronic signature into the agency's information system at no cost and in a simple manner.

Programs or systems to make signing easier for citizens

- Just as agencies need programs to make electronic signatures on their devices, citizens need programs to speed them up. Therefore, there should be an information system, unique to the state, that citizens can install on any type of device (including cell phones) to make electronic

signatures easily. Ideally, this same *software* would be valid both for citizens in general and for specific groups, such as civil servants, lawyers, businessmen, etc. In some countries, by regulation or sectoral interest, the electronic signature of lawyers is provided by the bar association; that of doctors, by the medical association; business organizations provide electronic signatures to companies, etc. Although electronic signature systems are varied, it is important that the *software* that processes them is common or compatible.

Electronic signature system in the cloud

- Given the inherent complexity of certificate-based electronic signature systems, it is common to try to reduce their use for citizens. With electronic signature systems in the cloud, this problem is solved, since the citizen does not have to sign in on his device, but the signature is made precisely in a system in the cloud. It happens that, according to traditional systems, the citizen has to install a signature *software* on his device, which is the one that allows him to perform the cryptographic process of signing a document. In cloud systems, to avoid the need for this *software* (and its technical complexity in relation to installation and use), the document is uploaded to the information system, which performs the signature in the cloud and then makes the document available to the user with his signature to download or send it to the next user who needs it.

However, it is important to note that these information systems reduce the complexity of use and the elements involved for the citizen but increase the burden for the agencies or service providers, since not only two information systems are involved (the user's and the service provider's), but a new one (a signature system in the cloud) is added and must be triangulated with the first two. Therefore, it is important that instead of each provider setting up its own system or processing mode, which increases complexity exponentially, this is done in a centralized manner, as a shared service that is valid for all.

Time stamping systems

- These are important when it is necessary to attest when the different acts that are signed or performed take place. They are also essential to provide security to long-lived signatures or to perform time extensions in digital signatures, since the expiration of these is one of the great challenges of PKI-based systems. It happens that digital certificates (and their associated signatures), as well as root certificates, expire; they have a certain time of life, which means that after that period, the signature made is marked as an invalid signature due to the expiration of

the certificate. Solving this problem of signature expiration and knowing reliably from a trusted third party when a transaction has been carried out are common needs in a large number of public entities. Ideally, a common service should be available to all of them, without having to create a different one for each one.

Electronic sealing systems or electronic signatures of legal entities

- The signature regulation or policy may or may not allow electronic signatures of legal entities as such (not through a representative), but in any case it is usually of interest to have a special type of electronic certificate that is associated with legal entities. This not only facilitates the electronic signature of companies and institutions; it is also useful for mass processes and signatures, and for providing features such as integrity and security to certificates and documents not signed by legal persons.

Accessible system for publishing and searching for a trusted service provider

- The lead institution should encourage the creation and ongoing maintenance of a centralized system to facilitate the publication of the list of CSPs. This list should break down the different providers that have achieved a certain qualification and the services for which they are qualified.

The systems of electronic signatures based on certificates are complex, as well as having a high cost associated with their creation and maintenance. It is therefore necessary to think of parallel systems. In general, these are based on associating certain data to the citizen's identification, forming a package of information that makes up the signature. In order to ensure the veracity of the signed document, its long-term integrity and inviolability, the interoperability of the information, and other characteristics that cryptographic electronic certificates have by definition, an electronic seal or signature of the competent body can be applied to the information package of the signature.

Regardless of the solutions that the market establishes through private entities, the lead institution should encourage the sharing of a technology transfer center for this type of tools among the sectoral institutions. This will result in

- Standardization
- Improvement in the quality of services.
- Reduced costs in both construction and maintenance.

Finally, it is interesting to note the possibility of making the signature through the telephone system. For this, if the system is prepared for use over the internet, the transition to the telephone signature is not complex and is also standardized. This can be achieved with secure telephone identification systems (e.g., ID card number, some ID card information or password of the citizen, and a cell phone backup). The automatic voice recognition system packages all this information and applies a traditional electronic signature to it, so that the complete package of information has the character of a signature and can be used as evidence.

SOME IMPORTANT EFFECTS OF THE SIGNATURE

ALTHOUGH IT IS A NECESSARY CONDITION, A NORMATIVE REGULATION, SUCH AS THE ELECTRONIC SIGNATURE POLICY, IS NOT ESSENTIAL.

- The country's electronic document and record system requires a signature to ensure integrity, nonrepudiation, the relationship between the document and the signatory, long-term preservation, etc. Electronic documents and records are the foundation of e-government and digital government; therefore, the signature is a fundamental component of digital government.

- The entire information exchange system (data, documents, files) requires electronic signatures, so the standards on which they are based must be known in order to promote interoperability and, ultimately, digital government.

- The digital signature is one of the fundamental building blocks of digital government, so it has a minimum of requirements and a multiplicity of potential uses. It is essential to have a regulatory framework that makes digital signatures viable. However, it is not necessary to wait for the regulatory framework to develop the technological tool that allows the use of electronic signatures based on certificates, for example, following international standards and operation. It is also possible to set up the digital signature ecosystem and use it on a voluntary basis or restricted to certain types of procedures, while the general regulation of electronic signatures in the country is being generated.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo has to sign a document at home and is unable to install and configure the *software* to do so. He does not understand how he already has three electronic signature components on his computer, and, now that he is going to sign at another entity, he is forced to install a fourth one. It would all be so much easier if there were a single national electronic signature system that did not require downloading any *software* and was very easy for a citizen to use.

Vice minister of health
Sara

Sara wants to take advantage of the fact that her citizens regularly use cell phone messaging to offer them services in this way. However, she has no way of getting citizens to sign with this modality; she only knows the signature she uses as a civil servant, based on certificates, but clearly she can't set it up, due to its complexity, for the citizen in general. It would be very useful for her if there were a national digital signature system that, in a simple way, would allow citizens to sign documents without the need to use certificates. If this system could also work by telephone, it would make life much easier for citizens.

Mayor's advisor

Daniel

Daniel is in charge of the administrative management of a very critical legal system for the state. He has full confidence in the electronic signature, but he is not sure that it is done at the time it has been indicated in the requests; he wonders if a trusted third party could give reliability of the dates of entry of the documentation, as it is critical for his service. It would be very useful if the digital signature system were accompanied by a time stamp.

EXAMPLES

Click on each flag or icon to go deeper.

Spain

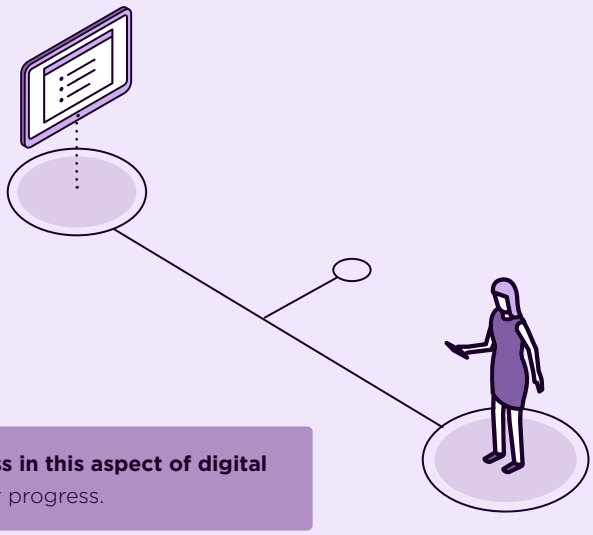
Cl@ve Signature platform

Uruguay

Digital Signature

Estonia

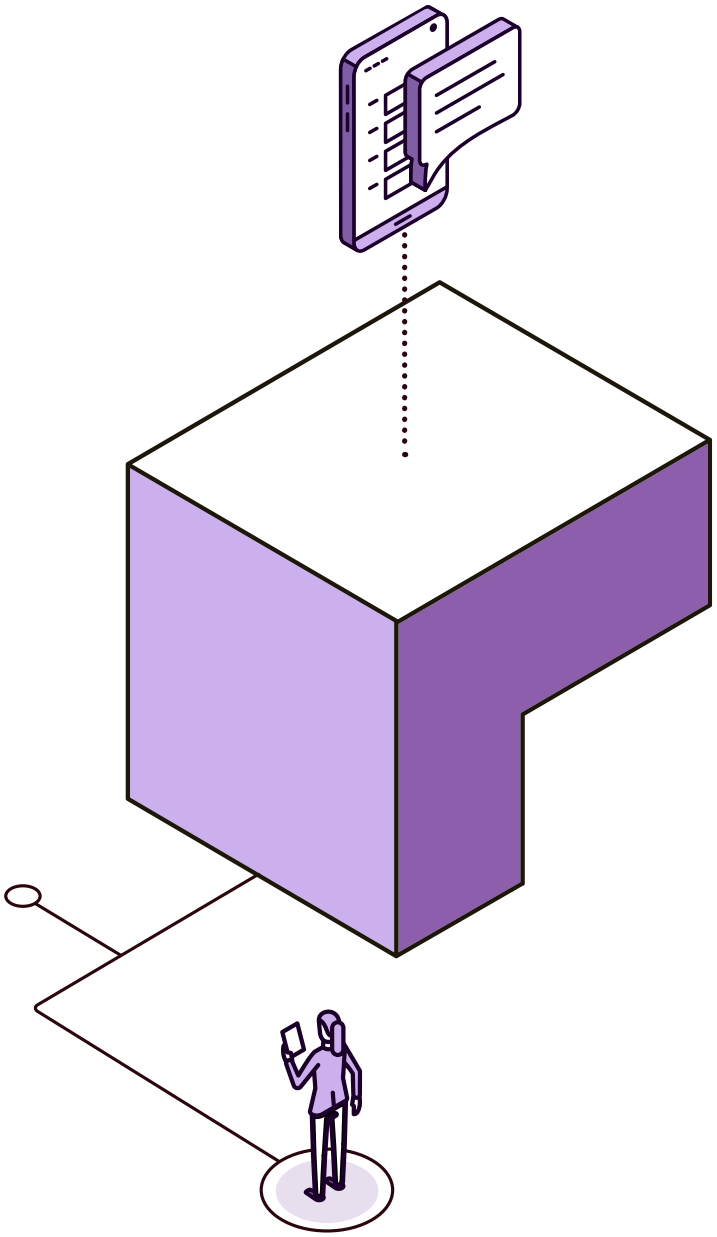
The simple how and why behind the digital signature



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a digital signature in the country?
- Does it have time stamping functionality?
- Does it have electronic sealing functionality for legal entities?
- Is the signature made through cryptographic electronic certificates?
- Is there an information system that allows public institutions to check the validity of certificates, whether national or international, at a single point?
- Is there a system that makes it easier for citizens to obtain a signature?
- Is there an electronic signature system in the cloud?
- Is it integrated in all public institutions of the central government?
- Is it common for electronic signatures to be used by civil servants?
- Is it common for electronic signatures to be used by special groups, such as businessmen, lawyers, doctors, etc.?
- Is it common for electronic signatures to be used by citizens in general?



4.5

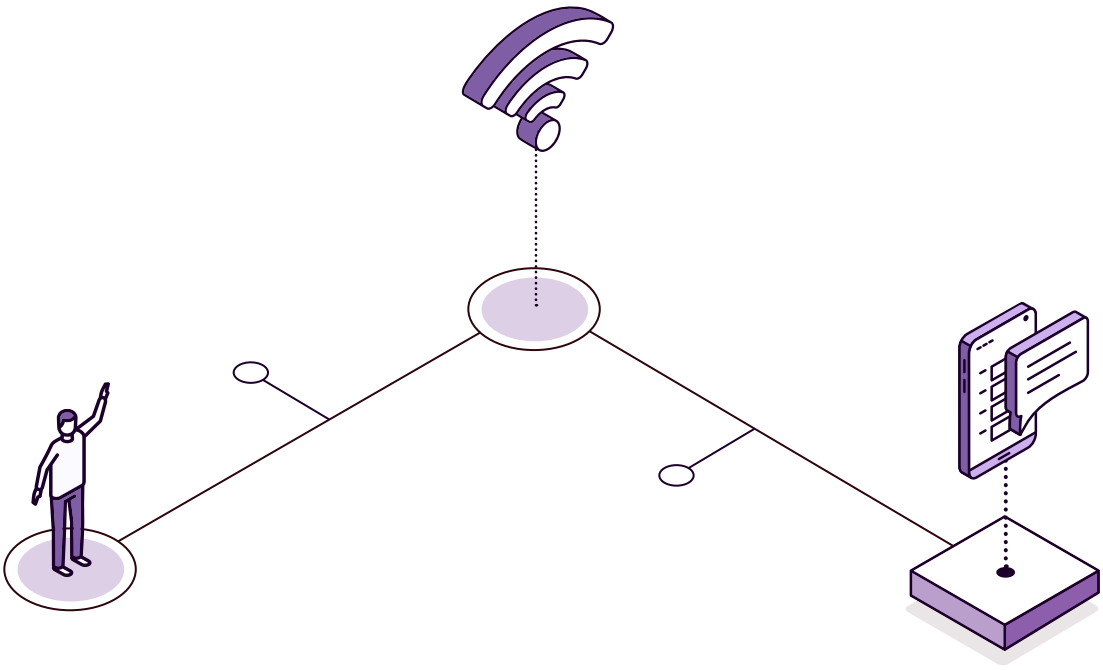
Electronic notifications

In relations with citizens and companies, public institutions sometimes have to communicate with them. Whether it is to inform them of the content of a procedure, to request more information, to proactively warn them of something that affects them, or for other reasons, it is necessary to contact and make information available to the citizen or the firm.

Digitization changes the paper support for digital documents and data. This poses a challenge in the communication of these elements with citizens and companies, as well as between administrative units. What happens is that all these relationships, internal and external, were formerly contemplated to work by face-to-face, telephone, or paper means, and digitization involves a disruption in the way of communicating and exchanging information.

Indeed, digitization transforms some fundamental concepts. For example, agencies have always worked with originals and copies, but in the digital world there may be thousands of originals (which, moreover, can be replicated at virtually no cost, and generally without control). In addition, communication and processing can be immediate, which affects certain administrative actions where deadlines and dates are crucial. Moreover, automatic and proactive processing appears, and communication systems have to incorporate this type of concepts. There no longer always has to be a human being making decisions.

Therefore, it is important to comment on some of the proposals made in this section of the document.



SINGLE POINTS OF COMMUNICATION ENTRY AND EXIT

Previous communication between entities and citizens or companies used to be done by sending a letter to their mailbox. In digital media, although email can be used for certain procedures, it is usually the citizen or company who has to go to a website to collect the information. This is not sustainable: if there is no single point of communication between institutions and citizens/companies, if the thousands of agencies in a country have a different website, or if the costs for citizens and companies are enormous, they will never be able to check all these websites to collect this information. Of course, this point can or should be integrated with the government's single point, but in this section the question is how to develop this information system, which must be prepared to be able to carry out communications automatically.

This is especially interesting for companies, since they integrate the communications system with their information systems automatically, which is a significant leap in efficiency. Therefore, it is essential that each agency avoids setting up its own communication or notification system, and instead uses a single point to operate in a homogeneous, simple, and easy to use and locate way for citizens and companies. Imagine that a country has three thousand public entities or agencies, and that each one has a different system for communicating with the citizen or company; they would have to go through all of them to find out if they have something pending, and in each case with a different way of operating and accessing information, which is not sustainable.

In turn, the same is true in the opposite direction (i.e., for communication from the citizen or company to public entities). It is therefore interesting that there is also a single point of entry to send documentation to any public body, of course through the web, but also in a fully automated way.

Precisely in order to be able to contact citizens and companies for electronic communications, it is important to have an information system where contact data (telephone, email, applications for sending messages to smartphones, etc.) are necessarily stored and where citizens can define their preferences for notifications, as well as update or manage their data.

Although there are sites where the citizen is informed for certain procedures through communications, the fact that there is no single point generates confusion and causes difficulties in terms of access and loss of notifications; thus, the model of going to different counters is replicated, but through the internet. Therefore, the existence of single points of citizen services does not prevent that at some point the document or electronic data arrives or leaves the entity in question, which may be distant (both physically and in terms of its competence) from such single points. It is therefore essential that, in an increasingly interconnected world, the communications network and the scheme allow the exchange of all these data and documents between all public entities in the country.

However, administrative notifications do not always consist of making certain data available: in some cases, they imply that from a certain point in time deadlines apply (for payments, for appeals, for obtaining benefits); in others, it is necessary to identify who collects the information, or to control access. The single point of exit offers all these functionalities for the necessary cases and avoids the need for each public entity to develop a similar system when needed.

Administrative notifications or communications have special characteristics in terms of security, confidentiality, and time management. The single point of exit facilitates the relationship with the citizen, but it is possible that the agencies, for political or institutional reasons, already had or have their own relationship system. On the other hand, although the single point of exit could do this job in a fresh start scheme, usually the country already has entities that communicate through the internet and others that, on the contrary, do not have the technical capabilities to allow this type of relationship with citizens. For this reason, this information system or interoperability node is needed to cover different objectives.

However, not everything will be done through the web page, but also through web services or any system that allows the automation of interaction. Also, by automatic means, it will be possible to consult the list of pending notifications, choose the ones you want to collect, sign or accept, and access the available contents. To promote automation, it is good that the notifications and the single point handle metadata associated with them. Thus, through the automatic systems it will be possible to know details such as

- The unit issuing the notification;
- The target unit;
- The file or administrative procedure to which it refers.

In this way you can automate the management of notifications, route them, and even process them automatically.

WHAT CAN THIS INFORMATION SYSTEM PROVIDE TO PUBLIC ENTITIES?

For public entities with the technical capacity to integrate with the single point of exit automatically, the system functions as an interoperability node. In this way it does the following:

- Manages outgoing and incoming messages.
- Facilitates certifications and delivery information of the notification or communication to the citizen.

- Consolidates and standardizes information from the different possible reporting channels:
  - At the Citizen Service Office
  - Through the telephone
  - Through the internet
  - On paper
- Connects to automated printing, enveloping, and mailing systems through a postal operator.
- As a processing *backend*, it allows for the following:
  - Management of notifications and communications.
  - To make such notifications and communications
    - In electronic format (through a single point or not)
    - On paper, by traditional means;
    - Through a visit to an office integrated with the service, where citizens can pick up their pending notifications.

For those entities that do not have the technical capacity to integrate with the system automatically, the system provides:

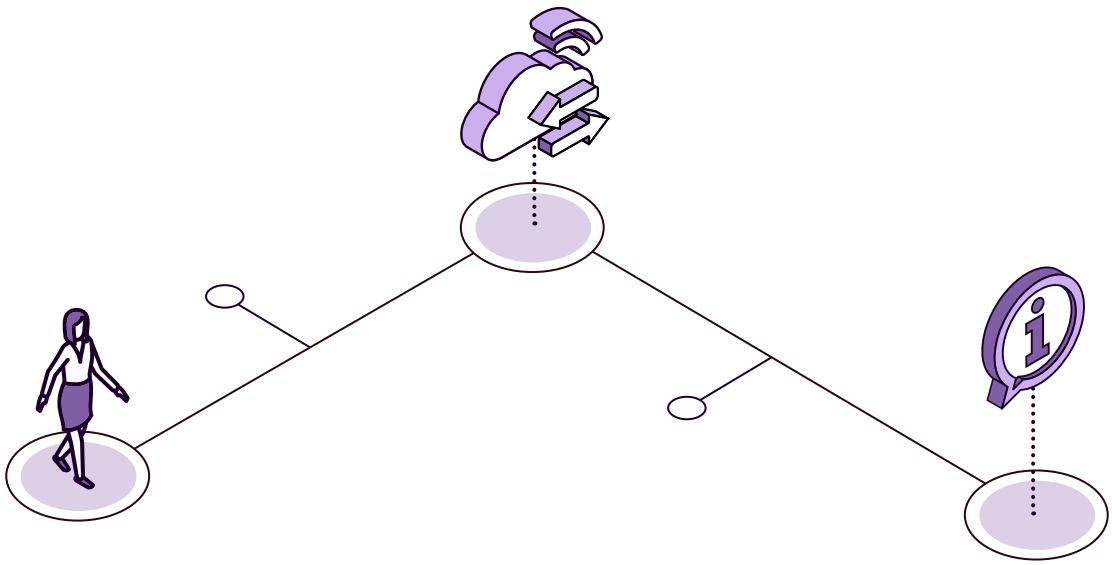
- A cloud service, so that an official identified in the system can easily send the notification or communication to the citizen from his organization, through any of the available channels, without having to do it on paper.

MODULES REQUIRED IN THE NOTIFICATION SYSTEM

Unlike the communications system, the electronic notification system serves to manage official communications for legal purposes and, therefore, needs functionalities such as the guarantee of sending and confirming receipt and recording the dates on which actions occur in relation to the notification. For this purpose, it must have

- Cloud services to route notifications to the single point and get response of their collection from agencies communicating through automated systems.
- Cloud service for small entities and organizations, so that they can manage their business through a web application.
- Integration with printing and enveloping centers.
- Integration with information from other services or web pages where notifications can be made, in order to keep the information consistent.
- Documentary repository of notifications, communications, and delivery certifications, when the institutions integrated in the system cannot manage them by themselves due to lack of technical capabilities.

THE NOTIFICATIONS CONTAIN CONFIDENTIAL INFORMATION AND CITIZEN DATA, SO IT IS ESPECIALLY IMPORTANT THAT THE SYSTEM FOLLOWS CYBERSECURITY GUIDELINES, AS WELL AS PERSONAL DATA PROTECTION GUIDELINES.



REQUIREMENTS THAT SHOULD BE MET BY ELECTRONIC NOTIFICATIONS OR COMMUNICATIONS

- **Be identified with semantic metadata of the nation.** Thus, there must be a relationship with
  - The directory of administrative units, to mark the communication with the issuing unit.
  - The directory of procedures, to associate the notification to the corresponding administrative process.
    - *Example:* The company or the citizen will be able to know if they are being informed about a sanction or a subsidy, and which administrative unit is doing it. As the code is common in the nation and automatically processable, the target information system, if any, could make decisions or do automatic processing based on that information.
- **Include the code of the destination unit,** so that the notification can automatically reach it if it has an adapted information system. As in almost all cases, there is a relationship with
  - Electronic identification, in order to know who the citizen is and to be able to show him/her only the corresponding notifications;
  - The electronic signature, for the citizen to sign the access or collection of information, in the event that it has binding legal effects and it is so considered.
- **Integration with the power of attorney management system,** especially in the case of companies, so that the person authorized by an organization to collect notifications can fulfill his or her role. This service is one of the most valued, since citizens and companies do not suffer the complications involved in searching for communications through thousands of web pages. For this reason, it is especially important to incorporate this system into the citizen folder, so that all notifications and communications can be viewed there in an integrated manner.
- **Integration with the notification system,** so that when a notification or communication is available, the citizen or the company can be notified of its existence so that he or she can pick it up. This notification system covers two fundamental and complementary needs:
  - It stores the contact data of the citizens, by different ways. Thus, it will have the email address, telephone number, or other data that allow sending a communication to the citizen. This is important, in turn, for two reasons:

- Without data warehousing, some entities will not have this information and may need to contact citizens.

- Ease of use and service to the citizen: if there is no centralized database, the citizen will have to provide his contact information to each and every public entity, in each of the procedures. This is not only inconvenient for the citizen but also represents a problem for the citizen and the institutions in the case of procedures that are extended in time, and that may suffer changes in terms of contact in the middle of the processing process. It is likely that the citizen will not remember or will not be able to update the contact information, so that both the agency involved and the citizen could be left without communication possibilities.

- Technical availability issues, especially in the case of small organizations. It is not common for them to have *push* messaging systems or even to send messages to cell phones; therefore, having a common medium that offers these services to all entities is useful for all of them.

- **To facilitate end-to-end automated processing,** the electronic document guidelines and semantics agreed upon in the forums should be followed. If the notification, apart from the file viewable by a human being, has an associated data file, in a format agreed with the private sector, it can be processed at the destination automatically, which is a quantum leap in terms of administrative efficiency.

REQUIREMENTS TO BE MET BY THE CONTACT DATABASE

- The citizen can manage it conveniently (update his/her data, activate or deactivate alerts, select a preferred method of sending, such as SMS or *email*), usually through the single point of service.

- To record the authorized uses, as it is important to ensure the protection and control of data by the citizen.

- Regarding the loading of information and updating of data in the system, apart from the self-service that the citizen may have at the single point of services/citizen folder, the system must be available to the entities that use it, so that, through an authorized official, at the time of carrying out a procedure with an institution, or if he/she approaches an office of said institution, the citizen may register in the service or update his/her data.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Entrepreneur
Ana

Ana is in charge of relations with public entities in her company. She misses the times when communications came to her on paper. Now that they are electronic, instead of being easier for her, she has to search thousands of different web pages. On some of them, she has missed notifications because the pages are difficult to access and navigate, which has negative consequences for the company. Ana would like to have a single point to receive information from all public entities more easily.

Ana is the director of a company and has always applauded the efforts of her country's tax administration service to conduct business electronically. Ana has always been able to access electronic communications of her tax issues through their system. Now that the country has made an effort in favor of digitalization and has a single point of collection for agency communications, she does not understand how the tax service and the social security service have not joined the same system, and her company has to connect to three different services, instead of simply connecting to one. She would like everything to be at a single point.

Citizen
Camilo

Camilo changed his address and recently changed his telephone number. He is concerned because he has several pending procedures with public entities, and due to these changes, he fears that he will lose any communications that may be addressed to him. He thinks that if there were a contact database that could be updated, he would not lose any communication and, in addition, he would not have to fill in his contact information every time he carries out a procedure.

Mayor's advisor
Daniel

Daniel works in a medium-sized municipality. He would love to have a more efficient system than postal mail to communicate with his citizens when doing administrative procedures, but unfortunately his municipality does not have the technical capabilities to allow the use of a mobile messaging system.

Vice minister of health
Sara

Andrés is the ICT manager of the Ministry of Health, where Sara works, and has integrated electronic notifications with the general access point but continues to process paper notifications manually. Andrés would like the paper notifications to be printed and sent on their own, industrializing the process and avoiding having to dedicate staff to low value-added services that can be done by machines.

EXAMPLES

Click on each flag or icon to go deeper.

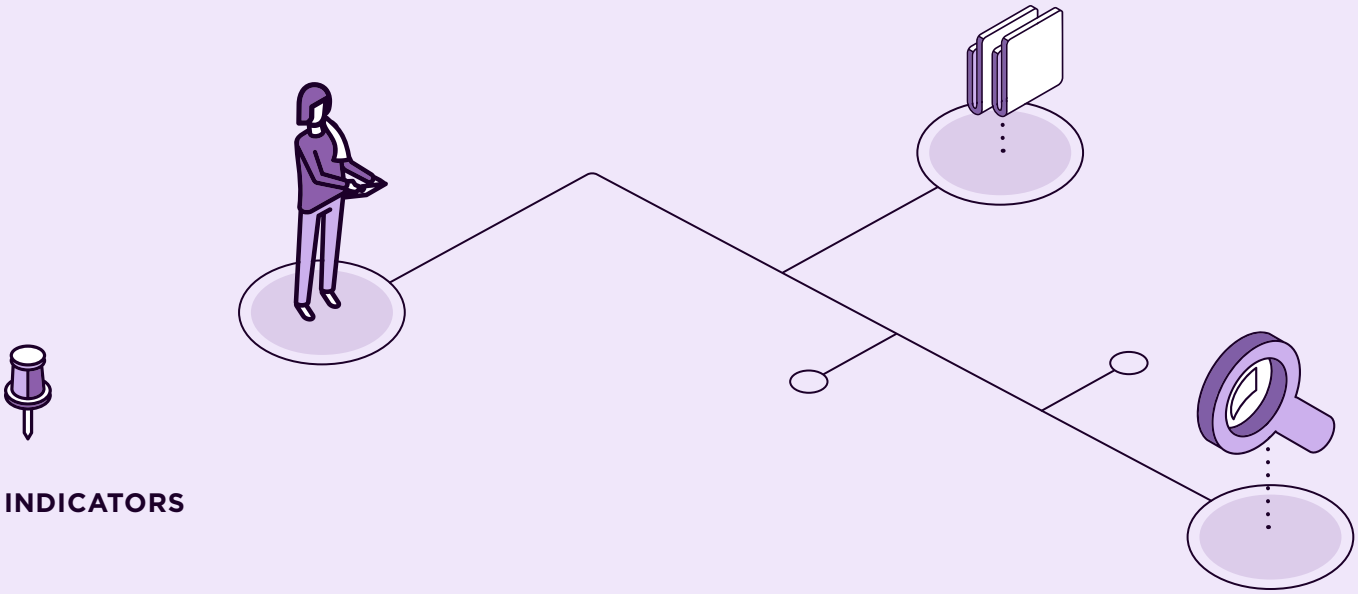
Uruguay
Digital Communication

Uruguay
Notifications

Spain
E-Mail Enabled Only (Dehú)

Spain
Single Point of notifications for all public administrations

United Kingdom
Notifications service



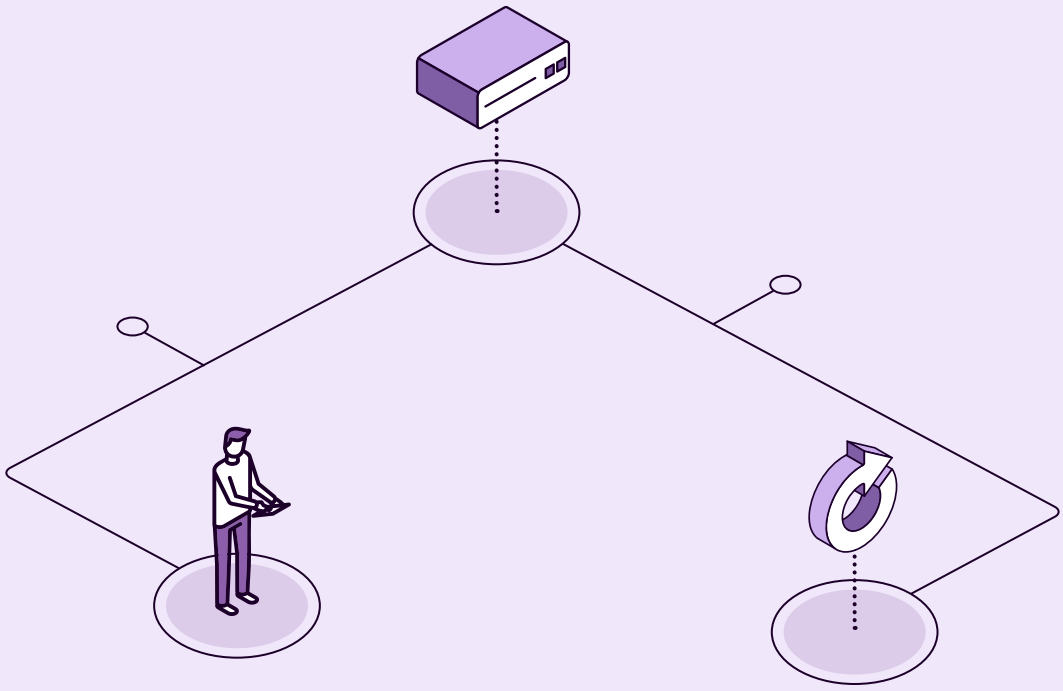
INDICATORS

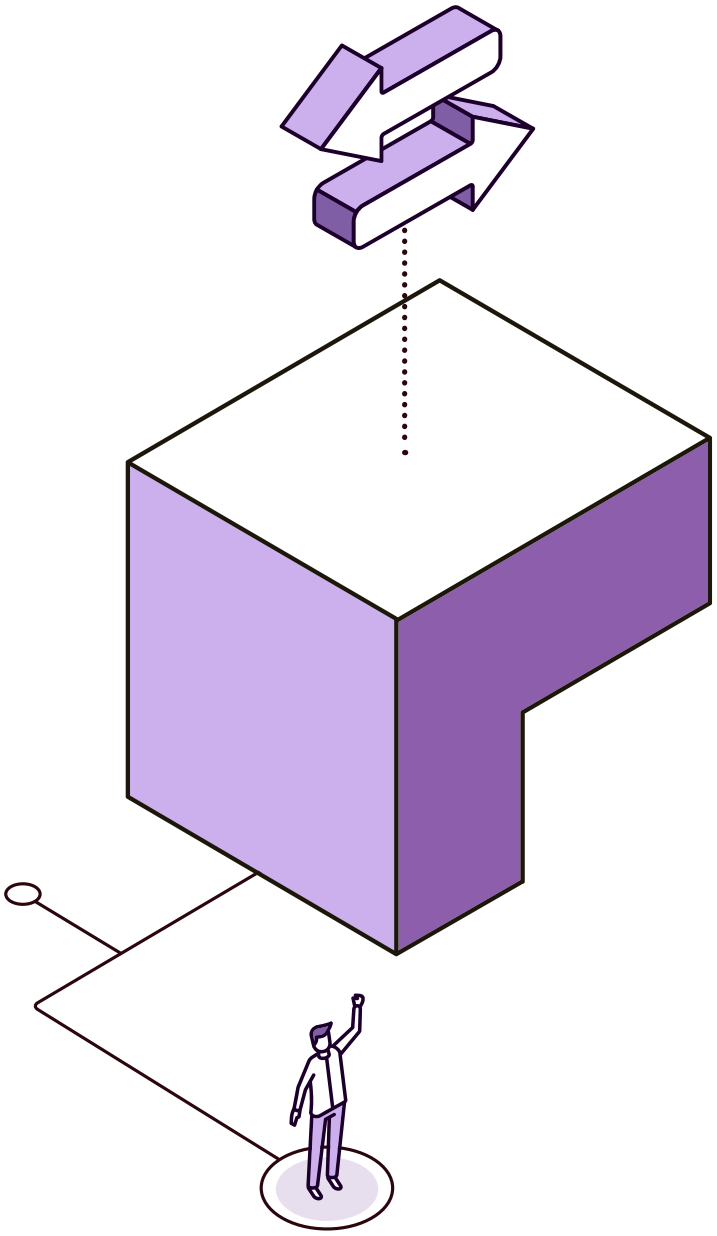
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a single point of exit for sending notifications or communications with the citizen, or similar? If so:
  - Is it integrated to the citizen folder (if any)?
  - Does it allow you to identify who is collecting the information?
  - Do you have a time stamping functionality that serves time counting with legal implications?
  - Do you handle metadata associated with communications?
  - Does it integrate the communications of more than half of the central government institutions?
  - Does it integrate the communications of all central government institutions?
  - Does it integrate the communications of more than half of the institutions across the government?

- Does it integrate communications from all institutions across government?

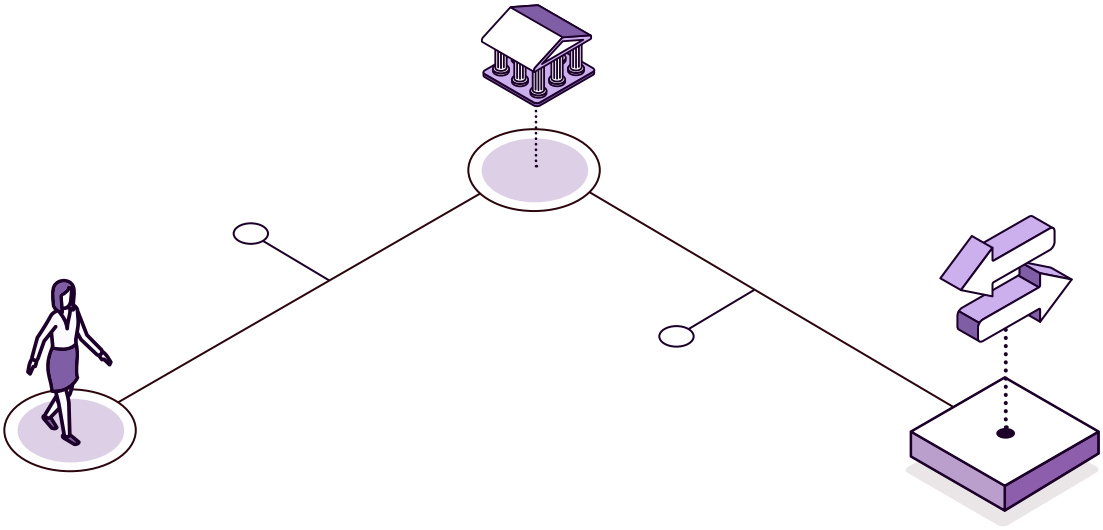
- Is there a unified database of citizen contacts that citizens can manage and update?
- Is there a unified database of company contacts that companies can manage and update?
- Is there an electronic notification system that allows sending and receiving communications with legal implications?
- Are more than half of the central government institutions incorporated into the system?
- Are all central government institutions incorporated into the system?
- Are more than half of the government-wide institutions incorporated into the system?
- Are all government-wide institutions incorporated into the system?
- Of the central government procedures that have official notifications associated with them, is it possible to receive notices through the system for more than half?





4.6

Digital input and output register



Public administrations, both in electronic communications or procedures ad intra between administrations and *ad extra* in their electronic relations with citizens, need an electronic system that provides legal security to these information transactions, whether they are data, documents, communications, or notifications. To meet this need, there is the digital input and output register: a system that allows the agency to record everything that is presented in electronic format in a public administration or body dependent on it, as well as all those official output documents addressed to other bodies or individuals.

The implementation of an input and output register allows the agency to maintain the traceability of all the information that enters and leaves the administrations, providing the whole process with a set of characteristics that make it reliable and will allow the parties to have means of proof of the completion of a procedure, evidence of presentation, etc. These attributes are

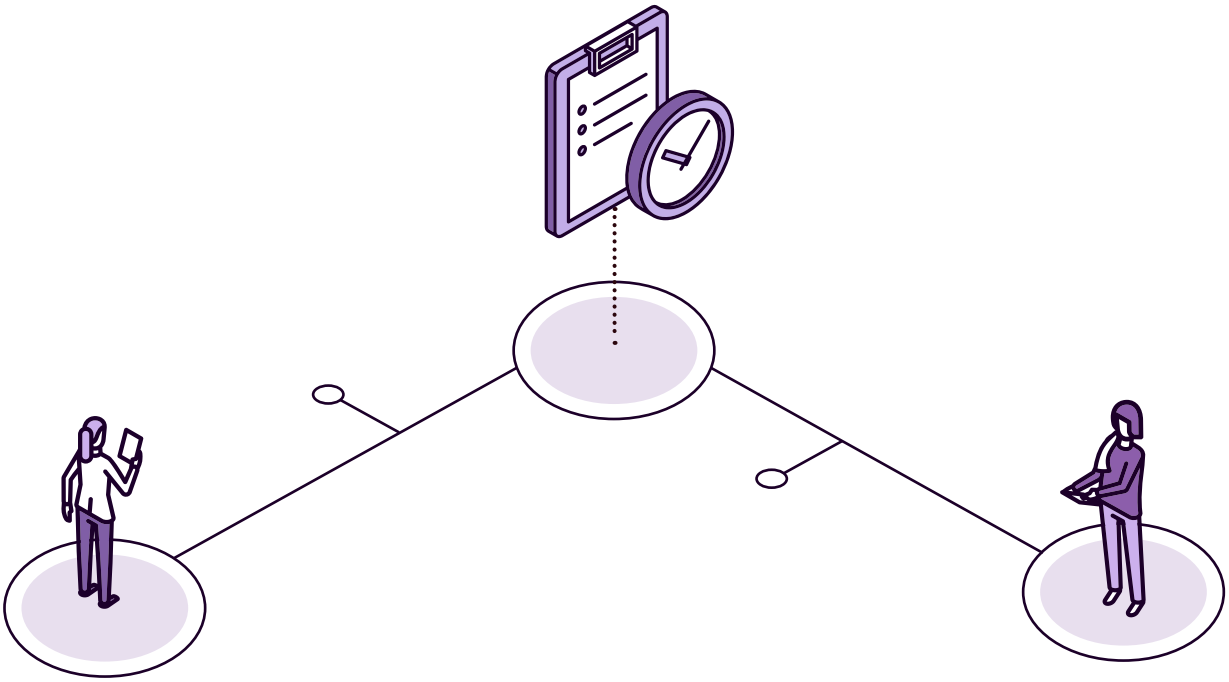
- Authenticity;
- Integrity;
- Nonrepudiation or reliability of actions and communications in dealing with the administration.

THE SYSTEM FOR REGISTERING INCOMING AND OUTGOING NOTIFICATIONS IS CLOSELY RELATED TO THAT OF ELECTRONIC NOTIFICATIONS, IN ORDER TO BE ABLE TO "REGISTER" EVERY NOTIFICATION THAT GOES OUT TO THE INTERESTED PARTY'S MAILBOX. BUT THEY ARE CLEARLY DIFFERENT SYSTEMS WITH DIFFERENT TASKS.

WHAT NEEDS TO BE COVERED BY THE INPUT/OUTPUT REGISTER

- **Formalities corresponding to administrative procedures that are identified and catalogued among those offered by the corresponding administration, normally through electronic offices.** In this case, the system functions as a support to the electronic channel of relationship with the public administration, providing it with legal security by guaranteeing the characteristics indicated above (authenticity, integrity, nonrepudiation, or authenticity of the actions and communications). In other words, the registration process must guide and accompany users through the necessary forms in order to collect all the necessary information in a structured format, so that it is defined in a specific way for the procedure in question.

- **Submission of requests, writings, or communications addressed to public administrations that do not comply with the previous catalogued administrative procedures.** This is because citizens, in their relationship with the administration, are in a position to submit to it whatever they consider necessary in the exercise of their rights. In this case, in addition to the registration and the automatic generation of acknowledgements of receipt, a generic presentation interface will be needed that allows the user either to write a generic text, or to attach any file, or both.



THE BASIS FOR IMPLEMENTING A DIGITAL INPUT/OUTPUT REGISTER

The digital input and output registry must function as a single system, allowing citizens to interact with the administration as a single entity, without the need to know its organizational characteristics. Thus, regardless of the place of presentation, the documentation must reach its destination. For this purpose it is necessary to do the following:

- Interconnect all registries in a single network that allows the interoperation of any registry entry made in any body belonging to the administration. In this sense, it is important to have a solid interoperability regulation, as well as technical regulations related to the exchange of registry entries.

- Have an infrastructure deployed and available for the interconnection of offices in the digital administration ecosystem. This ensures the real interoperability of registry entries between them. Note the need for a directory of public entities.

- Make the registry system work as a means of digitalization of the paper presented by the citizen, in those cases in which this support is chosen. In the transition from paper-based processing to electronic processing, this will be key to the elimination of paper in its entry into the public administration.

- Have a digital input and output register, which the lead institution for digital transformation will make available to the sectoral institutions for their use and, if necessary, adaptation and/or improvement. This should include:

  - The corresponding entries of any document that is submitted to or received by any public administration or agency under its authority;

  - The output of official documents addressed to other bodies or individuals.

  The agencies linked to or dependent on each sectoral institution will be in a position to have their own digital input and output register, but this must be:

  - Interoperable;

  - Connected to that of the institution or administration on which they depend;

  - Part of the national network of digital input and output registries, allowing full interoperability of registry entries and documents throughout the territory.

THE RELATIONSHIP OF CITIZENS WITH THIS SERVICE

The digital input and output registry must be available to citizens from the internet and will be offered from the electronic office of the corresponding administration. In this way, people will be able to access the service through an electronic certificate or other element that allows both electronic identification and the corresponding electronic signature of the submission form, and the possibility of attaching associated electronic documents must be provided.

In the event that the citizen goes to a physical office of the administration that offers the entry registry service, the office itself will digitalize the information presented to incorporate the documentation into the electronic file and will deliver the corresponding acknowledgement of receipt to the citizen along with the originals. The system can also implement associated services that increase the usability of these systems with citizens, such as:

- Consultation of different registry entries;
- The sending of notices by SMS or *email* with the changes in the status of the registry entries.

The registry entries shall be recorded in the order in which the documents are received or issued, and shall include at least the following information:

- Unique identification number
- Epigraph expressive of its nature
- Date and time of your presentation
- Identification of the interested party (name, surname, national identification number)
- Sending administrative body, if applicable
- Person or administrative body to whom it is sent
- Reference to the content of the document being registered, if applicable

The acknowledgement of receipt after submission shall be issued automatically, shall be signed electronically, and shall at least contain the following information:

- Individualized registration number or code

- Date and time of presentation

- Copy of the letter, communication, or application submitted, or, if applicable, literal reproduction of the data included in the submission form

- If applicable, the list and name of the documents attached to the filing form or document submitted, followed by the electronic fingerprint (*hash* code) of each one of them, as a guarantee of integrity and nonrepudiation

- If applicable, information regarding the maximum administrative term established for the resolution and notification of the procedure.

The filing may be made at any office that offers the entry registry service, and it will be this same office that will forward it to the destination office in the event that they are different, making use of a platform that allows the interconnection of the registries within a single network. The operation of such a platform will be based on mandatory compliance with a minimum information structure and minimum technological requirements for the exchange. To this end, it will be necessary to have a technical norm or standard that standardizes and establishes a single, global, and complete data model for the exchange of entries between registry offices, regardless of the registry system of origin or destination, and regardless of the exchange technology.

MAIN REQUIREMENTS FOR THE IMPLEMENTATION OF A DIGITAL INPUT/OUTPUT REGISTER

- **Directory of administration units:** It is necessary to have a directory of administration units, identified with a unique code, which will be able to work as registration and delivery offices. This allows the agency to

  - Univocally associate the registry entry to an entity;

  - Support the system of interconnection of records, so that it is possible to identify the origin and destination of communications.

- **Procedure catalog:** The documents submitted or sent that are recorded in the digital input and output system belong to an administrative procedure or process. They should be marked as such, and if there is a unique catalog of procedures, that code should be used to mark them.

- **Interoperability:** The exchange of information between different registry offices will require the possibility of exchanging registry entries and documents, which will require an interconnection platform to support this functionality.

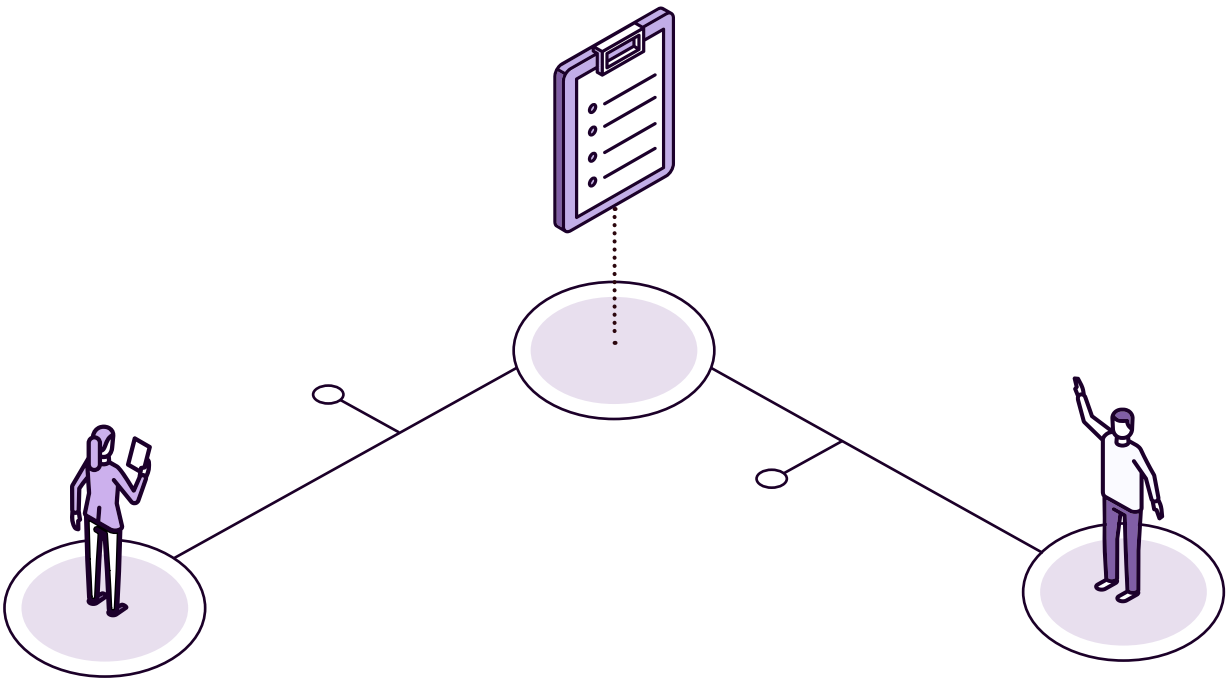
- **Digital signature system:** Both the submission of documents by citizens and the issuance of acknowledgements of receipt after the corresponding registry entry must be signed electronically, which implies having a system that allows the signature of both the form submitted and the acknowledgment of receipt issued, as well as the possibility of validating the signatures submitted.

- **ID system:** The presentation of documents by citizens requires prior digital identification by them, so it will be necessary to have a system of these characteristics.

- **Electronic headquarters:** The universal digital channel for the relationship between the administration and the citizens is the electronic headquarters, so it must be available for the provision of digital entry registration services.

- **Digitalization system:** In the event that the presentation of documents is done in person at a physical office, the office must have a system that allows on-site digitalization of all documentation presented by the citizen.

- **Notification system:** If functionalities are offered that provide added value to citizens, such as sending SMS or emails to notify them of any change in the status of the registry entry, systems must be in place that allow the management and issuance of such notifications.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo is waiting to apply for a scholarship for one of his children, but the application deadline coincides with him being sick at home and unable to go out. He fears that he will not be able to apply because he has to go to school in person, driving his car for several kilometers with all the paper documents. When he thinks about his case, he wonders how much he would benefit from being able to apply from home.

Education officer
Lucia

Every year, at this time of year when all parents apply for their children's scholarships, Lucia thinks about the problems caused by all the paperwork she receives and the complications caused by the handling of the corrections of undelivered or erroneous documents. In addition, she has to suffer the complaints from parents about misplaced documents. She thinks about when the time will come when all the documentation will be electronic and she will be able to have it available on her computer, without having to allocate part of her office space to organize the information received, with the consequent risk of losing some paper.

Vice minister of education
Sara

Sara just found out that more than 50 percent of the scholarships could not be applied for because of a flu outbreak that has kept most of the parents at home, unable to go to the school in person to hand in the paperwork. She does not understand how children's education can be jeopardized because their parents are sick. She decides to promote the implementation of digital check-in systems that allow parents to access scholarship services from home, because she wants to offer the best educational opportunities to her citizens.

EXAMPLES

Click on each flag or icon to go deeper.

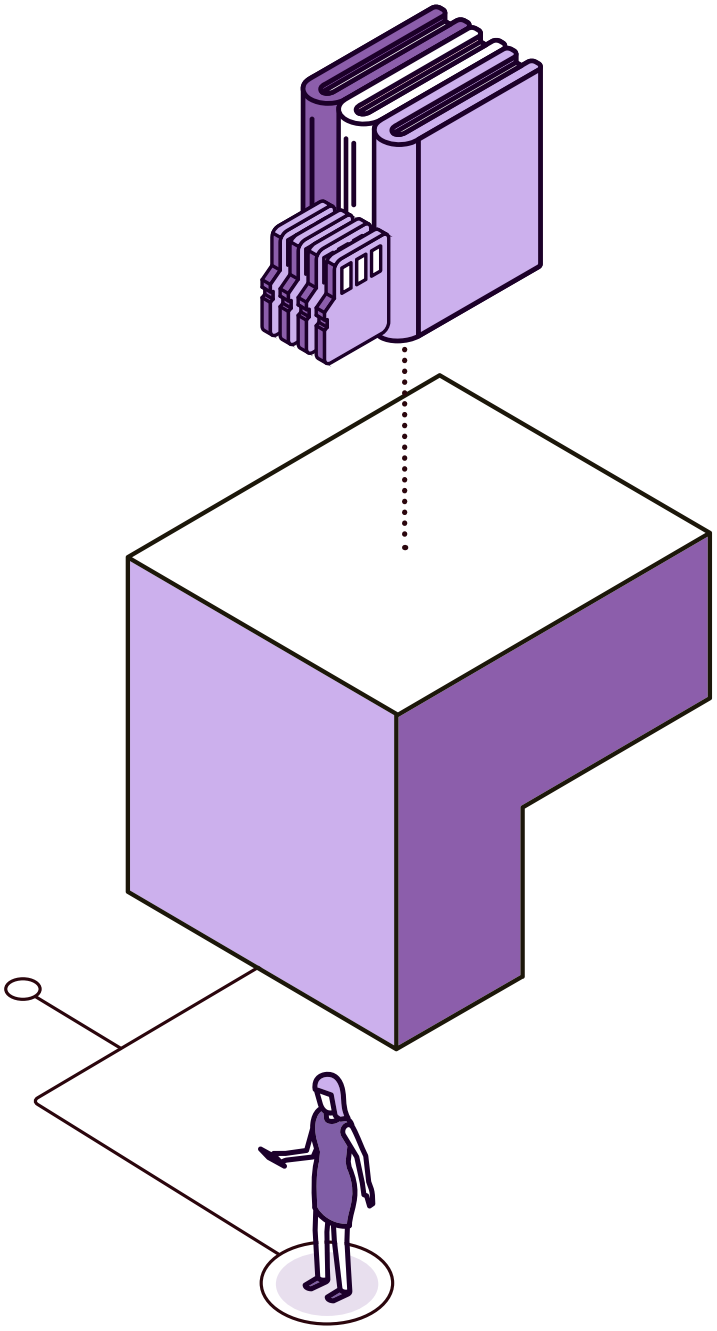
Spain
System of Interconnection of Registries (SIR)

Spain
Common Electronic Registry

INDICATORS

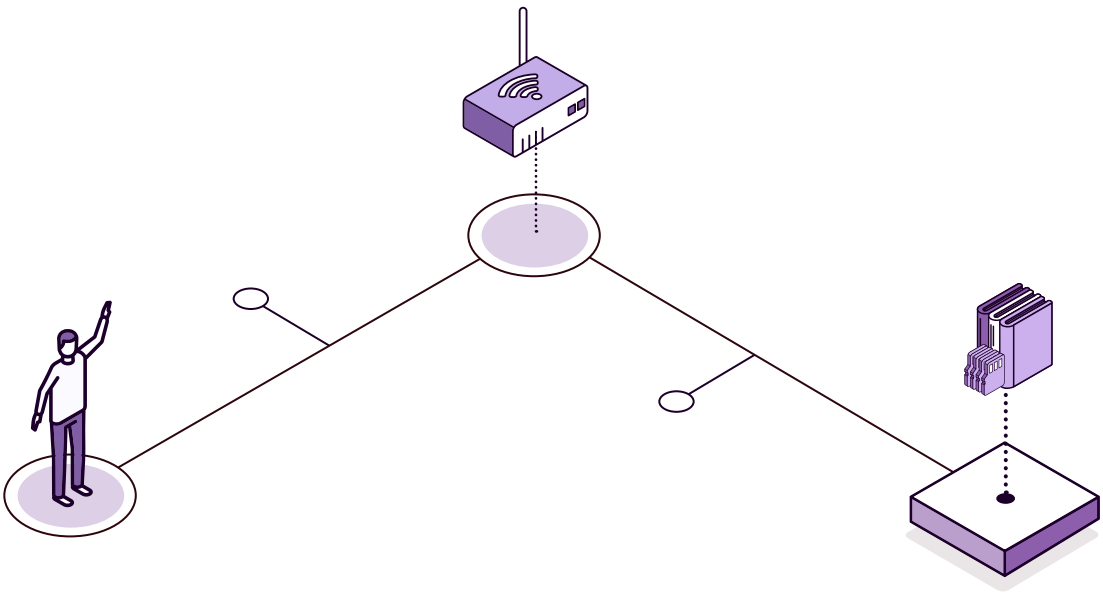
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there entry and exit registers in the administrative bodies?
- Is there a common electronic registry?
- Is an acknowledgement of receipt delivered in digital format?
- Is there a system that interconnects the different registers?



4.7

National digital archive



Within the electronic document management process there are, broadly speaking, three phases:

- **Capture:** After the creation or production of the document.
- **Maintenance and use:** Once the administrative processing is finished, where the documents still maintain their administrative validity and are available.
- **Conservation and selection:** Where document conservation policies are applied (administrative, legal, archival, historical or research, and social utility), based on which documents it is decided should be kept and which should be destroyed.

It is precisely in the last phase, once the administrative process has been completed, that the national digital archive must come into operation. This is a service that allows the electronic storage of all documents used in administrative proceedings. It also supports the centralized national archives, as well as those entities that do not have the capacity to generate and maintain an electronic archive for the long-term preservation and retrieval of files and documents.

TASKS FACILITATED BY A NATIONAL DIGITAL ARCHIVE

- Management of the file's conservation status
- Archiving metadata management
- Execution of conservation policies
- Document format changes
- Management of document classification tables

CONSERVATION AND ACCESS: TWO FUNCTIONALITIES THAT GO HAND IN HAND

Today is the time in history when more information is being generated and, at the same time, more information is being lost. Well-preserved paper can last for centuries, as demonstrated by many archives and libraries; on the other hand, a standard LTO *backup* tape,[38] which is still in use, has a life span of thirty years. For this reason, it is essential that the country prepares itself with a national digital archiving strategy to prevent the loss of the nation's documentary heritage, as well as to provide support from the lead institution for this task.

It is vitally important to keep in mind that many institutions will not be able to maintain electronic documents and records in the long term. Unlike paper archiving (which is expensive and complex but can be done by a small office), the inherent complexity of electronic archiving means that only large organizations are likely to be able to do it properly. It is essential, therefore, that one of these institutions (or the national archives) can provide this type of service, to avoid losing key information for the nation.

Likewise, the reason for archiving information should not be forgotten: to be able to consult and consume it. It is very common for great emphasis to be placed on the archiving process and on the maintenance of the information, but not on its access. The importance of archiving has to do with access; if you have perfectly preserved but inaccessible data, it may not make much sense to preserve it. Therefore, the archiving strategy must consider access to and exploitation of the stored information.

38. Magnetic tape, the standard model of physical support for long-term backup of massive information.

NATIONAL ARCHIVING STRATEGY

Regardless of the solution chosen for implementing the digital archive, whether commercial or designed by the administration itself, it is essential that the system's operation be based on compliance with common guidelines and standards for document management and preservation. To this end, it is essential to have a national archiving strategy such as the one mentioned above. This strategy will be materialized in the following ways:

- One or more electronic document management retention policies
- A national metadata schema for electronic document management
- Documentary classification tables
- Document retention strategy and schedules
- Criteria and conditions for access to archived documents
- Strategy and measures for long-term preservation of documents
- Policies for the transfer of documents between different archives
- Procedures for the destruction and deletion of information, in case its preservation is no longer required.

WHATEVER THE TECHNOLOGICAL SUBSTRATE, THE ARCHIVING SYSTEM SHOULD BE TECHNOLOGY NEUTRAL AND SHOULD COMPLY WITH NATIONALLY DEFINED GUIDELINES AND STANDARDS.

As in all transversal and critical infrastructures for the operation of the service provided by the administration, it is important to consider the aspect of technological neutrality. It is not possible to depend on specific technologies; rather, it is the technologies that must be adapted to the conservation requirements established. In this way, once the technology becomes obsolete, technological migration is possible, since the logical requirements remain unchanged over time.

CONDITIONS TO BE MET BY A NATIONAL DIGITAL ARCHIVE

- **It must be structured and follow all the indications and good archiving practices mentioned above:** The archive cannot be just a repository of information; it must have a specific structure. The information must be classified, described, qualified, and categorized (for example, in documentary series), and it must be equipped with business intelligence for its correct exploitation.

- **It must contemplate compliance with legal and regulatory requirements,** especially with regard to:

  - Security, accessibility, and processing of personal data;
  - The execution of processes related to interoperability;
  - Actions ruled on electronic documents;
  - The time of conservation of the information.

- **It must have an auditing system in place** in order to:

  - Record access to information;
  - Certify that documents are protected against unauthorized access, modification and destruction;
  - Ensure the authenticity, reliability, integrity, availability, and preservation of electronic documents.

- **It must avoid degradation or loss of the intrinsic characteristics of the documents:** This not only affects the preservation of the document, but also the context information and components of the document, which together guarantee its probative value and reliability as electronic evidence over time. To this end, it is appropriate to contemplate situations of:

  - Renewal of storage media and document formats due to technological obsolescence (it is recommended to opt for open document formats regulated by international standards, as opposed to proprietary document formats);
  - Migration of documents from one database to another;
  - Platform changes;

- Modifications in the electronic document management processes;
- Long-term preservation of electronic signatures.

- **It must have interfaces that facilitate the availability, access, and exploitation of information:** In addition to the data exploitation interface, it is necessary to offer interfaces for the exploitation of metadata in an automated manner. All metadata are essential:
  - Those associated with the information itself (i.e., the natural or legal person associated with the data, the type of data, the date of the data, etc.)
  - Those of the system itself, such as the document series to which they belong, the level of access, confidentiality, etc., which make it possible to process requests more efficiently.
    - *Example:* You can download the video data of a trial involving company X or the resolution awarding a contract to company Y, but also locate the necessary information automatically.
- **It must be interoperable with the state's information exchange platforms:** Thus, when a document is needed, it can travel automatically by electronic means or be made available remotely.

IT IS IMPORTANT TO HAVE ACCESS TO THE INFORMATION SYSTEM THROUGH THE INTERNET AT THE SERVICE OF CITIZENS AND SPECIALISTS SUCH AS HISTORIANS, JOURNALISTS, PERSONNEL OF PUBLIC ENTITIES, AND OTHERS.

CONDITIONS FAVORING THE IMPLEMENTATION OF A NATIONAL DIGITAL ARCHIVE

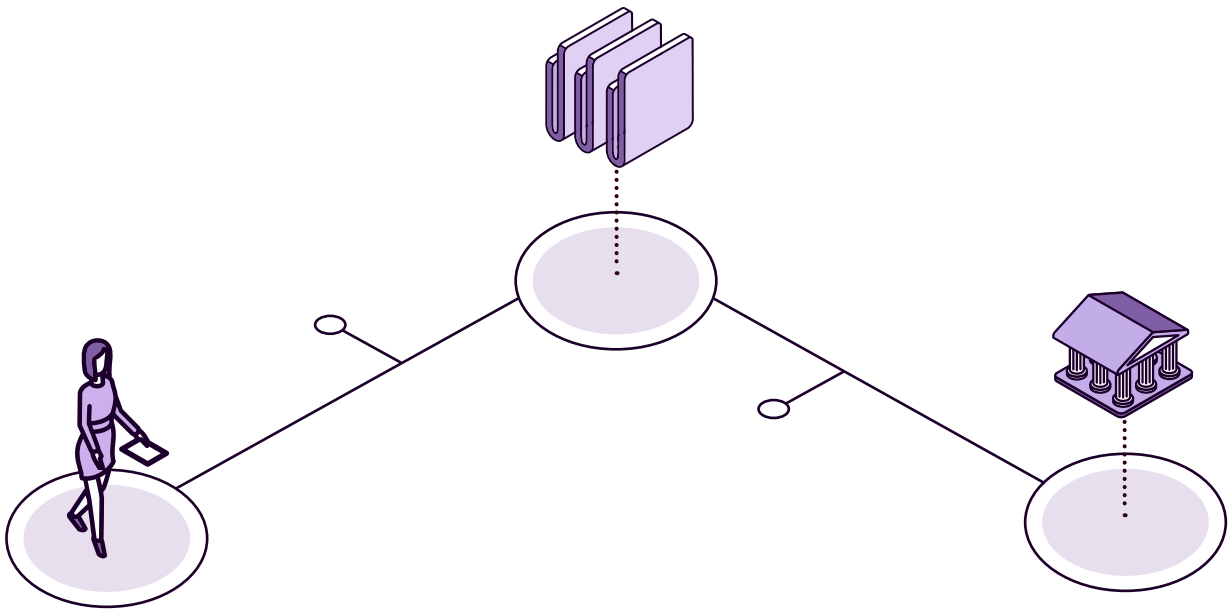
- **Digital document managers or digital records:** Without these inputs, it will be impossible or tremendously expensive to transfer information to the digital archive. In some cases, complex and expensive digital archiving systems have been acquired without the public entity working with digital records, and these spend their amortization period without use.
- **Directory of public institutions:** It is very useful to mark each document or file in the archive with the unit to which it belongs. The best way to do this is through a unique code that is common to all entities and univocal, and which identifies the institution that owns each document or file. The unit directory fulfills this function.

- **Procedure catalog:** The documents or files in the archive belong to an administrative procedure. Therefore, they should be marked as such and, if there is a single catalog of procedures, this code should be used to mark them.

- **Staff members of the various institutions must be able to access the archive:** The existence of a registry of staff members, with their respective access profiles, greatly facilitates the management of registration, deregistration, and use of the system. In this way, there is no need to create a database of officials, which runs the risk of becoming outdated.

- **The file exchange system may have a connection to the archiving system, to which files can be sent:** Typically, archiving systems following the international OAIS standard use file transfer packages, although it may be useful to integrate, if available, the file exchange system with the archive.

- The citizen folder and the *open data* and transparency systems should be accessible and allow consultation of the information in the digital archive.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

To renew his cab license at a discount, Camilo must indicate that his father was also a cab driver and that he had both the national and municipal authorization. He will save some money on the renewal, but it will take him quite some time, because the only way to get these old documents is to physically go to the municipal and Ministry of Transport archives. When he thinks about his case, he thinks about how much the country would benefit if there were a single digitized archive, where citizens could access all historical documents.

Entrepreneur
Ana

For the foundation of her company, Ana is making an exhibition on the history of technology firms in her country. She is looking for old documents about them, but in cases where the documents are in the possession of public entities, they only have them on paper, and to access them Ana is forced to do more than one procedure. She doesn't quite understand why so many interesting things are archived if they can't be used or accessed.

Vice minister of health
Sara

Sara has just found out that after the change of the contractor that was in charge of managing the health record, the patient data that this company handled was lost. She does not understand how something so serious for the people and the country can depend on a company. For now, through the judicial system they are trying to make all the information that the contractor had in its systems pass to the ministry. In parallel, the ministry's archiving strategy has been created, so that the health data will be digitized and available indefinitely in national archives.

Mayor's advisor
Daniel

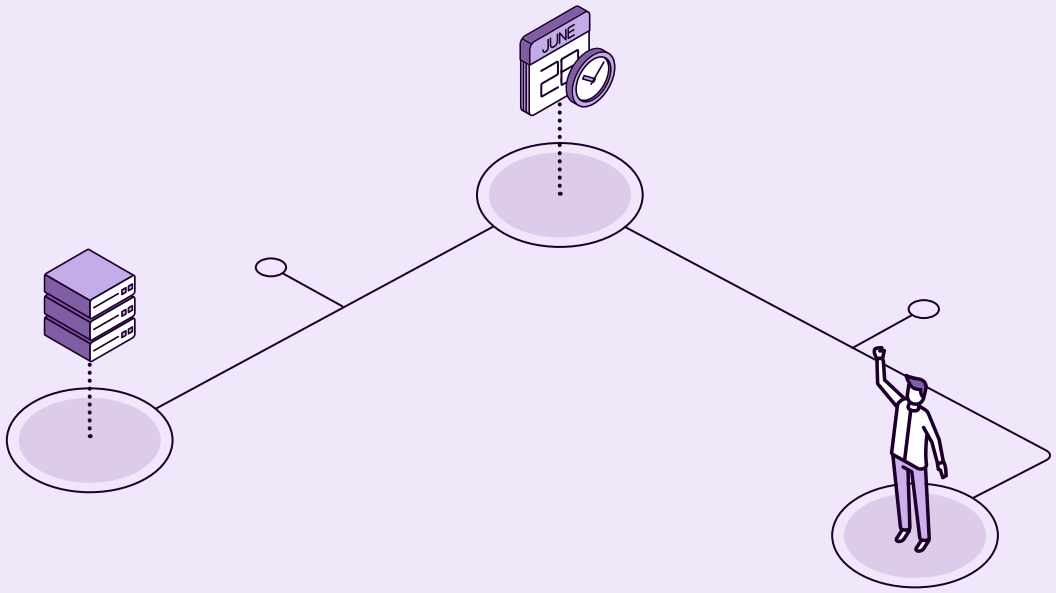
The information systems of the municipality where Daniel works work reasonably well, but each one is different. Following the national archiving strategy, and using the application provided by the digital government directorate to the municipalities, Daniel is working to have all the secretariats of the municipality record the information in a common archiving format, so that it can be preserved for the long term.

EXAMPLES

Click on each flag or icon to go deeper.

Colombia
National Digital Archive
Project – ADN

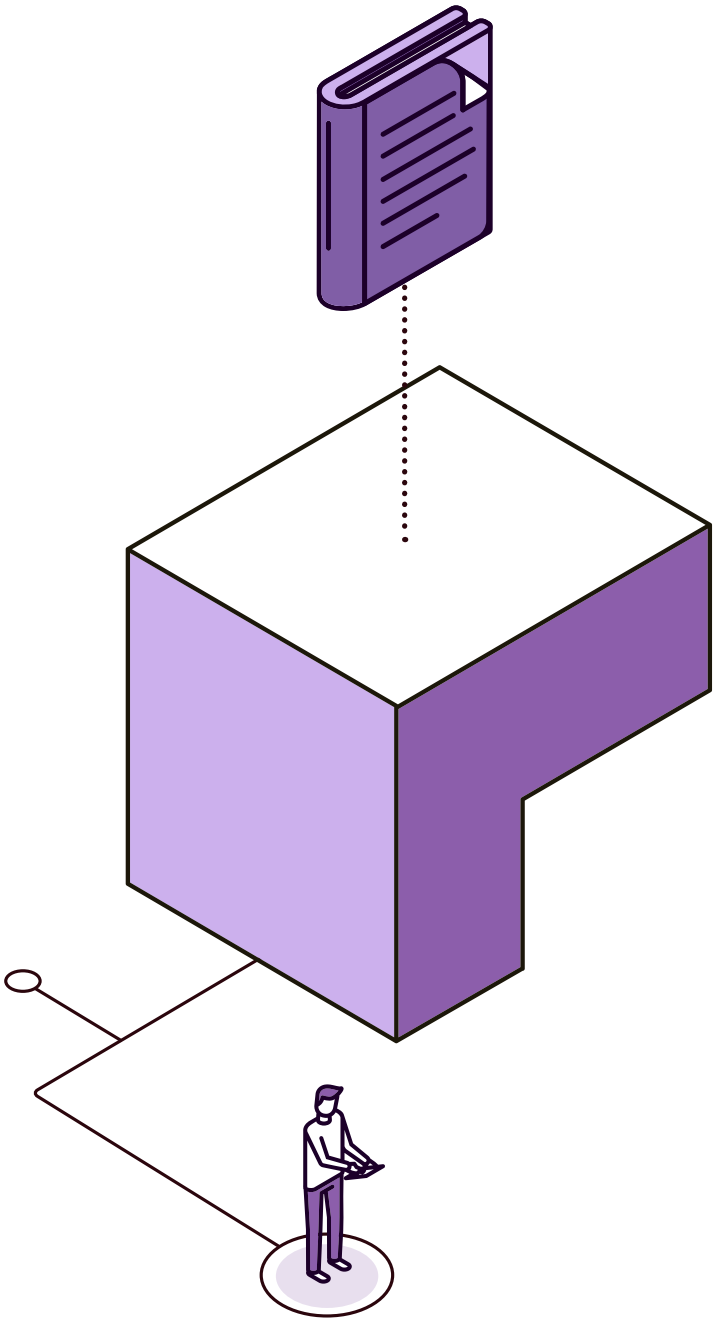
Spain
Electronic Archive



INDICATORS

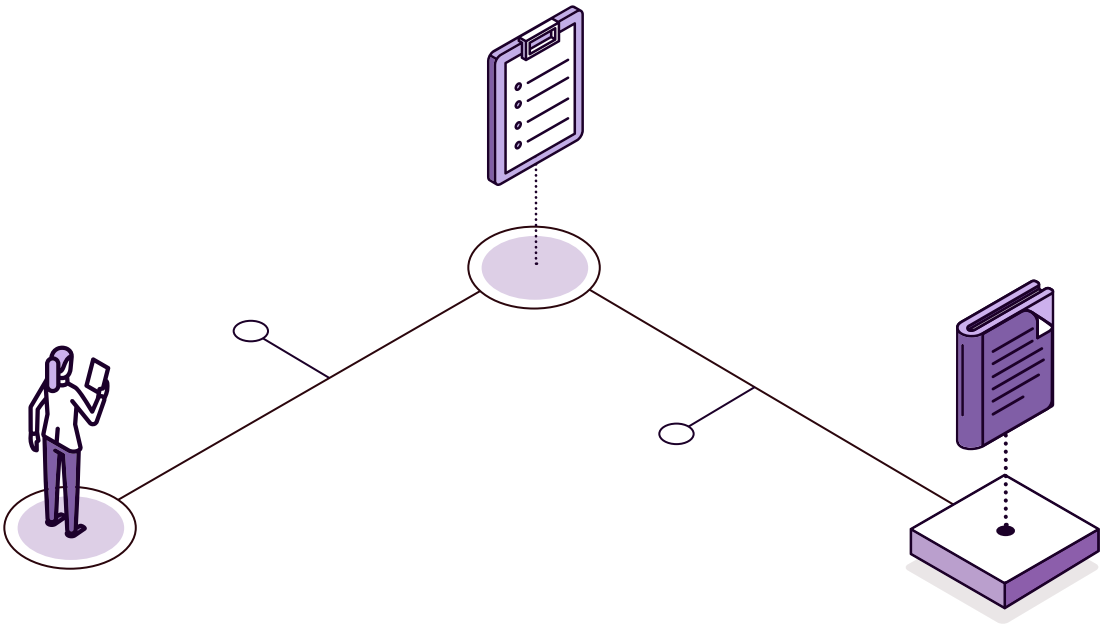
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a long-term national electronic archive?
- Are there standards that regulate long-term archiving?
- What percentage of public entities of the central government have long-term electronic archives that comply with minimum standards (Open Archival Information System [OAIS], an ISSO standard)?
- Do more than 50 percent of public entities across government have a long-term electronic archive that meets minimum standards (OAIS, an ISSO standard)?
- Are there national standards that exceed OAIS standards?
- Do more than 50 percent of public entities of the central government have interoperable archives or archives integrated into the national archive?
- Do more than 50 percent of public entities across the government have interoperable or integrated records in the national archive?



4.8

Electronic administrative directories



Records are understood as the information systems that—previously on paper—attest to certain information. They have administrative validity, although they are not sufficiently valued, and homogenize categories and data, which is why they have always been vital for administrative functioning.

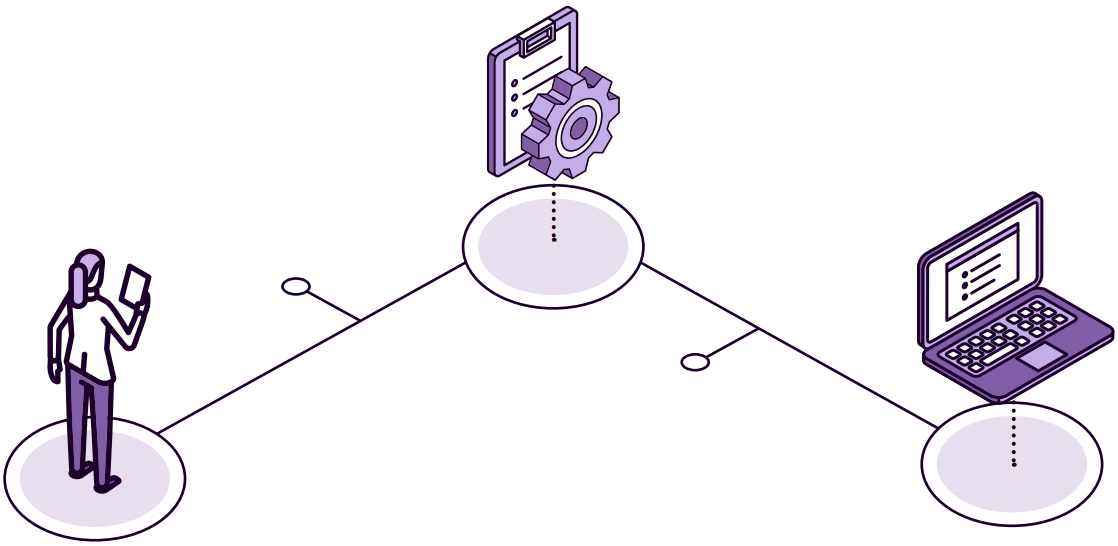
IT IS INCONCEIVABLE FOR A COUNTRY TO EXIST WITHOUT A CIVIL REGISTRY, PROPERTY REGISTRY, LAND REGISTRY, BUSINESS REGISTRY, ETC.

Records

- Provide legal security to the operation of the country;
- Are single points that control discrepancies;
- Standardize the information of certain sectors;
- Are recognized by the public sector (which generally manages them) and the private sector.

For the operation of digital transformation, the concept of registry is even more important than for the traditional administrative concept, since the reliability and standardization they offer are essential for, for example, automated processing projects. Therefore, within a country's digital transformation project, it is necessary to have new registries or adapt existing registries. Thus, it is necessary to have the following:

- A codified (and automatically processable) standardized registry of procedures, containing all the procedures of the different entities (and standardized information associated with each of them).
- Records of administrative units, in order to facilitate exchanges, both between entities and with the private sector.
- Business records, which allow for error-free and efficient routing of documentation or requests.
- Company power of attorney records. Indeed, it is no longer necessary for a lawyer to read a power of attorney to know whether a person can carry out a procedure on behalf of a company; the information system must be able to perform this evaluation automatically, which is a highly complex challenge.
- Registration of officials. As is the case with corporate powers, so is the case with the data of officials. In general, institutions relate to other institutions. Thus, it is necessary to know that the official representing an entity has the appropriate appointment to perform the task he or she is carrying out, from the simplest (such as sending a document to another agency) to the most delicate (such as intervening or imposing a sanction by a control unit on a particular entity). For all these reasons, there must be a registry of officials that makes it possible to know—and automatically process—the competencies that each one of them has.



4.8.1 DIRECTORY OF PUBLIC ENTITIES

Until now, in the paper world, there was a standardized way to locate and send information in each of the countries: basically, the name of the unit and its mailing address. However, in the digital world, how can documentation or information be routed? How can the "address book" be known, just as it was with telephones? This problem must be solved, since information must be exchanged, in this case by electronic means, and logically the email address is not an official or reliable method.

Of course, to solve this problem, some vertical organizations have their own partial directories; for example, the tax or social security sector. The point is that they are not common, unique, or interoperable. Thus, in one state (in a federal state), the department of mines may have the code "mines," which may be the same as the federal government's code for the Ministry of Mines.

Problems also arise with nonstandard nomenclature. For example, in finance there may be a code for "Santiago"; in social security, another one for "Santiago Municipality"; in the labor department, another one for "Santiago City"; etc. A human being could understand that it is the same thing, but an information system needs a unique code to interoperate without the possibility of error or doubt.

Therefore, a directory of public entities should be created, containing information on the administrative units and offices of all public entities, as well as their hierarchical and other relationships that may exist between them.

HOW DOES A DIRECTORY OF PUBLIC ENTITIES WORK?

1. First, a directory of unique codes containing all administrative units should be created. These codes could form the "snapshot" of all the nation's administrative units; they will be public and known to everyone, both in the private and public sectors.

2. To send certain information to one of these units, it will only be necessary to search for or know the code and indicate it in the corresponding information system, which will automatically send the document to the destination by electronic means.

3. The mailings end up going to individuals (at their email addresses) who are loaded into the system, with certain responsibilities.

    - *Example:* For a contracting issue, the name and email of the person in charge of contracting would be loaded into the system, and that official would receive the corresponding communications.

4. The code is not only used to route documentation; it is also used to associate files and documents (which assigns them to that unit), to relate users (which identifies them with that organization), to associate the procedures that each unit has, and so on.

IN SHORT, WHEN YOU SEE A CODE, WITH THIS DIRECTORY YOU KNOW WHICH UNIT IT REFERS TO, WITHOUT THE PROBLEMS CAUSED BY PARTIAL DIRECTORIES. MOREOVER, AS IT IS COMMON AND UNIQUE, IT FACILITATES INTEROPERABILITY BETWEEN ALL ACTORS.

USE OF METADATA

The entity directory is not only a table to associate a description to an alphanumeric code. As reflected in the following case, adding metadata will allow a proper management of the master tables of these administrative units:

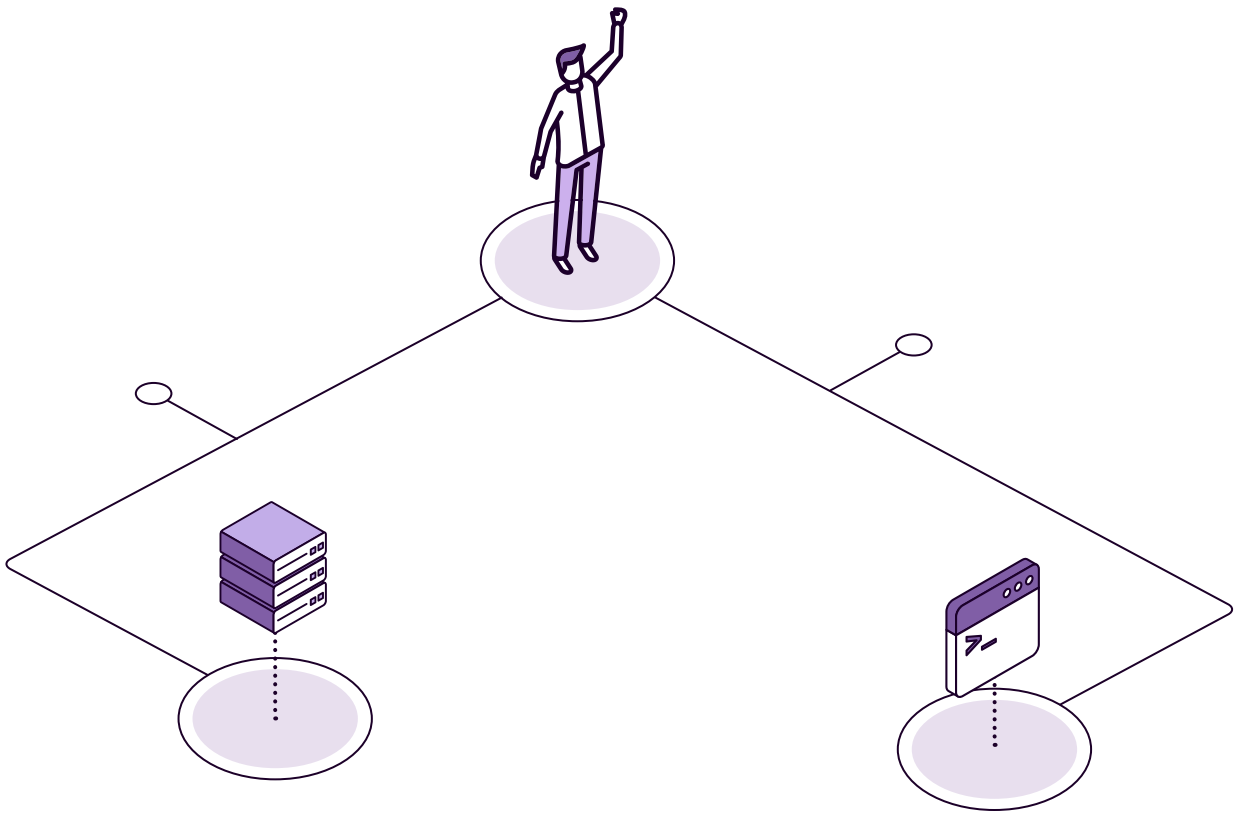
› *Example:*

- An office X is assigned a Y code and a Z description.
- Due to a competency or workload distribution decision, the office is split into two units.
- There are two options at this point:
  - Leave the Y code assigned to one of them, and create a new code and a new description for the spin-off.
  - Create two new codes for both offices, and, therefore, leave the Y code abandoned.

  Now, most likely the new offices, from a code point of view, will have to complete procedures that were being processed at the time of the change of office code. Therefore, one way or another, option a or b, the new codes will coexist with the old ones.
- In this order of ideas, it is justified to create two metadata items associated with each code: start date of validity of the code and end date.

It is also necessary to create the "routing" metadata, to route those automated messages, resulting from automated interoperability, when a sender uses an old code that can no longer accept new procedures. It can then be routed to the destination automatically. Obviously, there are many more possible types of metadata, but they will also have to be thought out and designed based on the problems and idiosyncrasies of each specific case.

Finally, it only remains to insist on the importance of these directories because, in an interoperable environment, they are one of the bases for an administration to exchange information in an automated manner. In fact, it would be impossible to create a unified entry registry, an electronic notification system, or a citizens' folder without a well-formed centralized directory of administrative entities, with interoperable codes and, desirably, standardized descriptions.



STORIES

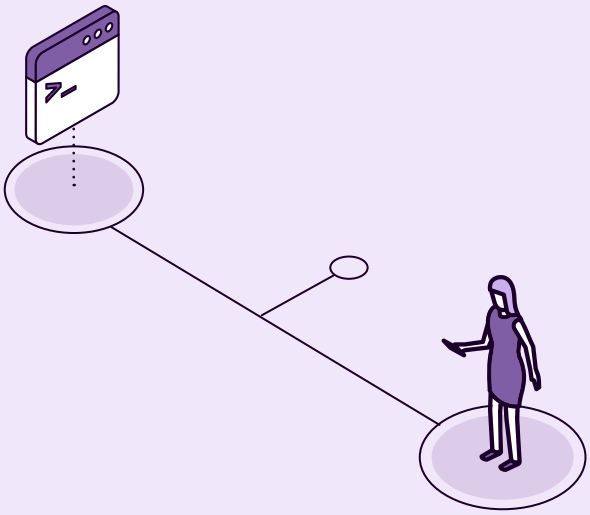
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Every semester, Sara has to send a management report to the Ministry of Modernization. Before, when this was done on paper, it was sent by physical mail to an address and an office that Sara knew. Now, thanks to the directory of administrative units, she only has to enter the code of the destination unit in the electronic documentation referral system, and the report arrives at its destination.

Entrepreneur
Ana

Ana wants to send some documentation to the unit that manages the granting of permits at the Ministry of Industry. How do you locate this unit and send them the information? She used to use the telephone, with little success in trying to contact them. Now this can be done electronically; as she knows the directory of units, since the information is published and accessible, Ana knows the exact code to send the documentation.



EXAMPLES

Click on each flag or icon to go deeper.

Uruguay
This is one of several countries that have unit directory systems. In this case it is based on *object identifier* (OID).

Spain
Information system of units and offices of public entities

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a directory of unique codes of public institutions? If so:
  - Does it contain all central government institutions?
  - Does it contain all the institutions of the entire government?
  - Is it integrated with the interoperability platform?

4.8.2 COMPANY DIRECTORY

In the same way as for the directory of public entities, there should be a directory of companies that contains the divisions or internal organization that the firms have, and that they themselves define. In general, in the case of businesses, there is a directory based on tax identification codes or similar, which is sufficient (because it is a unique code, known and shared by both the public and private sectors) for sole proprietors and small businesses. However, when the firm is medium or large, it may be necessary to have the different divisions that compose it identified and to ensure that these are known and homogeneous for all entities and the rest of the private sector.

The correct identification of companies becomes especially relevant from the moment they begin to offer procedures by digital means, not only inbound but also outbound. For example, if a company decides to inform the administration that its preferred channel for notifications is electronic, in which mailbox would the administration offices leave the notifications? It would not be possible if they were not correctly identified in a directory.

METADATA REQUIRED IN THE BUSINESS DIRECTORY

As in the case of administrative entities, the metadata associated with each of the codes, beyond the description, are of special relevance. It is suggested to use the following:

- Validity date ranges, in order to be able to operate with the codes with certain clarity.
- Specific metadata to represent the internal structure of a large company that needs to register more than one unit in the directory. This differentiation of functionalities can be generated through the creation of company structures by the companies themselves in the directory, and through the assignment of standardized competencies to each of these divisions.
    - *Example:* A large company may file documents using the main and general code of the root company but may have different units for judicial notifications or traffic notices.

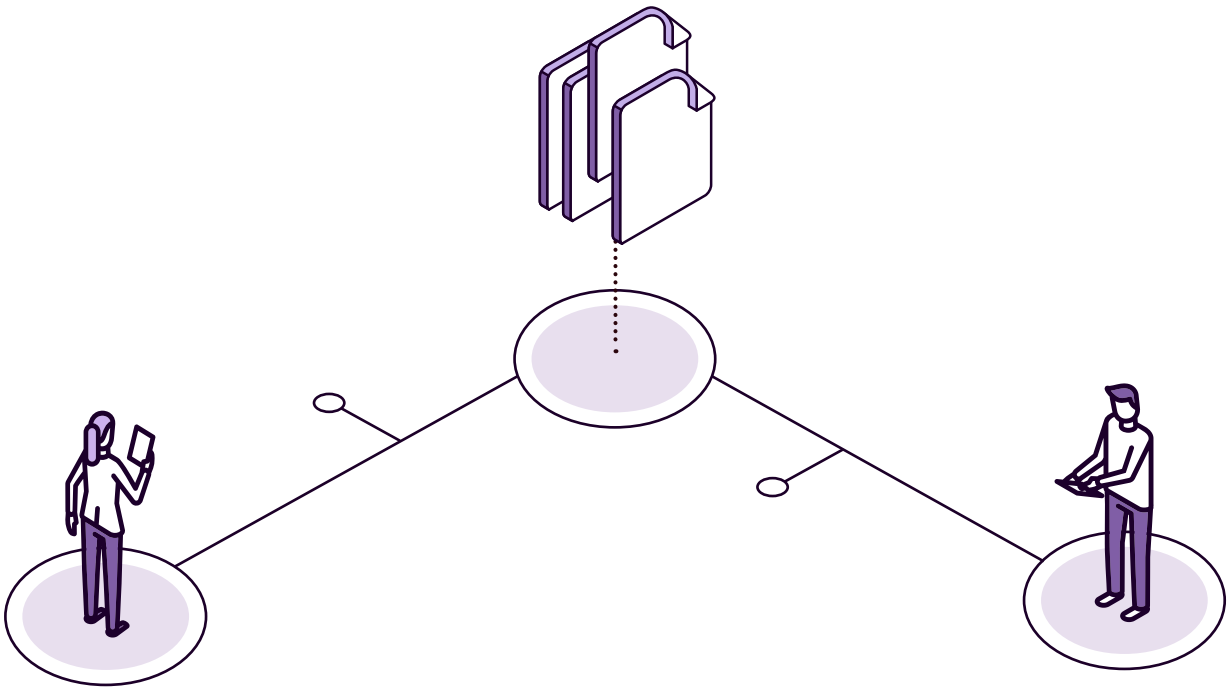
HOW DOES THE BUSINESS DIRECTORY WORK?

1. Normally, the beginnings of these unified and shared directories among all the units of the administration are in the tax or tax management units, since, naturally, they are the ones that first begin to relate with the companies and, therefore, the ones that create this directory in an operative manner.

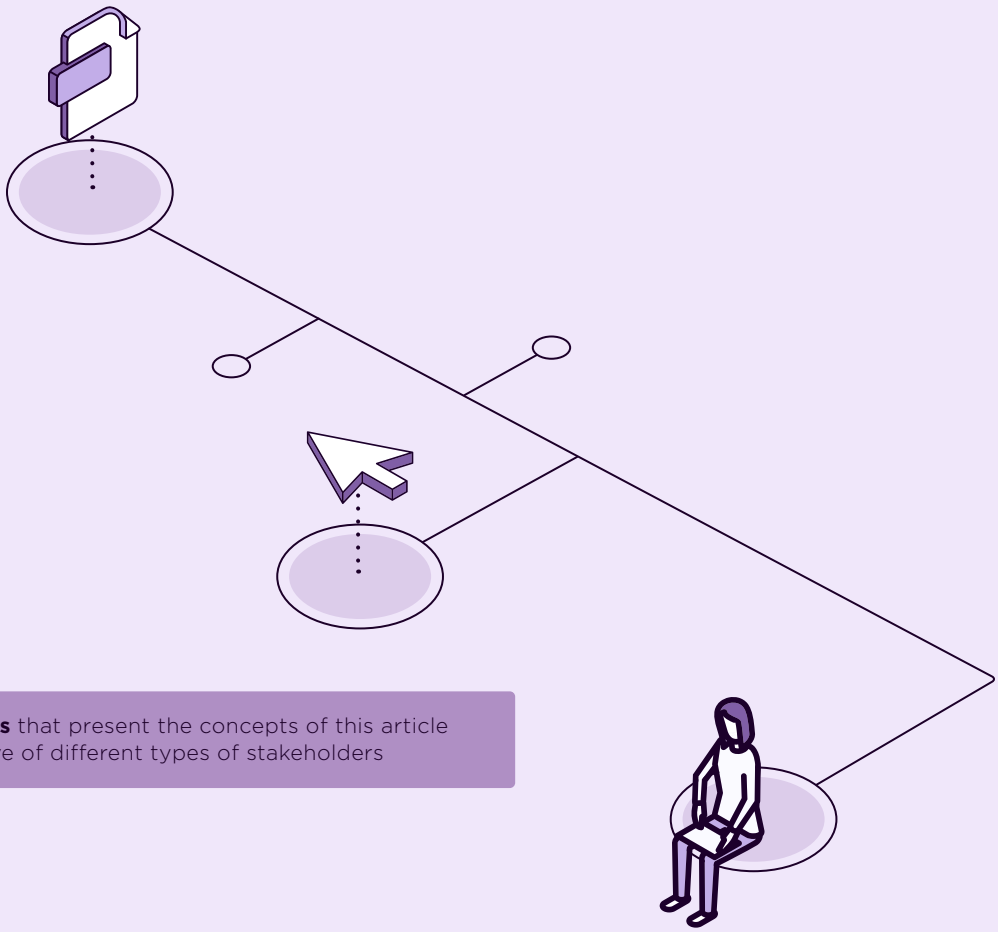
2. Through a web application, companies can manage contact data, mailboxes, departments, and so on. In this way, they generate their own relationship structure with public administrations.

3. Once the companies are well catalogued, by means of the same code in all the departments of the administration, it is possible to create joint spaces where these entities can have access in a unified way to all their information held by the public administrations:[39]

    - Files for each sector
    - Unified notification tray
    - Communication of change-of-contact information or tax domicile



39. Reference is made, of course, to the citizen's folder, but in a corporate version.



STORIES

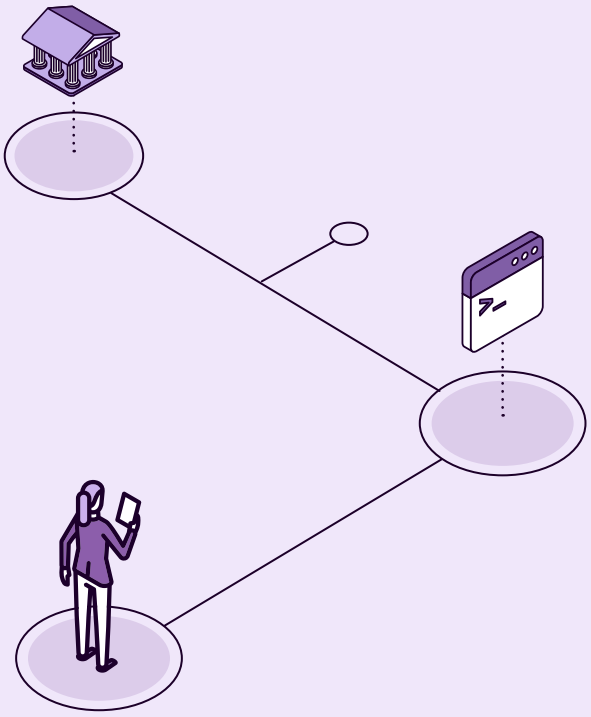
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Mayor's Advisor
Daniel

Daniel's municipality has just granted the building permit for a multinational clothing store. In the past, when this was done on paper, he would have sent the license to the store's office. Now that he has to do it electronically, the only information he has about the company is the tax identification code, so he fears that, by sending it to the central office of such a large company, the information will be delayed, because they have to process and manage the data, which then has to go from the capital to the municipality where the store is located, for the knowledge of those who applied for the license. Daniel would like to have a code that would allow the license information to be sent directly to the person who requested it.

EXAMPLES

Click on each flag or icon to go deeper.



Spain
Directory of Entities

United Kingdom
Company Directory

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a directory of unique company codes? If so:
  - Is it integrated with the interoperability platform?

4.8.3 ELECTRONIC REGISTRY OF AUTHORIZATIONS AND REPRESENTATIONS

Legal entities cannot act in the same way as natural persons in the traditional world; they require a representative. In the digital world this is complicated, in part, because, in addition to operating through a representative or natural person, especially when processed in an automated manner, there may be machines that perform actions on behalf of legal entities.

THE PROBLEM OF TRADITIONAL OPERATION VS. THE REQUIREMENTS OF THE DIGITAL WORLD

In general, in the traditional world, a number of persons, through authorizations granted by the company, may represent and act on behalf of the company. These authorizations are granted before a notary, commercial registers, or equivalent. The problem is that until now these authorizations have been based on legal prose, which must be interpreted in order to know whether a certain action can be taken by a person on behalf of the company. This has always meant the difficulty of carefully reviewing the authorizations, but in the electronic world the complexity increases, not in substance, but in practice: one is used to entering a web page, identifying oneself, and accessing or processing personalized information. Now, if the person is an attorney-in-fact, do we have to wait for a lawyer to review the authorizations associated with that person? This completely clashes with the uses and customs of the digital world, which is based on the immediacy of the transaction.

An information system is needed, then, that automatically knows if a person is a representative of a company and recognizes his or her associated powers. This is the only way that, once a person enters such a system, everything will work in a personalized way (to the human resources manager, personnel information; to the financial manager, tax information, for example) and he/she will be guaranteed that he/she can carry out the corresponding procedures on behalf of the company.

FOR ALL TYPES OF PEOPLE

It should be noted that although legal entities will be the main users, this system should be extended to individuals. In the case of legal entities, this is essential, since there is no other way of interacting with them, but for individuals it is very useful: from authorizations granted to friends or relatives to carry out procedures on behalf of someone else for reasons of experience (processing of a legal guardian for a child) or capacity (a husband granting power of attorney to his wife for an imminent operation), to situations of change of country (a son traveling), and many other situations.

INDIVIDUALS CAN BENEFIT SIGNIFICANTLY FROM EMPOWERING OTHER INDIVIDUALS TO CARRY OUT PROCEDURES ON THEIR BEHALF.

Therefore, this situation must be solved by means of an information system that stores the relationship between people and between people and organizations, which defines the representation, empowerment, or legal guardianship between these parties. This should allow the automated and simple management of administrative procedures, with the information available.

In all countries there will be a person in charge of paper-based authorizations, be it notaries, the commercial registry, chambers of commerce, etc. There is a possibility that this body will be the one to provide the information system for all institutions, but if this is not possible, the governing body of digital government will have to create the system, at least for public procedures. It is important to think from the outset about who manages the paper-based authorizations, if a parallel system is to be set up, since it may be a group that, due to a loss of power or income, may end up generating problems for the development of the project by ceasing to perform some of the functions it has performed up to now.

ELEMENTS OF THE PROXY INFORMATION SYSTEM

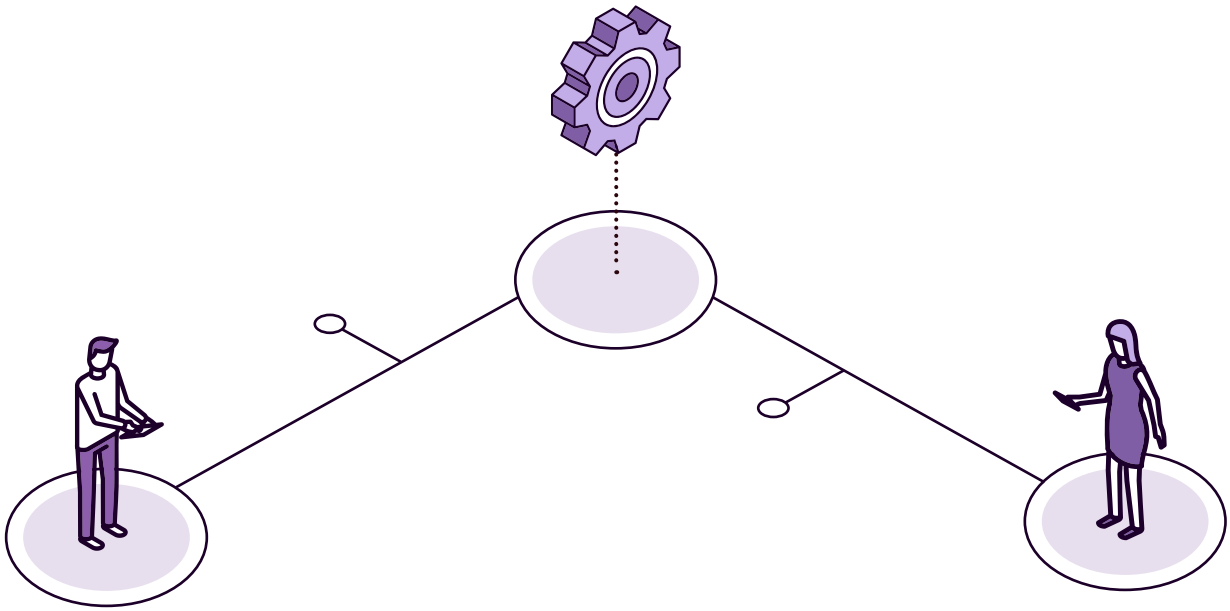
- Metadata to identify the scope in which the person has the power of attorney and to establish which procedures or types of procedures the person can perform.
- Metadata to identify the territorial scope. In large companies, there may be one representative for the capital city and, for example, three others for different areas of the country. Therefore, it is possible that the human resources manager in one state may not be able to do business in another.
- Metadata on the extent of power (e.g., without or with economic limit).
- Time metadata indicating the term of the power of attorney.
- Metadata on the type of transaction that the person can perform—for example, collect information but not initiate proceedings on behalf of the company, or initiate proceedings but not collect money from the company.
- Metadata that can be linked to a paper power of attorney, and a copy of the power of attorney, if applicable.

MANAGEMENT OF AUTHORIZATIONS

Authorizations should be managed from the multichannel service system, as well as from the single point of service through the web, at least in the case of citizens who are natural persons. In the event that a comprehensive service is not offered, which includes both classic paper and electronic authorizations, metadata, automatically processable and available to all public entities (at no cost or reasonable costs) by notaries or similar, and in any case to facilitate the digital transition, it would be interesting that, at least for MSMEs and individual entrepreneurs, this option is also provided in the multichannel service and single point of service through the web.

Something that is often closely related to the system of authorizations is the registry of administrative procedures, whose quality to classify and identify the procedures is essential so that the authorizations can be made effectively to the procedures and that everything can be processed automatically. It should be remembered that the objective is that someone identifies themselves on a website and can automatically carry out management in the area in which they are empowered.

THIS SYSTEM, WHEN AVAILABLE, IS ONE OF THE MOST VALUED BY CITIZENS AND COMPANIES.



STORIES

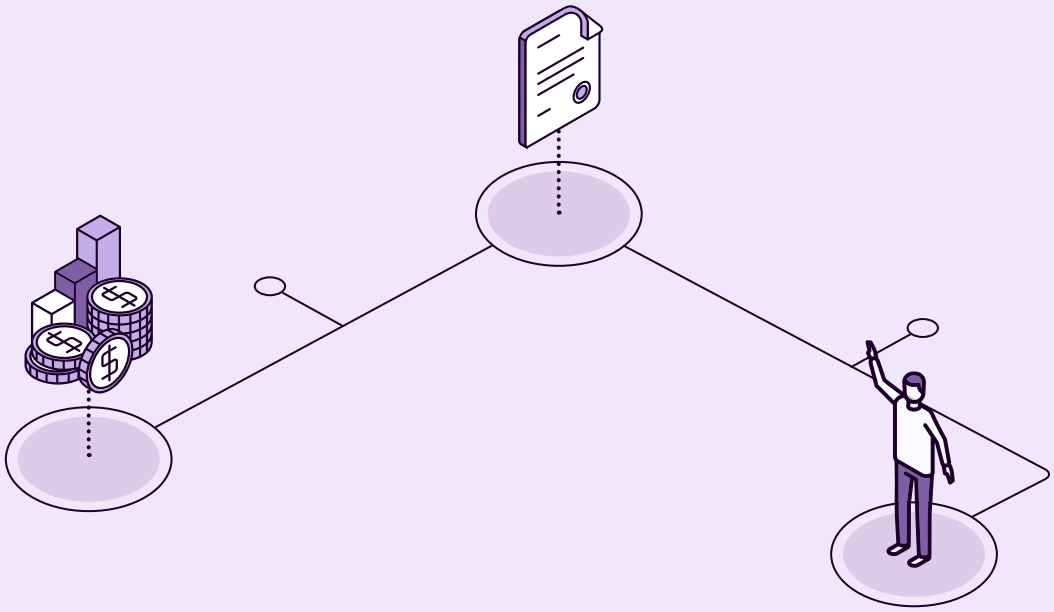
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Entrepreneur
Ana

Ana has Elena as her company's human resources manager. Although the electronic signature exists in her country, it is associated with the company in general, not Elena in particular. As she does not have the signature, all the procedures she has to carry out in her human resources area have to go through the management secretary's office. Ana would love it if there were a simple proxy system so that Elena could do the procedures in her area directly, although logically she would be prevented from seeing and managing other areas of the company.

Vice minister of health
Sara

Sara is responsible for health affiliation services in the ministry. Since the digitalization was implemented, she is delighted with the agility in the provision of services to citizens, but she sees a problem in the services to companies. They have to pass on the scanned authorizations, which in turn have to be checked by the organization's lawyer. Sara would like that, as in the case of citizens, the attorneys-in-fact could enter through the web and directly process without having to do any review of their authorizations.



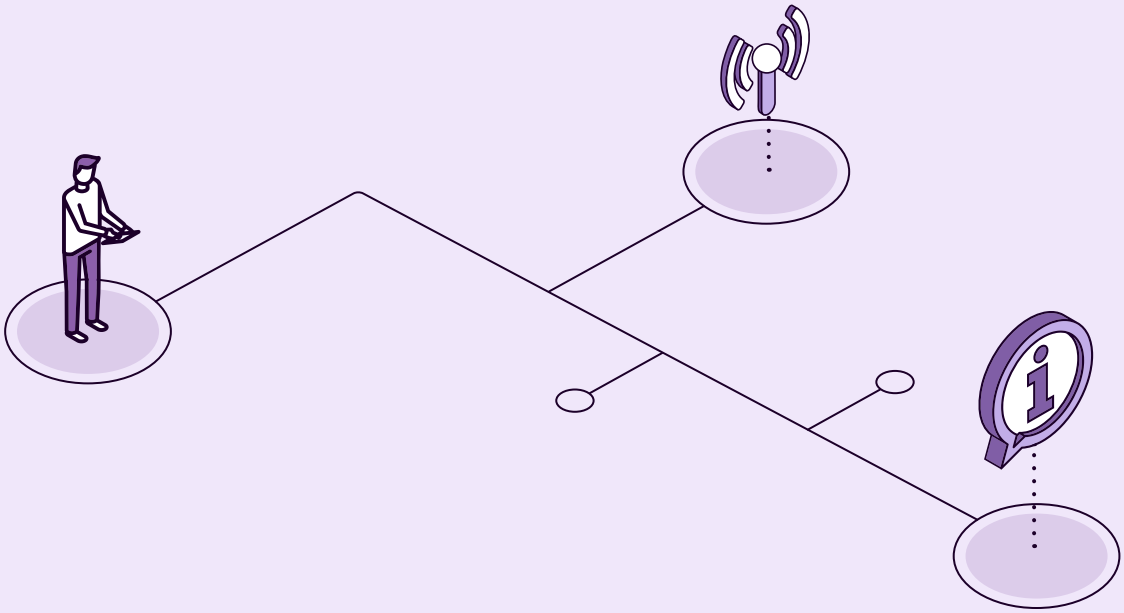
Citizen
Camilo

Camilo's brother is a specialist in tax management, which is particularly complicated for him. He has recently learned about the implementation of the electronic proxy registration service, so he has given the power of attorney for his brother to file the tax returns on his behalf. He is now much calmer, as he knows that his tax return will be correct. He is also happy because he has been able to deduct some of his daughter's expenses, which he did not know he could do, so the operation has been more beneficial than in previous years.

EXAMPLES

Click on each flag or icon to go deeper.

Spain
Electronic Register of Apoderamientos



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there an electronic registry of authorizations and authorizations? If so:
  - Does it include facilities for individuals?
  - Does it include facilities for legal entities?
  - Are more than half of the central government entities included in the registry?
  - Are all central government entities integrated in the registry?
  - Are more than half of the government-wide entities in the registry?
  - Are all government-wide entities integrated into the registry?
  - Are you connected to the multichannel care system?
  - Are you connected to the citizen folder?

4.8.4 REGISTER OF OFFICERS

The register of authorizations of company representatives has its equivalent in the public sphere: the register of civil servants. In fact, the same information system could be used, since both the functionality and use are very similar, if not identical. It is the database of civil servants and their attributes, in relation to the actions they can perform as such and on behalf of their public agency.

JUST LIKE THE REGISTER OF COMPANY AUTHORIZATIONS, THE REGISTER OF CIVIL SERVANTS SHOULD BE OPEN ACCESS FOR ALL PUBLIC INSTITUTIONS.

However, the analysis of this registry has been separated from that of empowerment because—in addition to solving the problem of civil servants, which is not usually related to commercial or business powers—it can sometimes have legal and implementation differences with respect to the private sector. In any case, the problem is the same: to enable public officials to carry out official procedures and actions in the digital environment. The system may also allow certain officials to perform certain activities by virtue of their position. For example, officials in a customer service office can carry out procedures on behalf of citizens; those who occupy certain positions can validate certain documents, etc.

Basically, it is a database that relates people with profiles or roles (and, for internal use only, their contact data), and these, in turn, with organizations. It should be noted that a person can have several profiles and even several relationships with different entities, and the information system has to contemplate this possibility.

KEYS TO THE REGISTRY OF OFFICERS

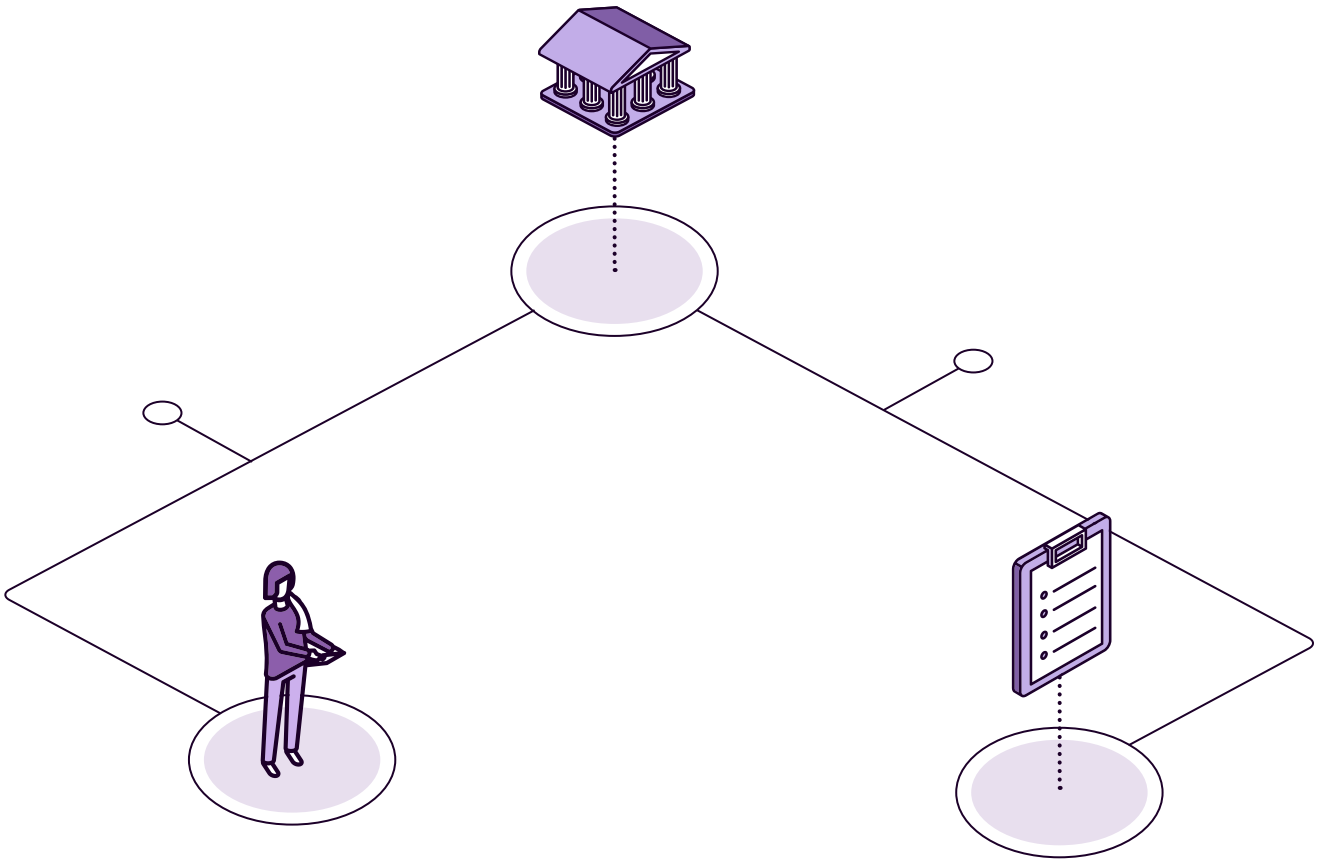
- **The system must be updated:** Ideally, it should be integrated with other official databases of civil servants in the country, so that if someone leaves his or her post, he or she automatically loses the permissions and capabilities that the system granted him or her. In this sense, both automatic and manual information capture and provision interfaces are required.

- **Use some of the country's basic services:** The civil servant registration system should make use of electronic identification and signatures to provide legal security for transactions, authorizations, and terminations.

- **Use the unit directory service:** To clearly and without possibility of error associate each staff member to the organizational unit to which he/she belongs. Be careful and emphasize that an official may be in several organizational units or entities at the same time, and that he/she may have a different role in each of them.

- **Integration with the procedures registry:** This makes it possible to establish clearly and without error which procedures can be carried out by a given officer and which cannot, in cases where this is required.

- **Mass and general use and consumption:** Virtually any information system that has to rely on a staff member, and especially common services, should be integrated with the registry so that access management is securely delegated to this common service.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo is overwhelmed because the subsidy that would allow him to keep his daughter in school expires soon, and he does not know how to access it. Fortunately, in his municipality there is a multi-channel service, so he goes to the office and the official carries out the application for the Ministry of Education grant on his behalf. The official explains to him that he is authorized in a centralized registry to carry out this procedure on behalf of citizens. He tells you that you have to sign an authorization for him to carry it out, but not to worry because he will do it right then and there and ensure that the process is done on time.

Entrepreneur
Ana

Ana has to give her secretary the power of attorney to carry out procedures with public bodies. Specifically, the task consists of collecting notifications and communications addressed to the company she owns. She goes to her neighborhood office and takes advantage of the service that a colleague has told her about, whereby there are public officials who can record in the power of attorney register the authorizations that the firms provide to certain individuals. When she carries out the procedure, Ana is amazed at how in a short time, without the need for paperwork or procedures involving third parties, her secretary can collect the notifications and communications addressed to her company.

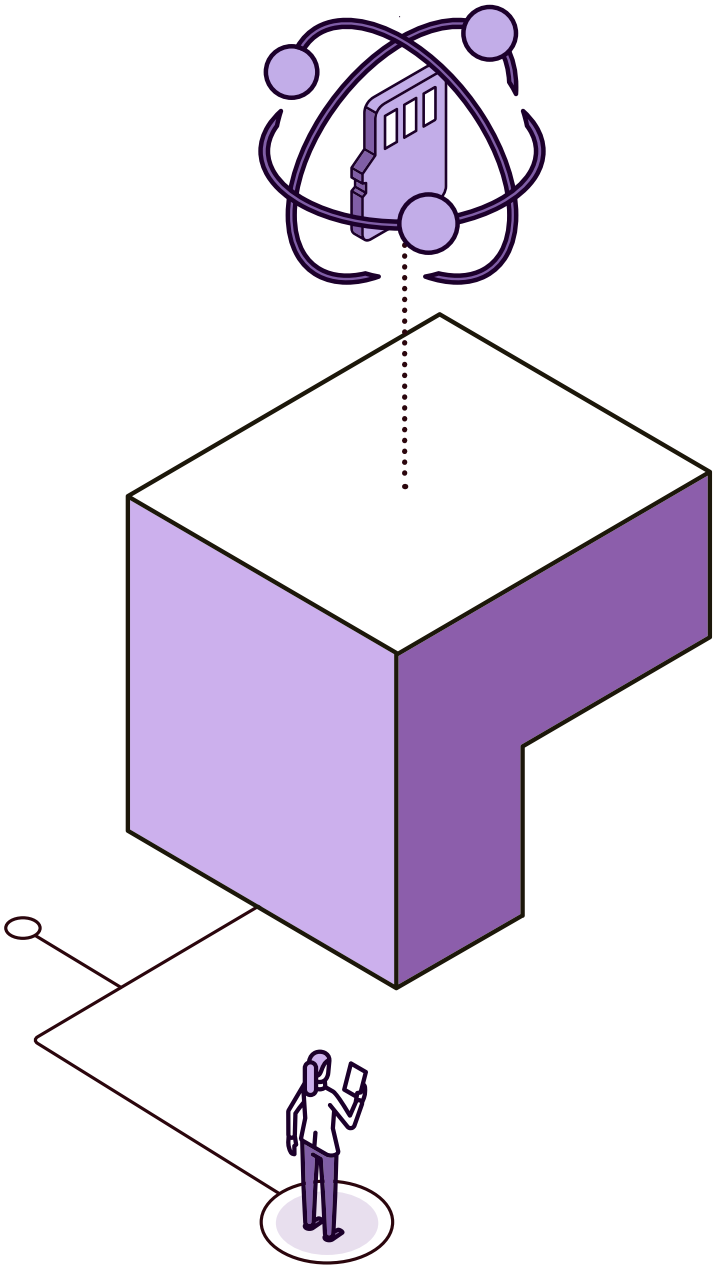
Mayor's advisor
Daniel

Daniel has been appointed responsible for an entire administrative unit of the city. The same day that this promotion becomes effective, he accesses the intranet and sees in his file that the role has been changed and that he appears as a unit manager. Thanks to this, he accesses the service portal of the institution in charge of electronic administration and sees that he can, in his new role, register his unit in multiple ICT services offered by this organization. He will now take a closer look at all the services, but he immediately joins the interoperability platform as a service, as well as the electronic document exchange system, making his unit paperless in most cases.

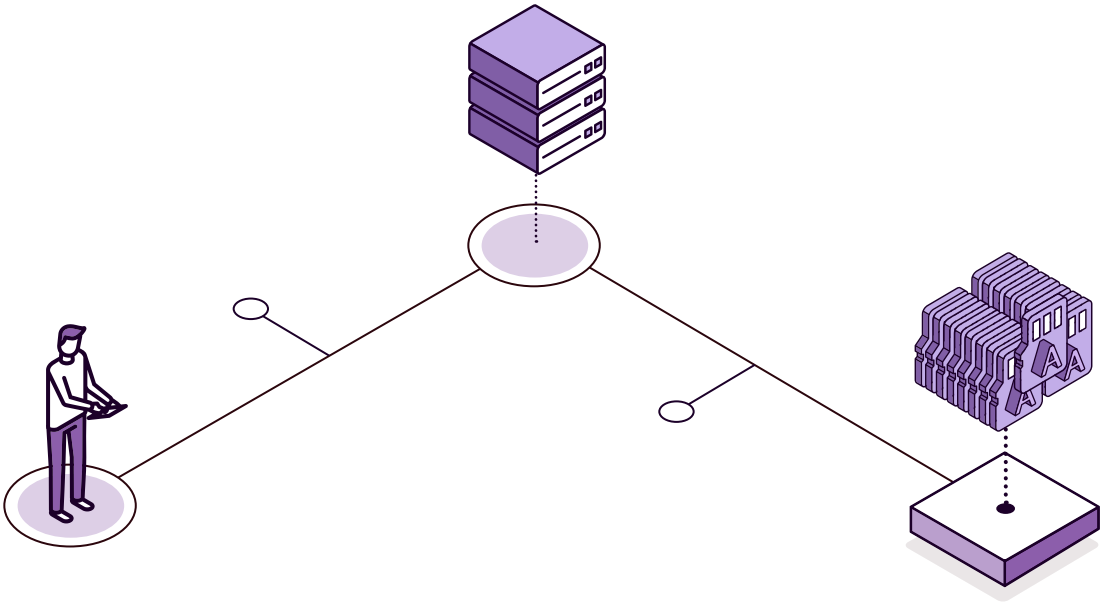
INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a registry of officers in database format with their associated roles and attributions? If so:
  - Does it include officials from more than half of the central government entities?
  - Does it involve officials from all government entities?
  - Is it integrated with the procedure catalog?



4.9 Data



For many years now, the whole world has been aware that data has become the oil of the new information age. However, data alone is nothing more than an infinite accumulation of bits that, without intelligence, do not provide value in and of themselves. The power of information comes when these data are given a layer of order, of transformation, of intelligence: when they are grouped with specific rules, when they are mixed in a defined way. In short, when intelligence is added to the data, it becomes information.

It is precisely the information that, represented in different ways and for different purposes, can provide value in different areas. For example, a set of georeferenced data can provide a special value focused on the territoriality of a specific area. In turn, the same data, correctly structured, can be useful for automatic processing by other information systems or, presented as a dashboard with graphics, can provide guidance for decision-making in a specific situation.

KEY ELEMENTS THAT A COUNTRY'S DATA POLICY SHOULD STIPULATE

- Different dimensions such as formats, exchange, publicity, exploitation, and validity, so that the policy is, as far as possible, common to all public bodies.

- Sufficiently flexible spaces so that each agency can adapt the policy to the reality of its own data.

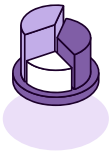
    - *Example:* The basic information describing a piece of data (originating agency, date of creation, policy version, etc.) must be standardized by the policy for all agencies equally, but, on the other hand, the data for a specific field must have a certain flexibility of description. Thus, health data will be semantically described by the Ministry of Health, and education data by the competent agency.

- A minimum of standardization in the semantic description of the data, in order to ensure proper interoperability between agencies, as well as compatibility in order to be able to mix data from different sources in the same dashboard or scorecard.

- The existence of a common repository for data loading and exploitation, either in the form of open data, georeferenced data, or dashboards. The idea is that, in a centralized way, all public bodies, under the same rules of the game established by the data policy, can load in a single repository the data that will be exploited and that, with the appropriate permissions in each case, can be accessed by the different systems explained.

The following are the open data systems, scorecards and exploitation, and georeferencing. Each of them will go into detail on the particularities and needs in order to add value to the country's global data system.

National open data system



Scorecard and statistical exploitation

Georeferencing system

Document management system

4.9.1 NATIONAL OPEN DATA SYSTEM

The objective of opening and publishing the data of public bodies is that they can be used and reused, and for this it is essential to know about their existence. Models in which each entity publishes its data individually, in different formats and through different technologies, are not scalable, since it is not realistic for a citizen or a company interested in data reuse to browse hundreds or thousands of web pages, all of them diverse, with varied formats, to find data that may be of interest to them for reuse.

In the same way that it is important to have a centralized system to facilitate data consumption and reuse, it is also important that the system allows those entities that, due to their size or lack of technical capabilities, cannot have their own data publication and exploitation system to generate data sets in a simple way. According to this premise, the information system should make it easier for these types of entities to publish and facilitate the consumption of their data, even if they do not have a developed technological infrastructure, based on this centralized data opening system as a common country service.

In view of the above, it is essential to create an information system that allows the effective exploitation of the data released by the entities, in a centralized manner, with homogeneous search and exploitation criteria.

THE NATIONAL OPEN DATA SYSTEM FACILITATES BOTH THE CONSUMPTION AND PUBLICATION AS WELL AS THE PUBLICITY OF DATASETS THAT PUBLIC ENTITIES, OR COMPANIES, PUBLISH FOR REUSE IN THE COUNTRY OR IN THE WORLD.

Although we generally speak of a portal on a web page accessible to citizens and companies, it should be noted that the information system should not be restricted to this. Ideally, there should also be standardized interfaces for the consumption of the different data and their updates, so that reusers can consume them and be aware of the updates, without the need for a person to access a web page every day and check if there are any new developments.

On the other hand, and in order to facilitate data reuse in all public entities (and the private sector, if applicable), the portal will also have, apart from the public consumer interface, a restricted interface for small public institutions to publish their datasets. Thus, this technological system that supports data reuse must be compatible and aligned with the country's data strategy, as well as with the existing open data regulation.

BASIC ATTRIBUTES THAT AN OPEN DATA PORTAL SHOULD HAVE

- Have an aggregator system for the datasets made available to reusers.
- Be easy to use and navigate.
- Have a search engine that effectively allows the user to find the data sets he/she is looking for.
- Reflect the information associated with the datasets that is relevant to know, without the need for downloading, whether or not they are of interest to the reuser.
- Allow data to be downloaded in multiple formats. In addition to data that can be visually interpreted by people, it is important to provide the possibility of downloading data that can be automatically processed.

SPECIFIC INTERFACES

All of the above is related to use and consumption, but the national system must also facilitate that those public entities (and ideally companies) that have data to publish can do so without the need to have their own associated technology. Therefore, the system will have a specific interface for these entities, characterized by the following capabilities:

- Allow identified users to upload raw data, in formats that are simple for any user (e.g., spreadsheets, which are commonly used).
- Guide the user to upload the metadata associated with the uploaded dataset (to facilitate its localization and exploitation).
- Make various formatting changes as needed. These can range from changing from spreadsheet, text, or printable documents, to XML systems that facilitate automated exploitation by including user-loaded or automatically generated metadata, such as updates, loading time, modifications with respect to preexisting data, author and organization that generates the dataset, etc.

AUTOMATED COMPLEMENTS

This data visualization for consumption and the simple loading system through a web page must be complemented by automatic systems that allow:

- **Automated consumption of information:** Here it is important to be able to inform reusers automatically of updates or additions to the datasets in which they are interested.

- **Provide interfaces for data producers:** In this way, those with the appropriate technical capabilities can upload the information and data generated without the need for manual uploading work. They will simply connect their databases or the systems that generate them to the national open data system, thus enabling real-time and automated updates and extensions, which saves the workload for these entities.

FEDERATING PORTALS: AN INTERESTING OPTION

Typically, countries have multiple public entities, and it is common for some of them to have their own open data system, given that the institutional structure of the country allows them to do so. If this is the case, both the institution in question and the reusers can benefit from federating the various existing portals with the national system, as a public entity has its own portal and in turn all the datasets are also in the national hub. This allows an improvement in the localization of data and, therefore, greater possibilities for reuse and generation of added value.

Similarly, it is interesting that the national open data portal can federate its data to international organizations or alliances. In this way, such information is concentrated, and its reuse beyond national borders becomes possible.

DISSEMINATION AND PROMOTION OF OPENNESS AND REUSE OF DATA

Finally, it is important to raise awareness of the importance of the culture of openness and reuse of data. To this end, it is useful to:

- Give examples of use;

- Present success stories of reuse companies that have achieved successful business models by exploiting available data;

- Share the reuse experience of the public entities and sectors themselves;

- Organize events, awards, and other activities that encourage openness and data use.

OPEN DATA AND REGULATION

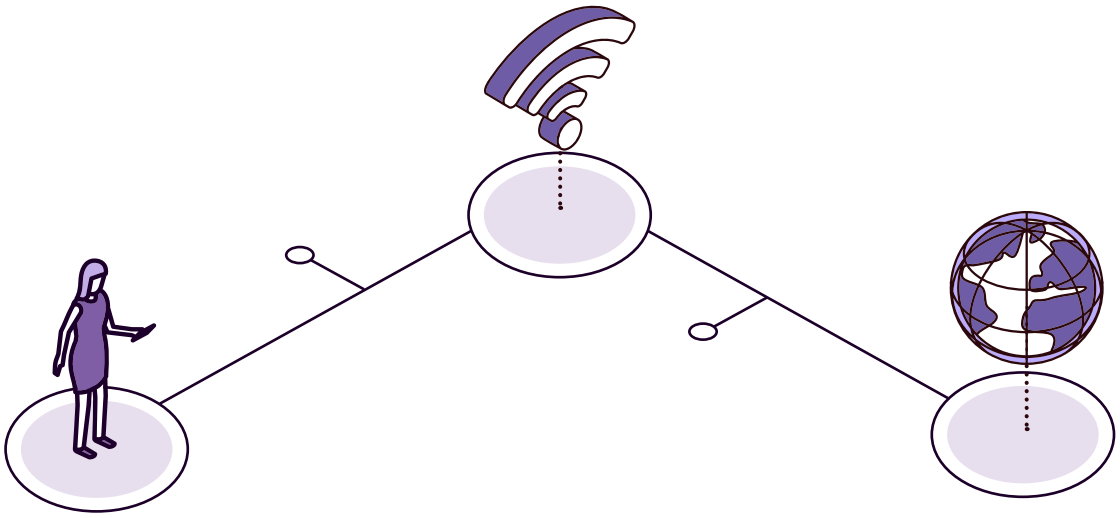
The open data portal is related to both the open data regulation and the country's data strategy. Its operation and capabilities have to be in line with the regulation and the strategy but, as in other cases, without being completely dependent on them.

A country can have an open data portal without an open data regulation or a general data policy for the nation. It is complex the other way around; there will hardly be an open data regulation or policy without a portal to access and exploit the data according to the licenses for its use.

The portal and its relationships also have a link with the document and electronic file policy, since in many cases these, if well formed, can be published as data in whole or in part, and their information can be exploited (always respecting the protection of personal data).

On the other hand, the portal will also be closely related to certain common services linked to data policy, which can make the use and exploitation of open data much more effective. Thus, it should not be underestimated that if there are certain common country data (directory of units, physical addresses or standardized georeferencing, directory of procedures, data models with semantic capacity, etc.), the exploitation of the portal data will be much more effective and will have a greater impact.

THE EXISTENCE OF THE PORTAL SHOULD BE CONSISTENT WITH THE SINGLE GOVERNMENT PORTAL POLICY AND COMPLY WITH DEFINED ACCESSIBILITY AND USABILITY REQUIREMENTS.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Entrepreneur
Ana

Ana is delighted with the new open data portal. Until now she had to go to different web portals of the different public entities to find information on projects open for bidding. With the single government portal, she can access all the information on tenders in one place and in a homogeneous way, which makes her work much more effective.

Vice minister of health
Sara

Sara has always believed in open data. Since being part of her country's open data committee, she has realized that due to the lack of homogenization of health databases, the information was not useful for doctors, companies, or researchers. Based on the lessons learned in the committee, she is adding data and standardization to health information, which has been very well received in the medical community.

Mayor's advisor
Daniel

Daniel wants the data published by his municipality to be used, as it took a lot of effort to make it public to the citizens. However, many of the potential users do not even know that the information is available. Thanks to his country having a new open data system, which has a portal that integrates information from the central government, states, and municipalities, his municipality now appears among the first in the *rankings* in terms of published datasets, as well as in terms of their effective use.

EXAMPLES

Click on each flag or icon to go deeper.

Colombia
Open data

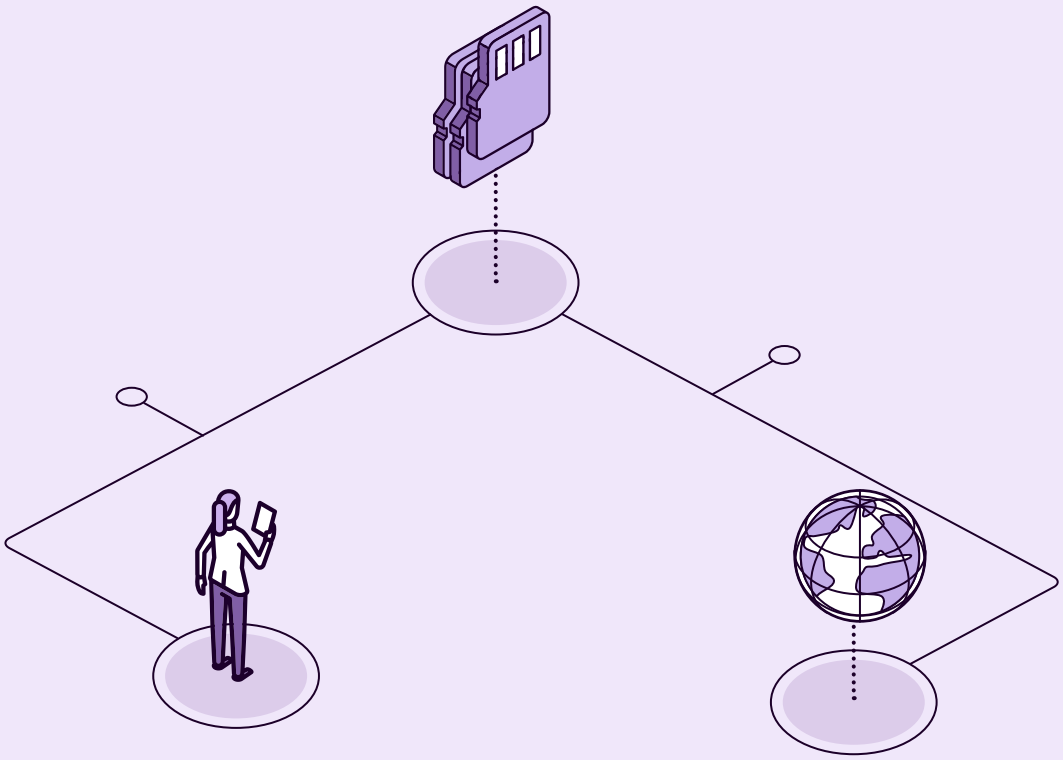
Spain
Decalogue of the public sector data reuse

Chile
State centralized open data repository.

Uruguay
Open data catalog

Spain
Open data initiative of the Government

Mexico
Open data



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Does a national open data system exist? If so:
  - Do you have standards for data structure and quality?
  - Do you have interfaces that allow easy consumption by data reusers?
  - Do you have an interface that facilitates the publication of data by public institutions that do not have their own systems?
  - Do you have a search engine?

4.9.2 SCORECARD AND STATISTICAL EXPLOITATION

The dashboard system consolidates data from different government sources and facilitates statistical processing and visualization. It is offered as a shared service for those public entities that cannot afford such a system, or for cases where the institutions in question can afford it but are interested in having the data and its exploitation in a single system to get more out of the reports. In this sense, a single system and data repository can serve three different groups:

- Public executives, for whom aggregated data and quick-to-understand visualizations are a priority
- Midlevel public managers, who are offered aggregated data and visualizations, but also access to microdata on specific cases
- The general public, to whom only aggregated data and visualizations are offered, along with tools to facilitate their own analysis.

BENEFITS OF BALANCED SCORECARD SYSTEMS

Although these information systems tend to have high costs and require specialized personnel to operate them, they have several advantages:

- They guide decision-making. Without data, it is like navigating without a map. The information can be especially useful for detecting gaps and applying the studies and results to eliminate the country's digital divide, or to propose policies or actions to minimize it.
- Offering these systems as a shared service provides access to public institutions that would not be able to generate this information on their own. It also facilitates the consolidation of a greater number of information sources, which enriches the possibilities for analysis.
- It allows citizens to "play" with the information, even with visualizations, without being experts in data manipulation. This is why these dashboard systems are so closely related to open data or transparency systems.
- They can be the basis for the exploitation of *big data* information, key to artificial intelligence, depending on the scope of the project.

THESE PROJECTS WORK IN CONNECTION WITH THE COUNTRY'S GEOREFERENCING SYSTEM, SINCE THIS WAY OF PRESENTING INFORMATION IS VERY USEFUL FOR EXPLOITING IT.

INTERDISCIPLINARY AND SHARED TEAM

In general, in order to take advantage of these systems, it is necessary to create a team of experts in different areas, such as statistics, visualization, information exploitation, etc. This group will work on a business intelligence system (in a broad sense, it can include *big data* and artificial intelligence), usually based on commercial *software*, since these systems are usually based on engines and technologies that are not always available through open systems, or that are complicated to develop from scratch.

In all cases, the cost of these systems and the complexity of their use make it much more interesting to have a shared dedicated team for all institutions than to carry out individual projects, which due to their complexity can take a long time or end in failure, multiplying the costs for the public administration. Moreover, a standard licensing model is usually not provided, among other reasons, because a user of an institution would not normally obtain the necessary benefit from the system to justify the cost of a license.

REGULATED USE

Normally, the source of the information is its place of production. That is, health data should come directly from the Ministry of Health, education data should come directly from the Ministry of Education, and so on, and each will have its own automated connection to the dashboard system to update the information available in real time. It is therefore essential that the system be accompanied by a data exploitation policy that establishes rules and procedures on aspects such as:

- Data access;
- Quality assurance;
- How data is kept up to date;
- Charging modalities;
- Periodicity;
- Predefined dashboards and reports.

Therefore, in many cases it is essential that the project team proposes interoperability or information exchange schemes with the interested entities, in order to carry out complete statistical exploitation projects that do not entail a high cost for the organizations and that have certain guarantees of success, as they are expert participants in the system.

Likewise, this system must have an access control that allows opening the access to officials, according to their needs and attributions, or to the general public. Thus, the public manager of institution X will only be able to access the microdata of his own institution, while the officials of the president's office will have wider access.

Hand in hand with access control is personalization. As this is a shared service for all institutions, it is essential that each one has its own entrance, where it can see, without any loss of detail, all the information relevant to its specific context.

THE DASHBOARD SYSTEM IS RELATED TO ALL THOSE SYSTEMS THAT CAN BE SOURCES OF DATA.

SOME IMPORTANT RELATIONSHIPS OF THE SCORECARD SYSTEM WITH OTHER SYSTEMS

- **With the open data system:** It is useful in two ways
  - To be able to exploit open data with analytical capabilities.
  - To dump analytics or statistics generated through the dashboard system into the open data system. In order for information reusers to take advantage of this data, it is also common for there to be connections to the brokerage platform or its equivalent.
- **With all those systems that improve semantics:** Data analytics and exploitation will be more efficient depending on the quality of the data. A very important aspect in this regard is normalization, to which the semantic capabilities of the data must be added. Thus, the dashboard will have a special relationship with
  - The unit directory;
  - The directory of procedures;
  - The directory of physical addresses;
  - The georeferencing system;
  - Semantic data models, among others.
- **With the directory of employees:** For use by employees in their handling of sensitive information. Officials must be authorized according to profiles for access to nonpublic information.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo's brother has always been interested in the new technologies used by the government. Thus, he likes to be informed about the progress of digitization in the country. That is why he knew that there was open data, but his interest was not enough to worry about exploiting it. Now, thanks to the dashboard—a powerful statistical exploitation system where all the information related to the progress of digital government is published—he can see the status of the implementation of the interoperability platform in the municipalities through maps, or graphs of growth in the use of digital identification.

Entrepreneur
Ana

Ana is part of a business association that is responsible for promoting the digital transformation of her country. For her, it is of vital importance to have detailed and real-time information on the use of e-government systems. Without this information, the association would not be able to put pressure on the public institutions that are lagging behind, nor would it be able to detect best practices in order to replicate them.

Vice minister of health
Sara

Sara is one of the advanced users of the government's statistical exploitation systems, and she is delighted that it is offered centrally; not only because it allows her to dedicate her ministry's resources to improving health, which is her goal, but also because, by having the system common and centralized, it is much easier to cross-reference data with information on population, citizen security, etc. Having all that information at your fingertips (literally, since you can access comprehensive and sensitive data from your cell phone) allows you to know firsthand the health situation when visiting different territories and to plan more efficiently the allocation of your ministry's resources.

Mayor's advisor
Daniel

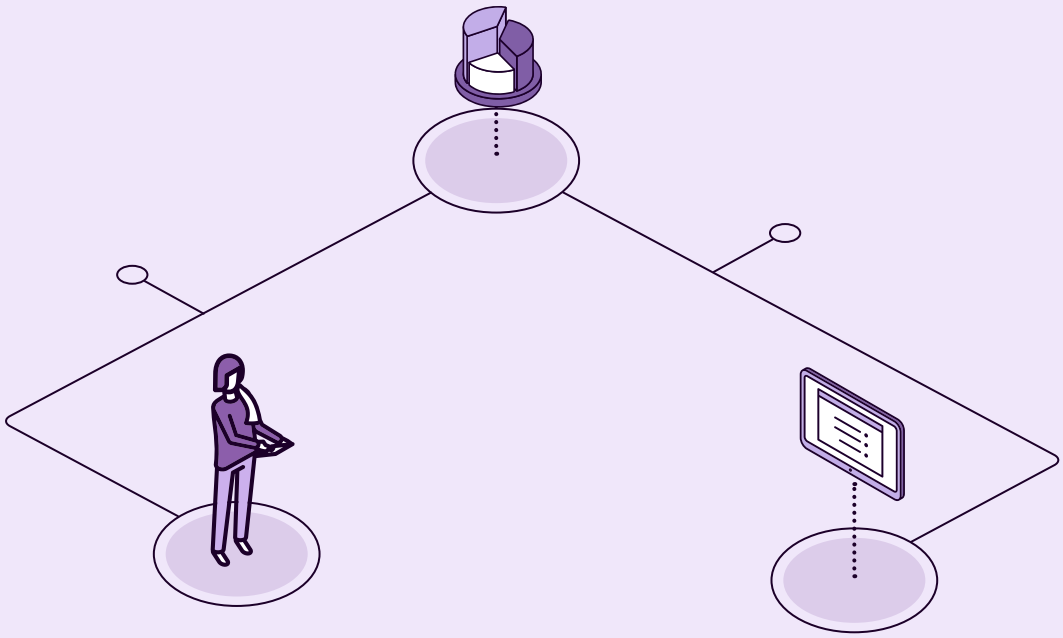
Daniel has always advocated for his municipality to use the resources offered by the national digital government office. His municipality uses the country's electronic identification and signature system and the interoperability platform and provides services through the national citizen folder. One of the conclusive aspects of his decision has been that by using the central platforms, he has access to view statistical usage data. In other words, he knows in detail what has been the use of these services in his municipality and can directly exploit all the result.

EXAMPLES

Click on each flag or icon to go deeper.

Spain
Area Citizen Attention and Business

Portugal
The numbers of Justice



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a dashboard system or similar, as a common service that can be used by any public institution? If so:
  - Does it have an access control system that allows opening access to officials, according to their needs and attributions, or to the general public?
  - Is technical support offered to facilitate the use of the system by other public institutions?
  - Is it integrated with the open data system?
  - Is it connected to the data brokerage platform?
  - Is the system in use in more than 50 percent of central government institutions?
  - Is the system commonly used for government reports and press releases?

4.9.3 GEOREFERENCING SYSTEM

The capabilities of georeferencing systems are very broad:

- They make it possible to visualize and make the activities or results of public entities more transparent.
- They are a useful tool for trend detection.
- They contribute to decision-making by senior management.

Therefore, it is necessary to have a system at the service of all institutions that cannot afford it, for economic or technical reasons, so that they are able to generate, count, and exploit georeferenced information, including graphical representation by layers.

GEOREFERENCED INFORMATION IS OF VITAL IMPORTANCE, EVEN FOR LOCAL GOVERNMENTS, TO DEFINE EVIDENCE-BASED PUBLIC POLICIES BASED ON GEOLOCALIZED DATA (E.G., CRIMES BY NEIGHBORHOODS, POLLUTION LEVELS BY AREAS, ETC.).

WHAT SHOULD A GEOREFERENCING SYSTEM HAVE?

- A scalable georeferencing engine that allows its use by different entities, without compromising the resources of the unit providing the service, neither in processing capacity nor in economic issues.
- A mechanism for data upload by public institutions. In this case, given the objective, apart from the usual uploads by automatic means, it will be necessary to facilitate that through a web interface and simple connection—for example, uploading flat files and/or data sheets—someone without georeferencing capabilities uploads information for georeferenced presentation.
- Systems for translating addresses (which is often the only thing available to the agency) into georeferenced information. Addresses must be in a standard format that allows their translation. In addition, as far as possible, as much data as possible should be georeferenced.
- A map validated by the country's highest authority, in which all administrative boundaries are well represented and agreed upon by the different levels of government. It is also often necessary to complement the georeferenced information consumption capabilities of the system, in order to make it easily integrated and exploitable by the entities that use it.

RELATIONSHIP WITH OTHER SYSTEMS

- **With the open data system:** As in the case of the dashboard system or the analytics system, the georeferencing system has a dual relationship with open data systems:
  - It allows the geospatial publication of data, which in many cases generates much richer and more comprehensible information.
  - It allows georeferencing data to be included in many of the datasets that in principle do not have georeferenced information, something that should be released to be exploited by reusers (for example, indicating pharmacies that are close to a specific point).
- **With the nation's data policy:** It would be ideal if the georeferencing system would allow standardization and normalization of georeferenced data, so that its use by any public or private organization would follow the standards set by it.
- **With the management system and staff profiles:** The system, especially for advanced uses, will have a cost, so access to it will have to be managed.
- **With the single government portal:** To georeference useful information for citizens, from offices to ministries, among others.
- **With the citizen folder services:** To provide specific information oriented to each particular case, and to provide data of interest, at a given time, in relation to the citizen's information.

THE AVAILABILITY OF AN ADVANCED GEOREFERENCING SYSTEM WILL MAKE IT POSSIBLE TO OBTAIN MAPS, INDICATORS, AND A SET OF VISUALIZATIONS THAT ARE MUCH MORE USEFUL FOR CITIZENS, COMPANIES, AND ORGANIZATIONS.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

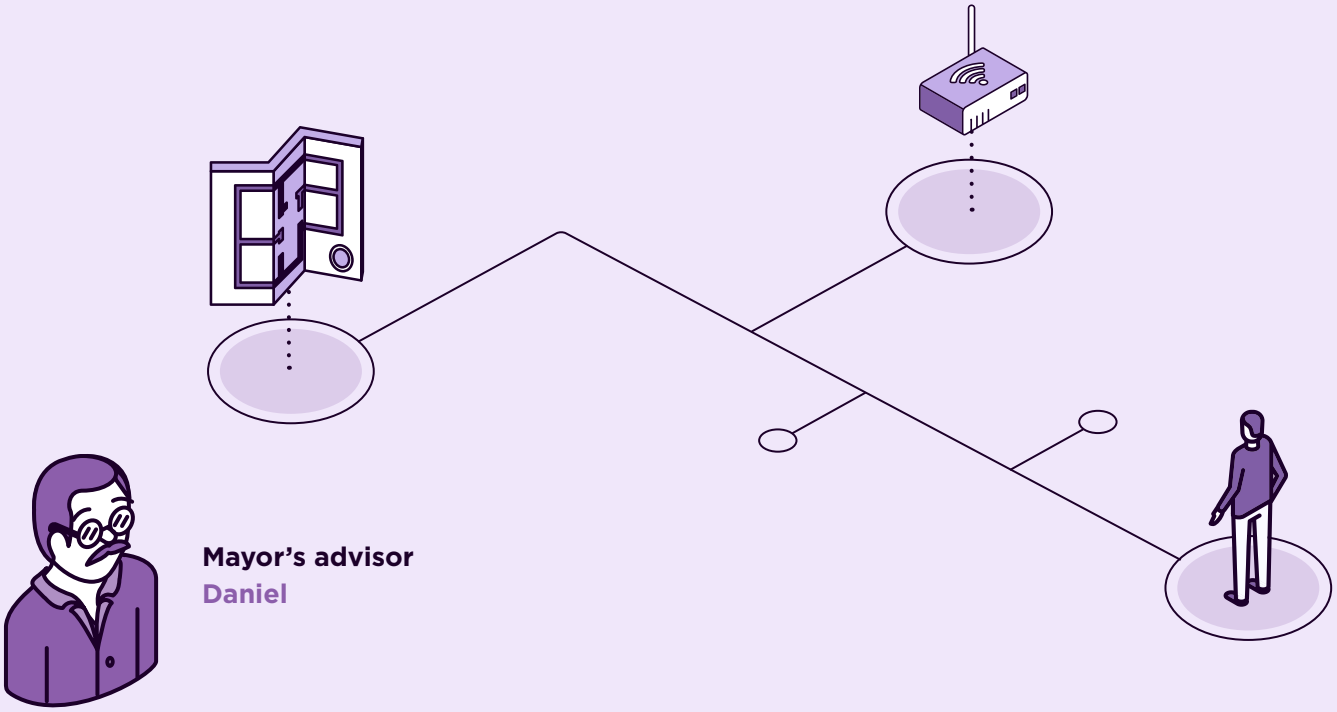
Camilo needs to apply for a scholarship for his daughter, but he is not sure where to go. Thanks to the georeferenced map system, he can see from his cell phone where the nearest information office is located and the easiest route to get there and complete the procedure.

Entrepreneur
Ana

Ana keeps track of *hardware* procurements because it is in her company's interest. Until now, she used to read tables and documents, but since the information is published in a georeferenced way, it is much more useful and easier for her to process it and, therefore, it is much more productive for her company's interests.

Vice minister of health
Sara

Sara wants to strengthen the fight against the human immunodeficiency virus (HIV) through prevention and early detection. That is why she has created a campaign to inform about the availability of free testing and care through various health facilities and other nongovernmental organization (NGO) partners. Thanks to the country's georeferencing system, citizens can use their cell phones to find out where to find and how to get to the nearest facility offering this service.



Mayor's advisor
Daniel

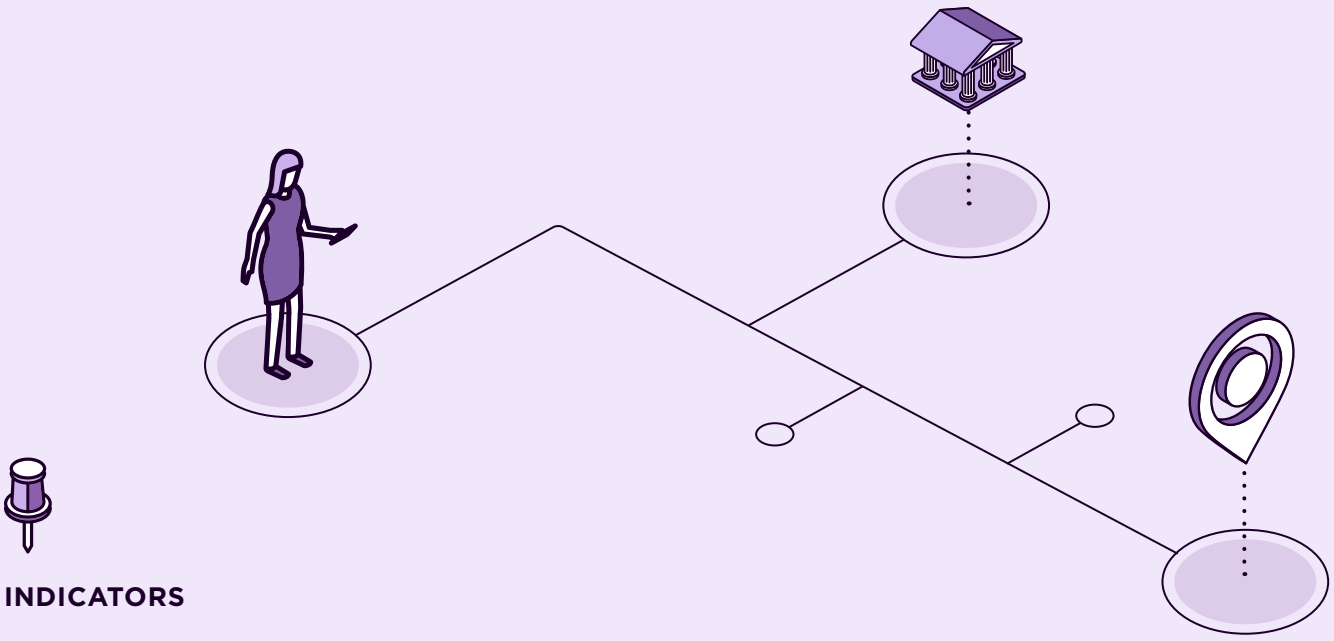
Daniel has just uploaded to the georeferencing system the tourist sites of his municipality, a map that was made in conjunction with interested businessmen. Thanks to this, the citizen can see restaurants, hotels, or places of interest, which improves the municipal tourist services in a clear way for all visitors.

EXAMPLES

Click on each flag or icon to go deeper.

Spain
Georeferencing

Colombia
Geoportal Instituto Geográfico Agustín Codazzi (IGAC)



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a georeferencing system as a common service that can be used by any public institution? If so:
  - Do you have an access control that allows opening access to staff members according to their needs and attributions?
  - Is technical support offered to facilitate the use of the system by other public institutions?
  - Is it integrated with the statistical dashboard/exploitation system?
  - Is it integrated with the open data system?
  - Are you connected to the data brokerage platform?
  - Is the system in use in more than 50 percent of central government institutions?
  - Is the system in use in more than 50 percent of subnational governments?

4.9.4 DOCUMENT MANAGEMENT SYSTEM

It is the information system that allows the storage of documents, data, and metadata, and the creation of an electronic file that gives structure to the stored information. It generally operates within a single agency; it does not include interagency exchange.

BEYOND AN IMAGE

When organizations move toward automatic or proactive administration, it is not enough to have documents stored securely; it is essential to manage them automatically. To this end, these documents must not simply be unconnected "photographs or scanned documents"; they must be organized in an "administrative file."[40] In addition, they need to have associated metadata, such as the following:

- Dates and times
- Signatures
- Users who have worked with the document
- Traceability elements
- Information related to each of the documents themselves.
    - *Example: An administrative resolution must have metadata on the following:*
        - The high position that signs it
        - The institution to which it belongs
        - The administrative procedure to which it refers
        - The exit registration number

40. It contains, for example, the citizen's request, a request for correction, the response to the request, internal reports, certificates from other entities, private documents, intermediate resolutions, official requests to other agencies, the final resolution, the notification made, a signature of collection of the documentation by the citizen, etc.

- The recipient's tax information number
- A sense of the resolution (i.e., positive, negative, partial, etc.)

THIS SYSTEM IS DIFFERENT FROM SIMPLE FOLDERS OR INFORMATION REPOSITORIES: IN THE CASE OF DOCUMENT MANAGEMENT, THE INFORMATION IS ORGANIZED AND LABELED WITH METADATA, WHICH ALLOWS IT TO BE BETTER EXPLOITED.

Structured and metadata information enables consistent and, in many cases, automatic file management. The file has a predetermined administrative process (the steps to be followed are known, depending on the procedure), and the electronic file system must keep track of it and know at all times at which step it is. This is also solved through metadata.

REQUIREMENTS TO BE MET BY A DOCUMENT MANAGEMENT SYSTEM

- To have an information system that stores files without losing the structure and associated data (not only the documents that compose it), as well as the annexed systems and services.
- To have definitions of all the procedures and codify their relationships with the files.
- To have a regulation and a consensus to carry out a normalization or standardization of the administrative file; otherwise, the advantages are not maximized, since interoperability between institutions is lost.
- To connect the information system to the file exchange system, so that complete files can be exchanged without losing metadata, and thus exchanged with different public entities, with citizens, or with the private sector (usually by making them accessible through the single point of services).
- To offer functionalities and interfaces so that the entities that need them can generate standardized interoperable administrative records automatically. From a technical point of view, the idea is that the dossier is composed of documents plus metadata, which are usually stored in relational databases that support the specific administrative processing. Although in principle this conformation of a file is not so obvious, because internally the documents are related to that processing and database, it becomes so when problems arise when the file is exchanged with another institution, when it is archived, or when the information system is changed due to obsolescence. In these cases, it is possible to find a large number of documents, unordered and disconnected, that have lost all their coherence and metadata.

Now, as not all institutions will be able to have automatically integrated information systems, it will be necessary to generate an interoperable dossier through a web page, manually uploading the documents and metadata associated with both the document and the dossier.

RELATIONSHIP WITH OTHER SYSTEMS

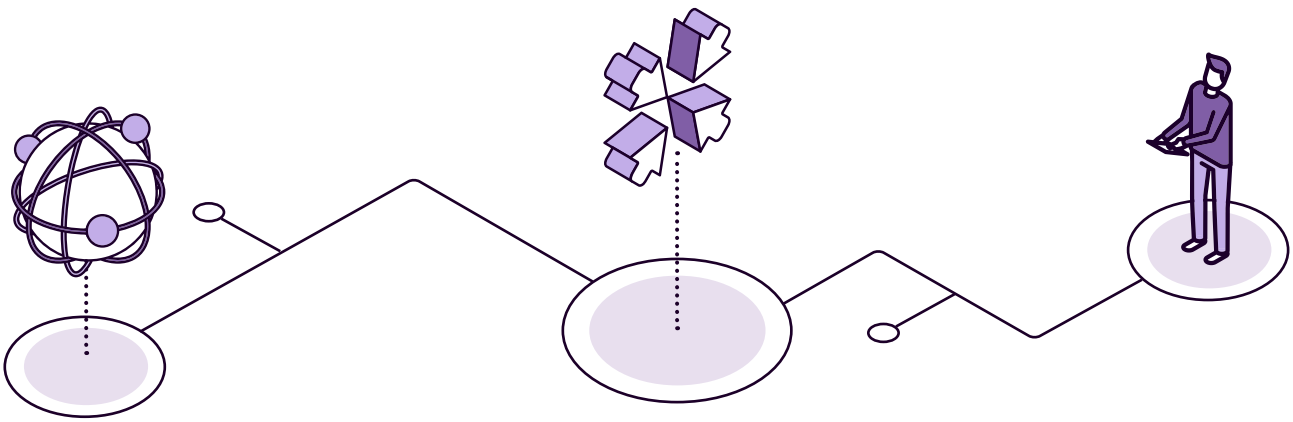
- **With the directory of public institutions:** It is very useful to mark each document or file in the document management system with the unit to which it belongs. The best way to do this is through a unique code that identifies the institution that owns each document or file, which is common to all institutions and univocal. The directory of public institutions fulfills this function.

- **With the catalog of procedures:** The documents or files in the document management system belong to an administrative procedure or process. Therefore, they must be marked as such and, if there is a single record of procedures, this code should be used to mark them.

- **With the staff registry:** Staff members of the different units must be able to access the document management system. The existence of a registry of employees, with their respective access profiles, greatly facilitates the management of registration, deregistration, and use of the system. In this way, there is no need to create a database of staff members, which runs the risk of becoming outdated.

- **With document and file exchange systems:** The document management system is enabling when it can exchange documents and files between the different entities through the system implemented for this purpose.

- **With a digital document manager:** It will be difficult to have a digital archive if the documents and files to be kept are not previously in a digital document manager.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara is happy that the Ministries of Health, Social Services, Labor, and Finance have decided to collaborate to offer a subsidy that seeks to eliminate health problems in the most disadvantaged sectors. What she does not understand is why the citizen's application document and all the attached certificates have to be copied and stored in each of these agencies, making multiple copies on paper or electronically. Sara is frustrated that there is no centralized repository that stores the information and can share it by simply sending a link.

Mayor's advisor
Daniel

Daniel needs to update the electronic repository of his municipality. He has asked around, but there is no national guide on how to do it. He is afraid to purchase any of the products that different companies are offering him, because he does not feel comfortable with their technical capabilities and fears that either he will put himself in the hands of the company, or the company will disappear at some point and leave his organization without maintenance or access to his information.

EXAMPLES

Click on each flag or icon to go deeper.

Spain
Infrastructure and systems of Electronic Documentation

Argentina
Electronic Document Management System

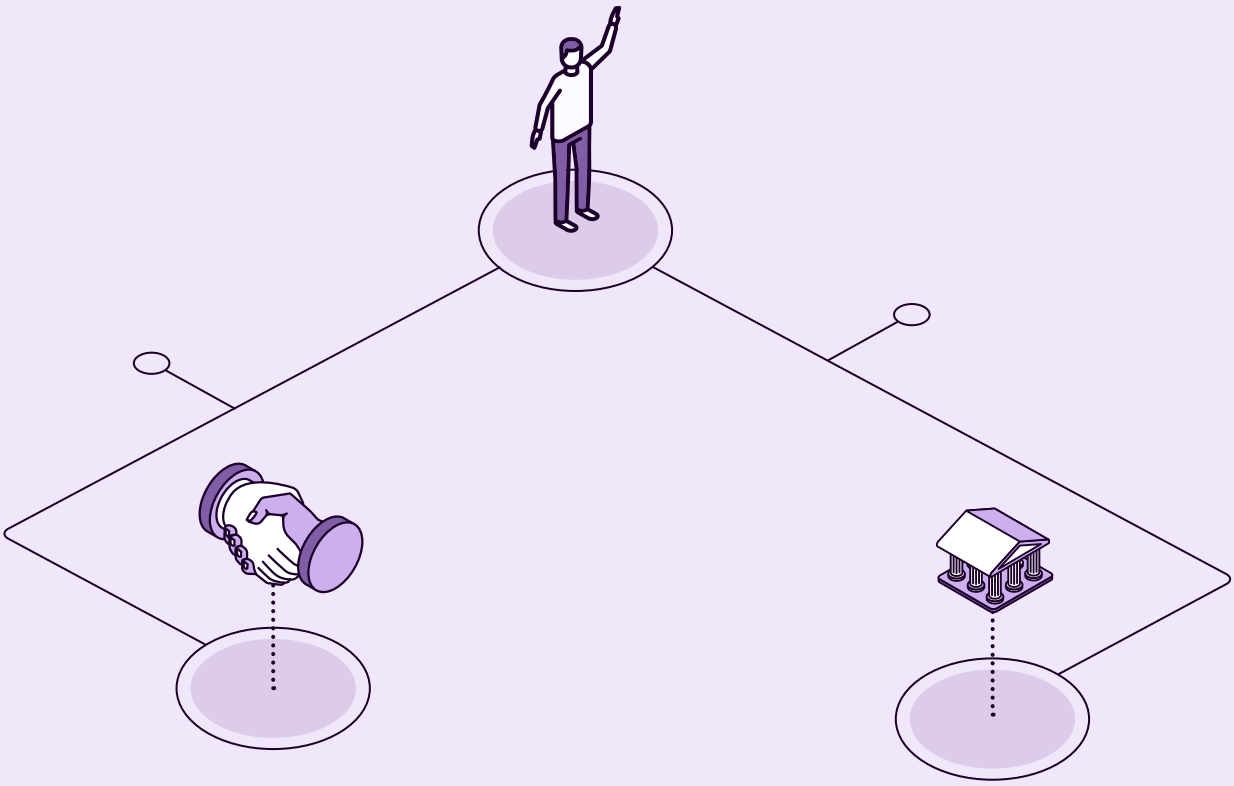
Spain
ACCEDA - Sede y Gestión-e de Procedimientos

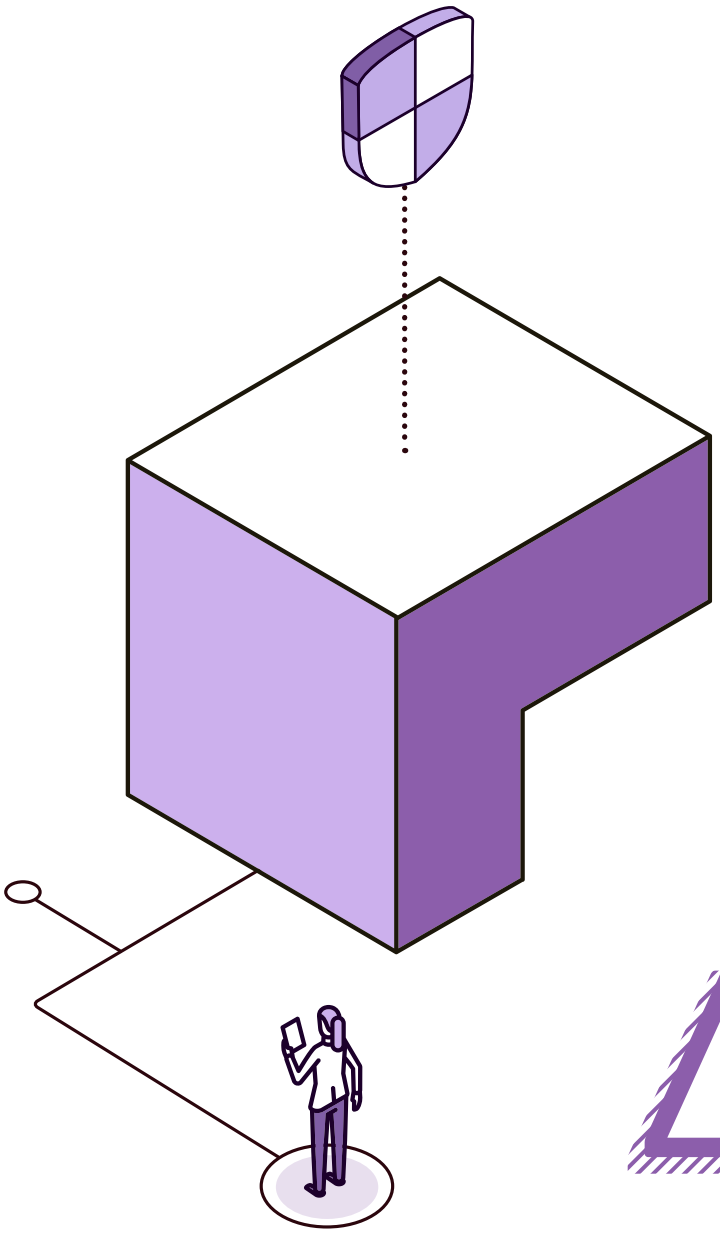
INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there established standards for document management?
- Is there a document management system?
- Are more than half of the public entities of the central government integrated to the document management system?
- Are all public entities of the central government integrated into the document management system?
- Are more than half of the public entities across the government integrated into the document management system?

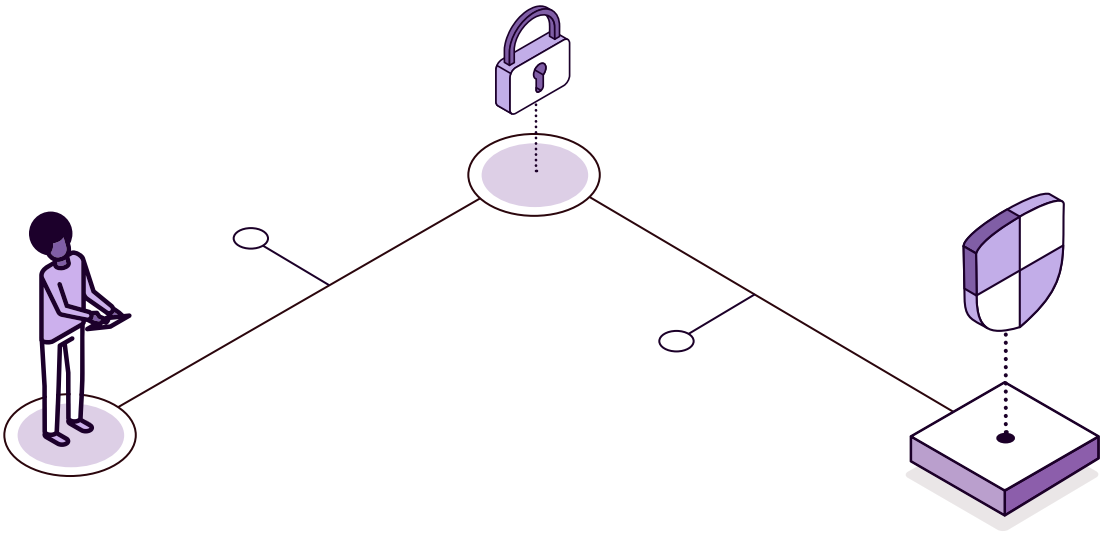
- Are all public entities across the government integrated into the document management system?
- Is the system capable of handling information of the following sizes?
  - Less than fifteen megabytes
  - From megabytes to gigabytes
  - A size greater than gigabytes.
- Does the system support the following types of procedures?
  - Internal to the organism
  - In relation to citizens/companies
  - Between public agencies.





4.10

Cybersecurity



Given the current situation, even at the time of the COVID-19 health emergency, it has been demonstrated that cybercriminals will not cease in their efforts to attack public and private organizations; on the contrary, the increase in cyberattacks worldwide is exponential. For this reason, the time has come for cybersecurity to become a priority for all types of organizations, especially for public administrations, due to the amount of information that affects the citizens of any state.

Within the framework of cybersecurity, there are a large number of tools that aim to become the main barrier between cybercrime and the systems of any organization. Some of the most relevant ones are described below.

INTRUSION DETECTION AND PREVENTION

This tool performs proactive monitoring of the infrastructure, looking for signs of intrusions and other anomalous activities. It includes detection and prevention techniques such as IDS, IPS, firewall, antivirus, etc. In addition, it generates security events that are sent to monitoring and reviews and approves security configuration changes in security elements such as firewalls.

- **IDS: Hardware devices or software** applications that use known intrusion signatures to detect and analyze incoming and outgoing network traffic for abnormal activity. They are responsible for monitoring incoming traffic through an exhaustive network analysis and port scanning. This type of technology allows detecting different types of attacks whose exploitation vector is based on the use of Trojans, backdoors, or rootkits, as well as detecting social engineering attacks such as “man in the middle,” which manipulate users to steal credentials and confidential information.

- **IPS:** Devices that enable proactive security management by inspecting a system's incoming traffic to eliminate malicious requests. A typical IPS configuration uses web application firewalls and traffic filtering solutions to block preemptive application attacks. This includes remote file inclusions that facilitate malware injections and SQL injections used to access databases.

- **Firewall:** A *hardware device* or software that manages incoming and outgoing network traffic. The function of a firewall is to protect the entire infrastructure—servers, systems, individual computers, and network equipment—against unwanted access by intruders.

- **Antivirus:** A software tool used to protect against, search for, detect, and remove malicious code inserted illegally. There are multiple vendors worldwide that offer different levels of protection and analysis of malicious code.

THREAT ANALYSIS AND COMMUNICATION

With this tool it is possible to proactively investigate and monitor security information to identify threats. Today, security threats are no longer static; advanced persistent threats (APTs) capable of constantly changing their behavior to evade detection must be addressed.

APT detection is closely tied to the technologies described in the previous section and how network control and remote access is performed. Network activity associated with remote control can be identified, contained, and disrupted through analysis of network traffic between zones. Techniques for APT detection, in particular, can be implemented through proprietary or open-source software tools such as IDS/IPS, network packet monitoring, and management (NSM) programs to monitor network flows (NetFlow), with logging elements that provide visibility into what is happening on the network and enable on-demand packet capture.

APTS OFTEN EXHIBIT RECOGNIZABLE PATTERNS THAT CAN BE MONITORED BY TOOLS. MONITORING FILE INTEGRITY DATA FROM SYSTEMS ALONG WITH NETWORK FLOW DATA CAN BE KEY TO DETECTING APTS.

VULNERABILITY DETECTION

This performs periodic and ad hoc scans of the infrastructure to identify system vulnerabilities and feeds the vulnerability database for easy use by monitoring tools. Vulnerability scanning can be performed using open-source or proprietary tools, which can scan both web applications and infrastructure. These tools often include multiple predefined scanner configurations that allow scanning of IP ranges or specific scanning of vulnerabilities associated with web applications.

MONITORING OF SECURITY EVENTS

This is the first-level equipment for the resolution of security alerts. It monitors the SIM/SEM (security information management/security event management) tool console in real time and manages the SIM/SEM infrastructure and event correlation. SIEM collects data and logs from a variety of sources to ensure that no important security event is missed. Once events have been collected, these tools allow them to be correlated using algorithms that look for trends and common attributes in order to derive meaningful and useful information.

Automatic analysis of related events creates security alarms and alerts to notify operators of any potential problems. SIEMs often include security alert visualization and aggregation panels (*dashboards*) to facilitate the processing of security events through graphical displays. In this way, it is possible to access events coming from different assets during different time periods, through a specific set of criteria defined in the SOC's operating procedures.

There are multiple vendors of SIEM tools worldwide. While early versions of these only allowed standardized integration of a few data sources, such as firewalls and intrusion detection systems (IDS/IPS), the current generation of SIEM systems has evolved to process large volumes and variety of data.

The current SIEMs allow the following:

- **User management, control, and account usage:** SIEM can correlate access and control logs of users with administrative privileges to detect inappropriate usage and generate alerts. It also monitors user activity based on access rights and user roles to detect application and data access violations.

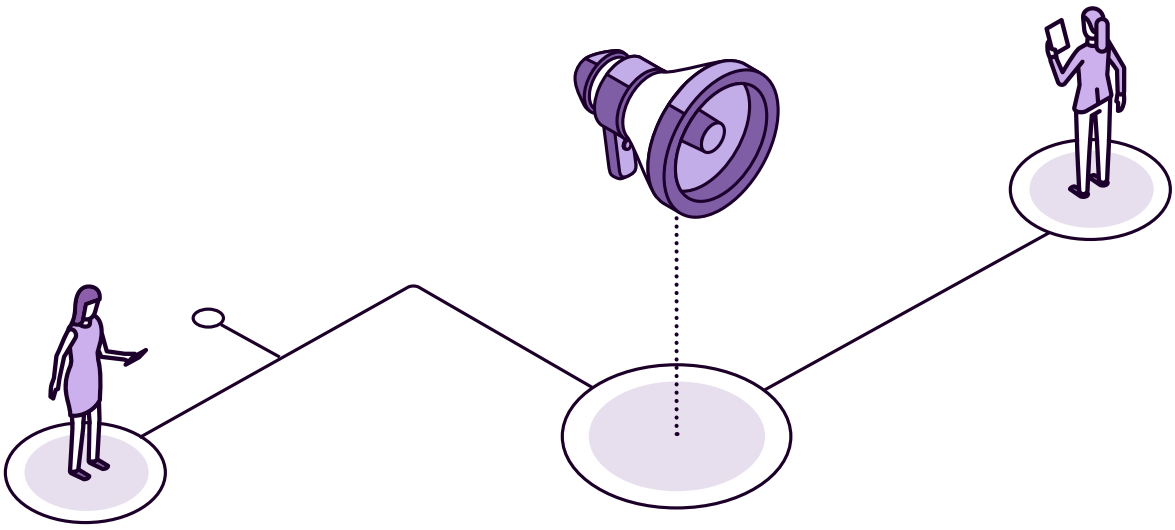
- **Configuration of protocols, network services and malware:** Through SIEM it is possible to correlate the configuration of network devices with log data to detect traffic through restricted ports, services, and protocols. These controls and alerts can be used to determine which ports and services are useful for the exercise of the activity and which types of traffic and ports can be restricted. The event correlation capabilities offered by today's SIEMs also allow alerts from antivirus and *antimalware* tools to be collected and their findings centralized in the SIEM, which will correlate with system data and vulnerabilities to determine which systems are most at risk from the *malware* discovered.

ETHICAL HACKING

This is the set of offensive security measures that analyze risks to prevent illicit access to data or communication, as well as unauthorized access to them by cyberattackers. Typically, ethical *hackers* are individuals who use *hacking* skills, knowledge, and techniques within a legitimate practice authorized by the organization.

Among the actions that comprise the work of ethical hacking are:

- Conducting audits such as
  - Black box;
  - Gray box;
  - White box.
- Security scanning through specialized tools that analyze the open-source TCP/IP communications ports, performing a scan of all communications ports, in the various IP protocols, and detecting their status.



CYBER EMERGENCY RESPONSE TEAM

States, public administrations, and private organizations must be prepared for security incidents that may occur for a variety of reasons, including maliciously planned or trusted insider attacks, as well as nonmalicious insider acts that may result in damage. Consequently, the management of these incidents is a central component of an organization's strategy in order to ensure its viability and resilience, as well as to support critical business processes governed by regulatory processes at both national and international levels.

Thus, IT security incident response has become a fundamental component of information technology programs. However, when an incident is identified, victims often do not have the capacity to deal with it:

- Sometimes, the occurrence of an incident may suggest that the cybersecurity team itself does not have sufficient capacity to prevent—and possibly not handle—such situations, exposing the need for specialists that may not exist internally.

- Often, when an organization suffers an incident, its own cybersecurity team is understaffed to handle a large-scale emergency, which can require numerous highly professional actions to be taken quickly.

- Even more often, when an organization suffers an incident, it does not have sufficient information to analyze which vulnerabilities have been exploited, which exploits have been used, what the root causes are, or which tools and remediation elements are the most effective, etc. The organization does not have enough information to be able to respond in a timely manner.

EFFECTIVE INCIDENT RESPONSE CAN BE ACHIEVED THROUGH THE DEVELOPMENT AND INSTITUTIONALIZATION OF EFFECTIVE SUBPROCESSES AND PROCEDURES.

As such, cybersecurity incident response has become a highly specialized profession/qualification. The team or service in charge of the operation of these procedures is known as a computer emergency response team (CERT) or computer security incident response team (CSIRT).

THE OPERATIONAL TEAM OR SERVICE MUST PROVIDE THE HUMAN RESOURCES, PROCEDURES, AND TOOLS TO REACT QUICKLY AND EFFICIENTLY TO ANY POTENTIAL SECURITY INCIDENT.

Given the criticality of these types of incidents and the potential impact they can have on an organization if they are not contained in a timely manner, the operation of these teams is usually characterized by having:

- 24-7 availability.
- Multiple communication channels so that security incidents can be reported as soon as they become known: internal/external email inboxes, social media, early warning telephones, communication forums with other CERTs, suppliers, etc.

Security incident management includes different phases, which include both proactive and reactive activities:

- Proactive services:
  - Alerts and warnings
  - Technology observatory
  - Security assessments or audits
  - Security configuration and maintenance
  - Development of security tools
  - Intrusion detection services
  - Dissemination of safety-related information
  - Monitoring and event detection (SIEM).

- Reactive services:
  - Collection of data related to the potential incident
  - Incident analysis and treatment
  - Incident response support and coordination
  - On-site incident response
  - Vulnerability analysis, response, and treatment.

CERTs are usually organized around a main incident response process known as *triage*, where the incident is classified according to its severity. Most are organized into three levels:

- Level 1 analysts receive the first reports, gather initial data, and perform the initial incident classification to determine the next steps to be taken.
- Level 2 analysts are typically team leaders, with extensive experience and enhanced skills, and lead the handling of more complex incidents as they arrive.
- Level 3 analysts analyze highly complex incidents in depth, using specialized tools to determine how the incident occurred, who might be behind it, what damage it has caused, and how similar incidents could be prevented in the future.

These units can exist within the organization they support or be established as external service providers, supporting different organizations. They may be commercial (in which case they serve a single company or provide a paid service), academic (working with universities) or governmental (serving units of government or a country). In this regard, it should be noted that there are benefits for centralized teams to manage incidents in different but similar organizations, as a higher frequency of incidents (the combined occurrence of multiple organizations) helps to generate knowledge within these teams, which is then passed on to many beneficiaries.

A national CERT faces a wide variety of cyber incidents in the country, which could be of high impact and national interest. On the other hand, sectoral CERTs, usually promoted by the private sector, provide services to sector-specific organizations, using contextualized knowledge of sectoral processes, priorities, and technologies, and capitalizing on the specific mechanisms of trust and cooperation within sectoral communities.

In addition, CERTs often perform other organizational functions, such as the following:

- Threat intelligence
- Publication of warnings
- Training
- Coordination of external or international relations
- Technical tasks for your own it systems
- Administrative and managerial functions.

CYBERSECURITY OPERATIONS CENTER

Cybersecurity attacks can be difficult to detect without the right tools to automate detection and response processes or the expertise to properly handle incidents and vulnerabilities, as many of them are designed to go undetected (especially in their early stages). Adding to this complexity is the fact that the number of incidents, as well as the number of types of threats, is growing continuously, year after year. In the wake of the pandemic, in particular, there has been a clear increase not only in the number of cyberattacks, but also in their severity.

In figures, during 2019, around 3,172 very high-threat cyber incidents were detected in a good number of countries' public bodies, specifically in the southern European region, while in 2020 they doubled to 6,690. Meanwhile, during 2020, a total of 73,184 total cyber threats were detected in the southern European region, an increase of 70 percent over the previous year.

Unfortunately, it is impossible to cover and resist all types of existing cybersecurity threats, as resources are restricted. Thus, the need has arisen to strengthen the capacity for prevention, monitoring, surveillance, and incident response, especially in the field of public administrations, where this kind of attacks pose risks to the strategic, economic, and social position of countries. This is why more and more countries are deciding to opt for collaboration between public bodies and private third parties to strengthen themselves in this regard. The analysis of the cybersecurity ecosystem carried out by each government makes it possible to identify the assets to be protected, the risk to which they are exposed and the resources available or required to manage the threats faced by the assets and the actors/entities involved in these activities.

The control of these actions can only be carried out through a *cybersecurity operations center* (SOC). This concept encompasses a set of people, processes, technologies, and facilities that focuses on the identification (detection) and response to incidents that arise as a result of the materialization of cybersecurity threats. The SOC is, in short, an operational unit whose purpose is to provide horizontal cybersecurity services.

Now, while early detection of incidents or anomalies that may indicate that an attack is taking place will bring more value, it is also true that to the same extent it will require greater specialization, automation, and the use of disruptive technologies such as artificial intelligence, machine learning, advanced analytics, data visualization, etc. Therefore, designing and managing SOCs is a highly specialized skill.

Among the actions of a SOC are the following:

- Monitor digital assets (belonging to one or more organizations).
- Monitor and analyze any anomaly that may constitute a cybersecurity incident and should be investigated.
- Carry out threat detection in the daily operation of the information and communications systems of the different bodies and administrations.
- Improve the response capacity of the different bodies and administrations to any attack.

SOCs can be part of a CERT or they can work autonomously; they can even have their own internal incident response unit. The SOC could also be considered as the "front line" of a CERT.

ONCE AN INCIDENT IS DETECTED, IT MUST BE TRANSFERRED TO AN INCIDENT RESPONSE UNIT.

The scope of service of the SOCs will be the administrations determined by the different countries and their public bodies. However, in order to be able to participate in the services of a SOC, the entity must be attached to the centralized internet outlet of the public administration of each state.

In order to articulate a SOC within the framework of public administrations, it will be necessary to have a body dedicated to national cybersecurity that is closely linked to the most representative bodies of the public administration of each country, with the aim of carrying out an implementation, operation, and incident-detection plan that is fully coordinated with a monitoring of the service by the public administration in charge. In this sense, the SOC must house the infrastructure and intelligence in the field of cybersecurity that a country must have for the protection and defense of its public administrations.

It is recommended, then, that the implementation of an internal SOC or the contracting of SOC services to third parties be part of an information security management strategy that includes a security master plan, as well as specific cybersecurity incident response programs. This strategy will include the specific objectives for which the SOC should be responsible, such as the ability to continuously monitor threats and establish clear procedures for the following:

- Analysis, communication, and evaluation of current and potential impact of threats and vulnerabilities
- Effective methods of data collection, analysis, and reporting
- Continuous monitoring of it infrastructure security
- Intrusion detection and prevention
- Establishing relationships with the various security incident management teams and internal and external stakeholders for escalation and crisis management

SOCs use a variety of general purpose and specialized tools, including the following:

- Security information and event management systems (SIEM)
- Orchestration systems
- Sources and catalogs of attack indicators and commitment indicators
- Sandboxes[41] for potentially malicious software
- Ticketing systems to handle incidents

41. This is a mechanism for inspecting potentially malicious software in a controlled environment, where its behavior is monitored to evaluate its characteristics, while it is contained so that it does not affect other systems.

- Communication channels with customers
- Information exchange systems

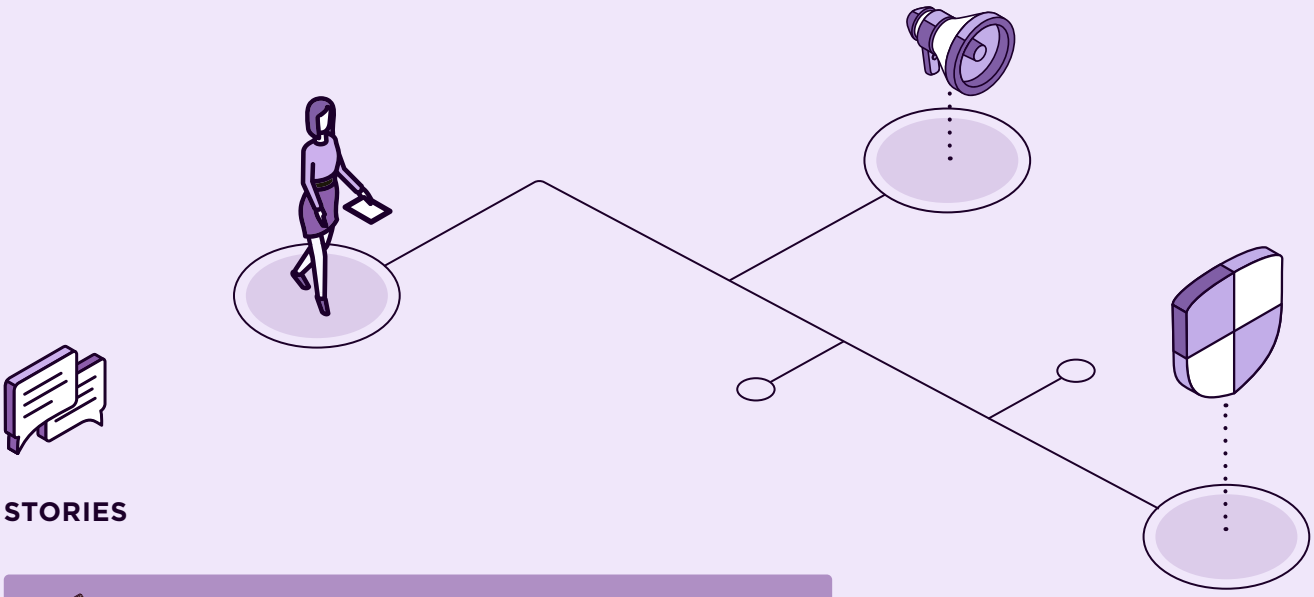
Naturally, these centers need a high-end IT infrastructure, both in terms of hardware (storage and communications) and software (virtualization, big data, and business intelligence applications). In addition, these centers should be especially well protected, because of the handling of potentially infectious malicious code that often has access to the monitored systems and the sensitive information on them, and because attackers may want to disable the defenses for their attacks.

Maintaining the privacy and confidentiality of information within monitored systems is an important issue. This, along with liability issues, among others, raises special legal issues. In principle, a SOC has the capability to monitor various systems, organizations, and types of technologies, up to the entire government. Some considerations in deciding on the scope of monitoring could be

- Organizational structure;
- The types of technology used;
- The need for specialized knowledge for certain systems (such as critical infrastructure operating technology) or sectors;
- Having a volume of cyber activity to monitor, trying to avoid an overload of work that leads to a neglect of some part of the obligations.

The creation of a SOC should be established in phases:

1. **Establishment of the SOC:** With an expected start-up period of no less than twenty-four months. In this phase, the development of conceptual design tasks for the SOC's own communications should be addressed.
2. **Pilot:** In this phase, tasks of defining parameters and service levels, installation, and acquisition of technical infrastructure, as well as implementation of basic cybersecurity services, are addressed to begin the process of annexing the first entities and agencies of the public administration.
3. **Consolidation:** With the aim of extending the service to all public bodies and entities agreed by each government. In this last phase, it will be necessary to evaluate the inclusion of new advanced cybersecurity services, as well as the establishment of tasks for the maintenance and improvement of the service.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

When Sara prioritized building her ministry's information security team, she realized how complicated (and expensive) it was to get cybersecurity specialists. So having access to the government's cybersecurity operations center, which works in conjunction with her team, now gives her the peace of mind she needs to know that her ministry is protected by the best and most up-to-date cybersecurity professionals.

Sara is very interested in cybersecurity issues and has asked to be included in the communications that CERT exchanges with her ministry. She is surprised by the number of attacks that her information systems suffer continuously, the security holes detected and protected before greater evils, and the importance of the ministry's security team for the correct functioning of the information systems.

Mayor's advisor
Daniel

Daniel did not know what to do when he was alerted to a potential cybersecurity problem in municipal systems. Thanks to his agreement with the government's cybersecurity operations center, the necessary adjustments were made so that this problem did not end in an attack on their information systems.

Daniel has just installed attack detection and protection mechanisms in his municipality's information systems. Before the Department of Homeland Security contacted his office, he didn't even know about this equipment. He now knows that they are essential for maintaining the security of municipal information systems.

EXAMPLES

Click on each flag or icon to go deeper.

SOC-CMM
Security Operations Center Capability Maturity Model.

In Latin America and the Caribbean, there are approximately twenty national CERTs or CSIRTs.

FIRST is the Global Forum for Incident Response and Security Teams.

Latin America and the Caribbean – CSIRTAmericas.org is an organization of CSIRT groups, founded by the OAS.A.

Carnegie Mellon University's Software Engineering Institute has a division and CERT coordination center, which helps set standards, train, and certify CERT teams around the world.

Most developed countries have national CERT organizations that provide professional incident response. Examples of national CERTs of reference, with a variety of structures and services, include the following:

Spain
INCIBE-CERT and CCN-CERT

United States
US-CERT

Israel
National Cyber Directorate

United Kingdom
National Cyber Security Center

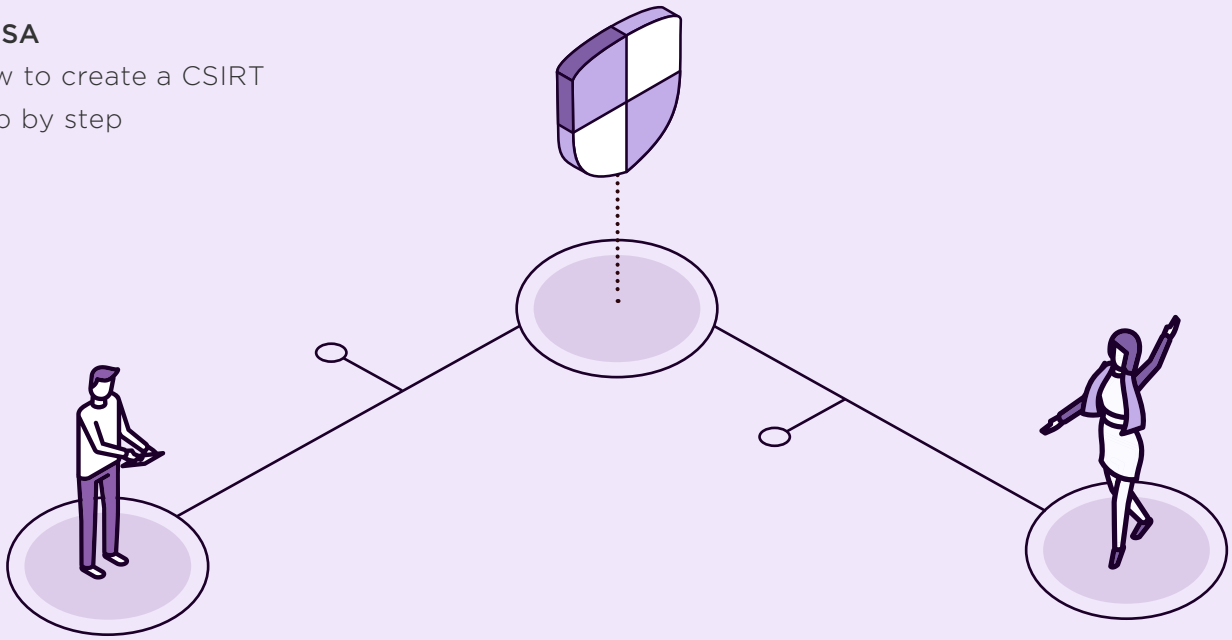
ENISA
How to create a CSIRT
step by step

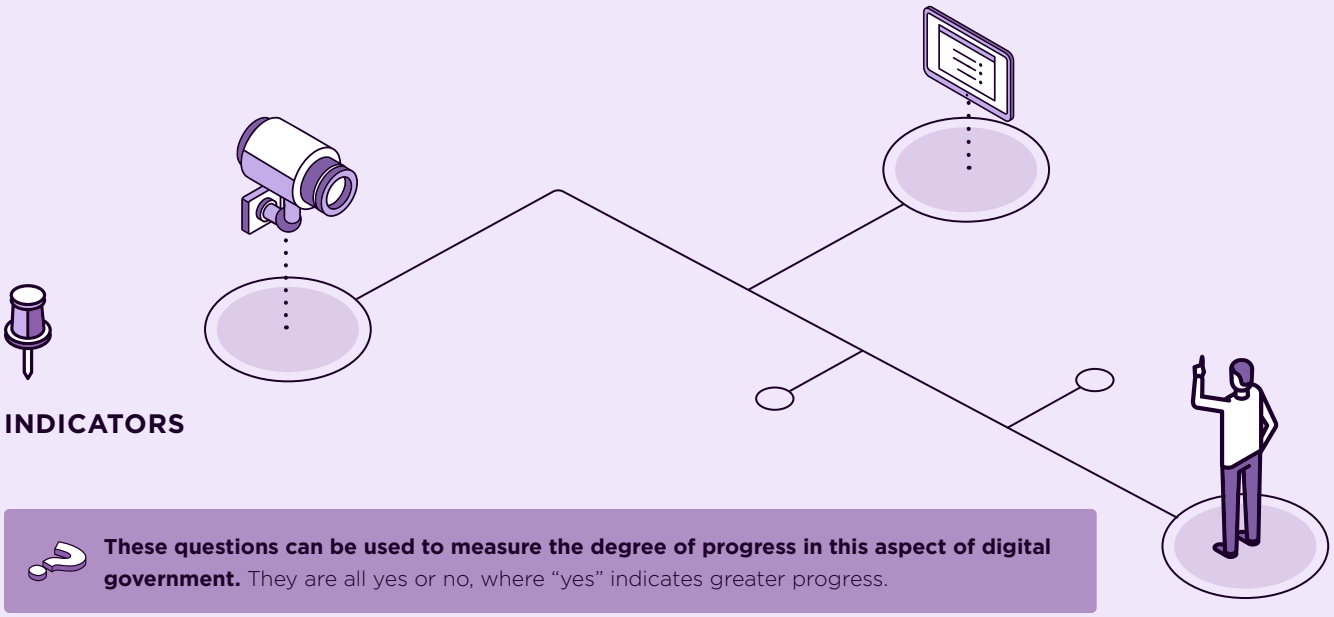
ENISA CSIRT Maturity
Assessment Model

SIM3
Security Incident Management
Maturity Model

First.org Service
Framework

Creating a Computer Security
Incident Response Team:
A Process for Getting Started

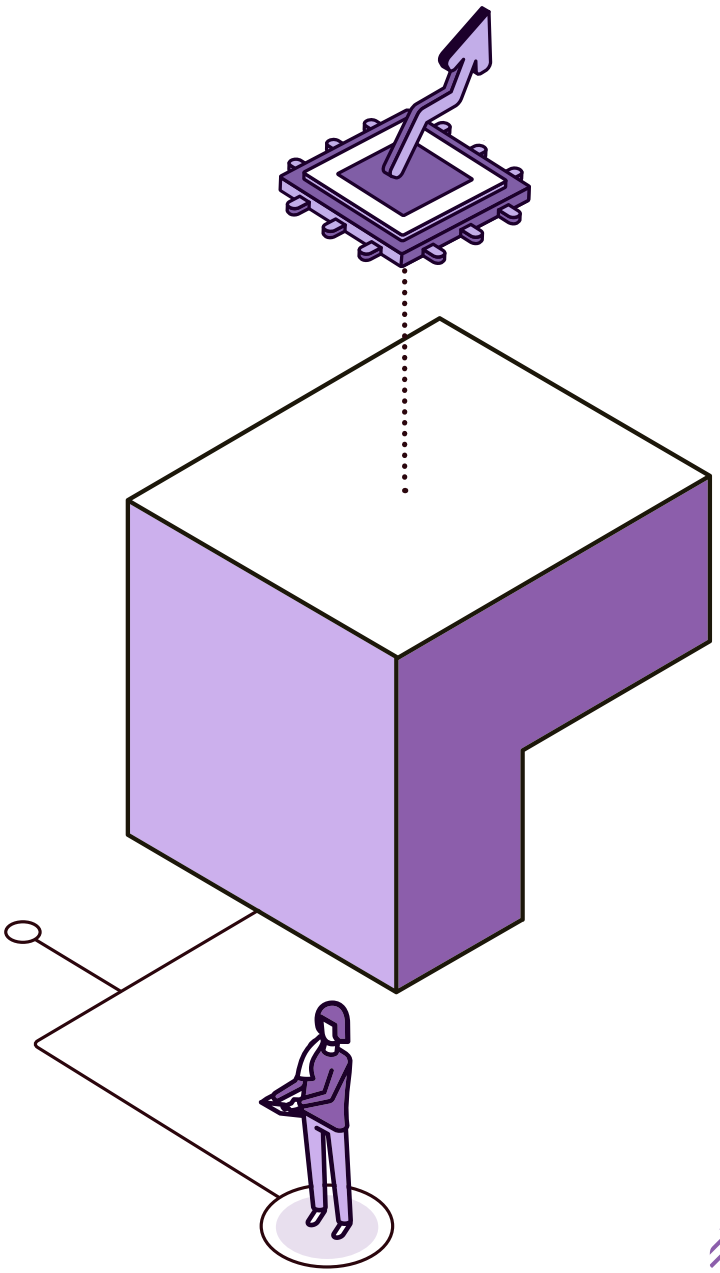




INDICATORS

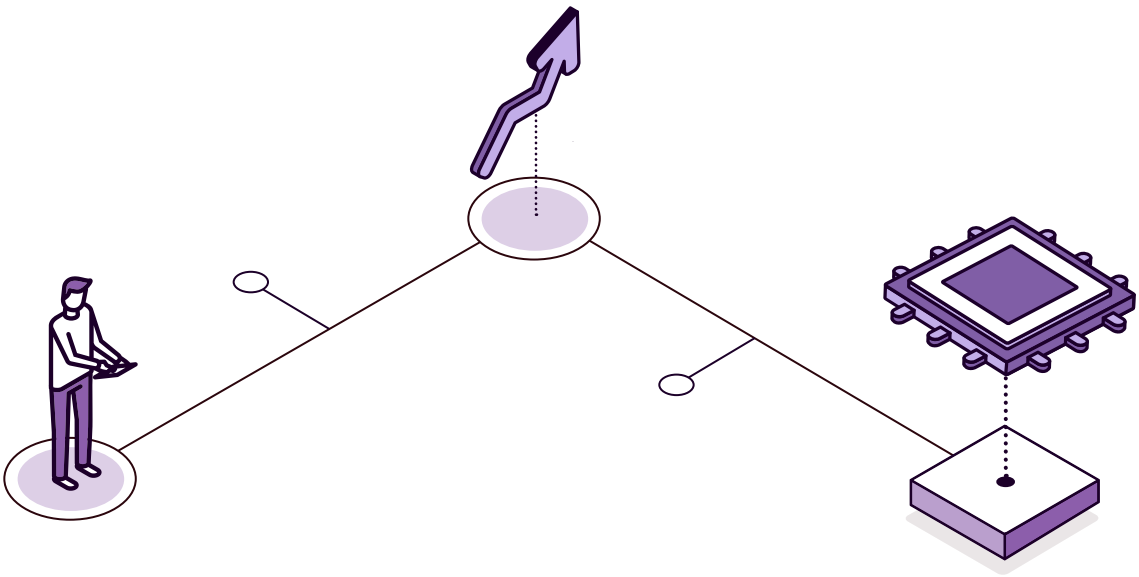
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are there central SOC facilities to monitor government digital assets?
- Are there central SOC facilities to monitor the country's critical infrastructure digital assets?
- What percentage of a government's digital assets are monitored by SOCs?
- What percentage of critical infrastructure facilities are monitored by SOCs?
- Are adequate metrics and indicators available to measure downtime of critical systems during an attack?
- Does the country have a national CERT?
- Does the country have sectoral CERTs for all critical sectors?
- Does the country have a body and procedures for coordination between the different CERTs?
- Has the country legislated incident reporting to the national CERT?
- Does the country have CERT implementation guidelines?



4.11

Disruptive technologies



It is a duty and an obligation of the public administration to make available to citizens and companies all those technological improvements that allow a better provision of service at levels of security, efficiency, rationalization of expenditure, and sustainability. The digitalization of society is advancing at an ever-increasing pace, and the fact that the public administration cannot be left behind makes it increasingly necessary to provide innovative public services. Thus, although it is true that it is possible to apply "traditional" or long-standing technologies, and the results can be very positive in terms of the modernization of the administration, within the digital transformation it is necessary to adopt new alternatives that transform the economy and society through the creation of innovative processes that enable a radical change in the way public services are provided to society.

It should not be forgotten that many of these technologies are in stages that are not mature enough for widespread implementation in such a critical service as the public one. However, progressive incorporation through the design of transversal platforms will make it possible to lay the foundations for future widespread adoption.

In order to be able to apply this type of technology to public services, the lead institutions must channel and promote feasibility studies by creating innovation laboratories that work within the administration, with its inherent data and problems. In this type of laboratory, the participation of society should be encouraged through citizens and private companies, in the first case to learn firsthand about the needs and opinions regarding these innovations, and in the second case to encourage cocreation and innovation in public services through the experience in these technologies that companies that have developed projects in these technological areas can contribute.

Some of these technologies will be described below, in order to narrow down those that can be directly applied to the provision of innovative public services.

BIG DATA

Data has become a very valuable asset when making decisions, either internally, for the continuous improvement of the administration itself, or externally, to understand the behavior of society and identify new needs that are emerging with the advance of digitization. Every day more and more data is generated faster and faster, so the correct management and exploitation of this information is an opportunity for the public administration to generate value for citizens, through the better use of public resources (increase efficiency, reduce costs, increase productivity) and the creation of new services for citizens and companies.

Now, although the current scenario is an opportunity to have large amounts of information available, as mentioned above, it is important to safeguard and protect citizens' personal data. Therefore, it deserves special attention to establish mechanisms that ensure the correct treatment of this information as a rule and not as an exception.

Within big data we can highlight two branches that make it possible to exploit information:

- **Data science:** Tries to predict and discover future behaviors through the analysis of old data patterns.
- **Data analytics:** Analyzes information to extract relevant information, trends, and metrics that can be used for decision-making.

In order to carry out a big data project, cross-cutting platforms must be established to enable the organization to:

- Collect information from multiple sources, whether homogeneous or heterogeneous, and data types (structured, unstructured, semistructured);
- Interconnect the different data warehouses and data lakes where this information will be deposited.

The platforms must be interoperable, so standards must be developed for the exchange of information. Likewise, given the heterogeneity of data, sources, and formats, it will be necessary to establish a data quality plan to homogenize these inputs, ensuring that their subsequent use is based on a reliable information base. It is necessary to contemplate data quality standards, such as ISO 8000.

In addition, the necessary technological infrastructure must be correctly sized, since the large volume of data requires a significant amount of resources for its collection, cleaning, integration, and standardization in a reasonable time for processing, before the information becomes obsolete. On the other hand, it is also necessary to establish a plan for data governance, ensuring that the use of data is authorized and organized and that access authorizations are in place. In addition, privacy and security will be taken into account as a basis for any work to be carried out.

The amount of information that is generated at high speed, with a diverse origin, makes its processing by individuals impossible. Today, data is a tremendously valuable asset in which private companies are investing huge amounts of money, and the public administration has all this information for free, so it cannot afford not to make use of it and must apply it to improve the public services it offers to society.

The use of *big data* allows the organization to:

- Identify problems that were not known;
- Be able to adapt more quickly and efficiently to changing trends;
- Identify new opportunities, enabling cost reduction and the implementation of new innovative public services.

ARTIFICIAL INTELLIGENCE

This is the ability of systems to analyze their environment and make decisions, with a degree of autonomy large enough to achieve specific, predetermined objectives. Associated with this technology is another called machine learning, with which software and systems use the information and data made available to them to adapt their behavior or improve the tasks they perform in response to changes in execution conditions, without having been explicitly programmed to do so. This gives the services flexibility and adaptability to the specific conditions of the moment.

These technologies have a direct application to public policies and can improve all public services provided, but they rest on two pillars that must be developed in order to control the results obtained:

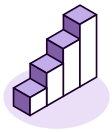
- **Data quality:** The entire artificial intelligence model rests on this premise; autonomous decisions cannot be made without quality information.

- **The development of a clear and transversal regulatory framework:** This must guarantee fundamental rights, the correct use of this type of technology, and the obligations of this type of system, such as human supervision and the limitation of its capabilities.

IN ORDER TO IMPLEMENT AN ARTIFICIAL INTELLIGENCE PROJECT WITH CERTAIN GUARANTEES, IT IS NECESSARY TO ESTABLISH ECOSYSTEMS THAT ENCOURAGE THE APPLICATION OF THIS TECHNOLOGY. HAVING A BIG DATA INFRASTRUCTURE CAN SUPPORT THIS EFFORT.

A factor to be considered prior to the application of artificial intelligence techniques in any field or project is the so-called useful information and the amount of it with which the models can generate new knowledge. Likewise, it is important to bear in mind that artificial intelligence processes, as in humans, are based on learning and, therefore, are not infallible. It must always be contemplated that failure may be present in this area.

Robotic process automation (RPA)



Internet of Things (IoT)

Blockchain

Smart contract (blockchain based)

ROBOTIC PROCESS AUTOMATION (RPA)

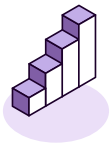
The public administration cannot afford that the people who work for it are developing activities where there is no contribution of intellectual value. Often, this corresponds to simple, routine, repetitive, stable, and time-consuming tasks. Robotic automation of processes aims to solve this issue through the creation of "robots," implementing software that works as a virtual employee and performs those simple and repetitive tasks for which a person was intended. In this way, it is possible to relocate people to tasks that add value to the public services offered, making a more efficient management of available public resources and increasing their productivity.

Likewise, these automations make it easier to quickly undertake integrations between applications, which would otherwise require developments that can take a long time. In addition, they also facilitate the integration of older systems, which usually present difficulties in interacting with more modern applications.

To implement these technologies with a certain degree of success, a transversal service for the entire public administration focused on the intelligent automation of processes is recommended. For example, the use of corporate platforms that allow the automation of administrative actions, incorporating different reusable components (building blocks) for the processing of data, documents, images, audios, etc., will give all administrations access to these homogeneous resources, generating synergies and reducing implementation and adoption times for this technology.

Most of the administrative procedures of any public agency contain the same processing phases, and in many cases a high number of common procedures, so it would be advisable to consider the possibility of creating a common administrative procedures processing platform, which is configurable and allows reducing time in the management of procedures. This would improve efficiency in the provision of services.

The application of these technologies, among other reasons, seeks to rationalize and increase the efficiency of the use of available public resources. In this sense, the "robotic automation of processes" makes it possible to allocate the administration's most valuable resources—people—to perform work of high added value for society, while automating simple, routine, and repetitive tasks.



INTERNET OF THINGS (IOT)

It is the representation of how the digitalization of society is advancing, in which objects and people can interact through the various communication networks available, and how these relationships can then be exploited to generate value-added services, both to the administration and to citizens and companies.

One of the great challenges facing the administration is the management and sizing of the interoperability platforms of these systems, in order to have the capacity to identify and provide service to the large number and diversity of existing IoT devices. It is therefore a technology that offers high-value services to citizens in the short term.

To carry out IoT projects successfully, a national Internet of Things ecosystem must be established. This requires working on platforms and infrastructures that allow the integration of the large number of different devices that exist. It is of vital importance to work with the different suppliers of these devices and other actors involved, with the aim of developing new work and business models based on this technology.

The exploitation of this technology can give rise to cities that are themselves an immersive public service for society, where the relationship between the administration, citizens, and companies arises naturally through the use of technology. It should be remembered that the use of this technology must be strictly regulated, as it affects people's basic rights.

BLOCKCHAIN

This technology allows both the administration and citizens and companies, without knowing each other, to mutually trust each other, through the collection of various kinds of evidence that guarantee the transactions carried out between each of them, without having to resort to a trusted third party. This evidence is securely incorporated into a blockchain, which is replicated in different distributed nodes by means of cryptographic techniques impossible to modify after the insertion of the evidence.

Thus, you have a tremendously powerful tool when it comes to customizing the information you share with third parties.

Given that this technology emerged as a means of providing security to transaction environments that were not regulated, its application to public administration, where environments are regulated, although possible, requires a feasibility analysis. In environments that are poorly digitized, heterogeneous, and highly fragmented, in particular, it can be a quick and relatively inexpensive solution for transforming and digitizing public services, while in environments where there is interoperability and where policies have been developed to standardize information and processes, its application may not be profitable.

Carrying out the implementation of blockchain projects requires the establishment of statewide cross-cutting platforms and networks that enable the secure provision of public services through blockchain. The common platform has to provide basic infrastructure, connectivity, the blockchain, and a necessary storage space. From there it can be overlaid with other specific end services developed on top of this infrastructure, such as electronic identification, electronic voting, etc.

It is important to make decisions about the type of blockchain to be used: whether it will be based on free and tested distributions, or whether it will be public, private, or hybrid. Since the information is encrypted in these systems, viewers must also be developed according to the type of information to be exploited. It is also necessary to establish national rules and standards for the development of blockchain code, which will make it possible to ensure its quality and offer it openly as a secure resource.

Currently, this technology is in expansion and still requires analysis and progressive implementation through the realization of small pilots to generalize its use in the base of e-government services.

SMART CONTRACT (BLOCKCHAIN BASED)

Esta tecnología se encuentra basada en la anterior, y da un paso más en la confianza entre distin-
This technology is based on the previous one and goes a step further in the trust between different actors, incorporating conditions that trigger actions automatically at the moment of compliance. It is an alternative that can be applied to the optimization of processes involving different actors, automating many of the actions that in a traditional procedure require human intervention.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo has discovered that there is an IoT network in his city, through which he connects his mobile device and can avoid traffic delays. His smart device is recommending the optimal route based on traffic congestion, government interventions (road works, temporary road closures, breakdowns, accidents), and route analysis.

Mayor's advisor
Daniel

Daniel has authorized the installation of a series of IoT devices that allow the city's traffic to be monitored. In addition, they have integrated into the IoT platform a new system of beacons that allows them to mark interventions in the city that may affect traffic. Finally, and with all the information they receive, they have decided to consolidate it through *big data* and, through the application of artificial intelligence, to have a system that makes automatic decisions regarding the best routes based on the user's destination, so that it directs people through a smartphone, identifying changes in the route depending on external conditions. Daniel has found that traffic problems have been reduced in the city.

Vice minister of health
Sara

Sara has implemented a big data system that receives traffic and air quality information from all cities in the country. By exploiting the information through data science and data analytics, she has realized two things. The first is that if nothing is done, in the next few years the air quality will be detrimental to health, according to the trend established directly between traffic and pollution. The second is that there is a city (Daniel's) where air quality is improving every month and traffic congestion is decreasing. After analyzing the data, Sara has realized that the application of IoT in Daniel's city can be an example that can be extrapolated to other cities in the country.

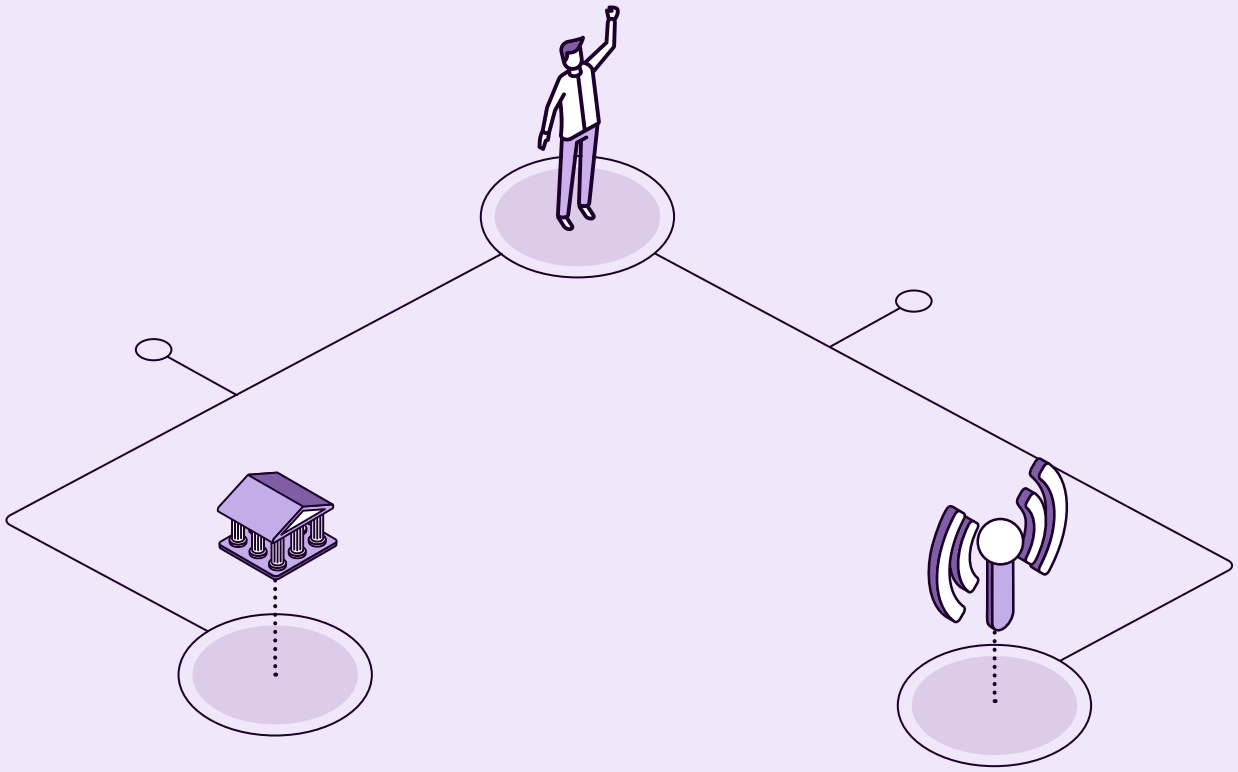
EXAMPLES

Click on each flag or icon to go deeper.

Belgium
Blockchain use case

European Union
Strategy for emergent techonlogies

Spain
National Strategy for Artificial Intelligence



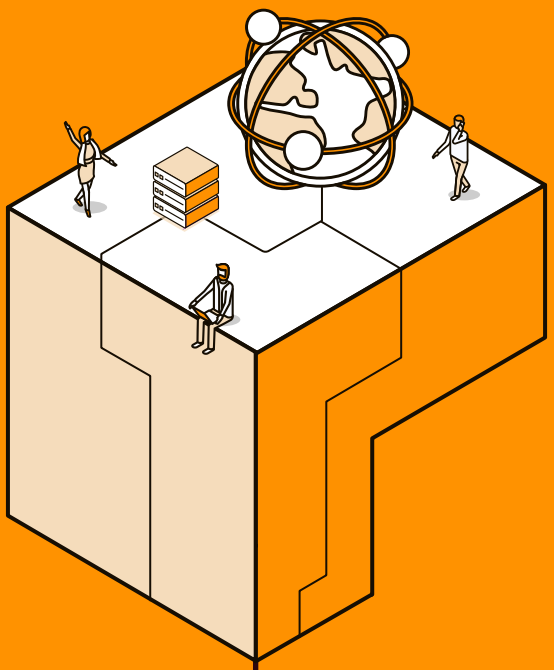
INDICATORS

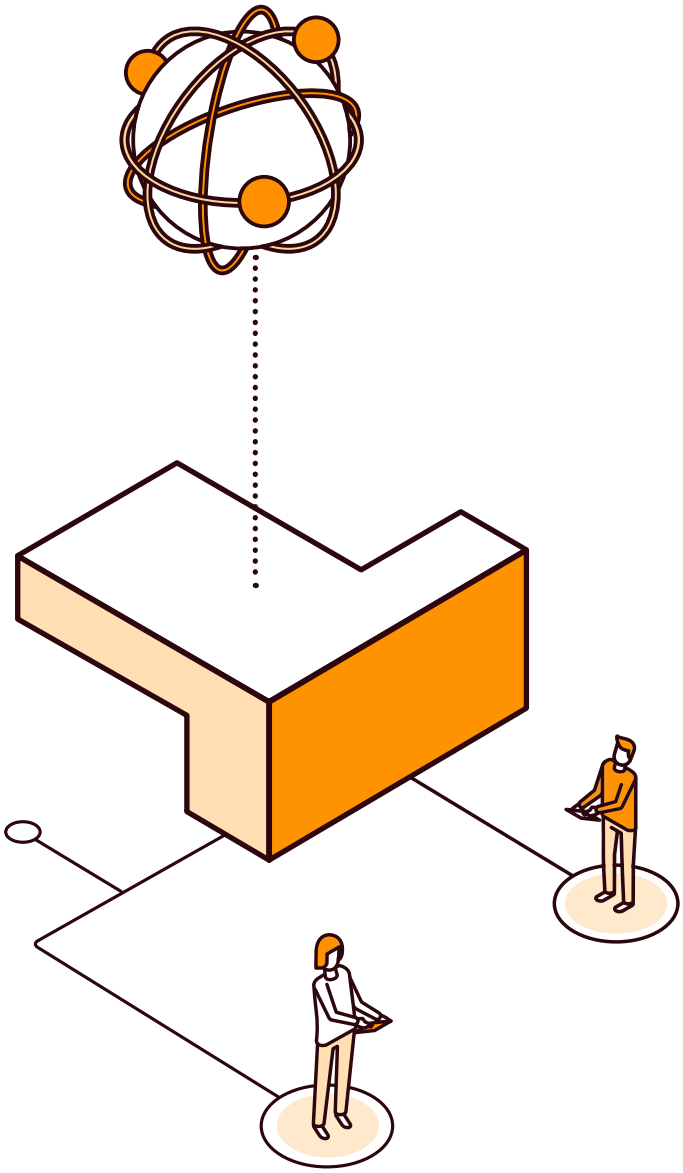
These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are disruptive technologies applied in public administration?
- Is an Internet of Things integration platform available?
- Is the information collected and exploited by the public administration?
- Is a data governance office available?
- Is it considered necessary to automate basic and repetitive processes?

05

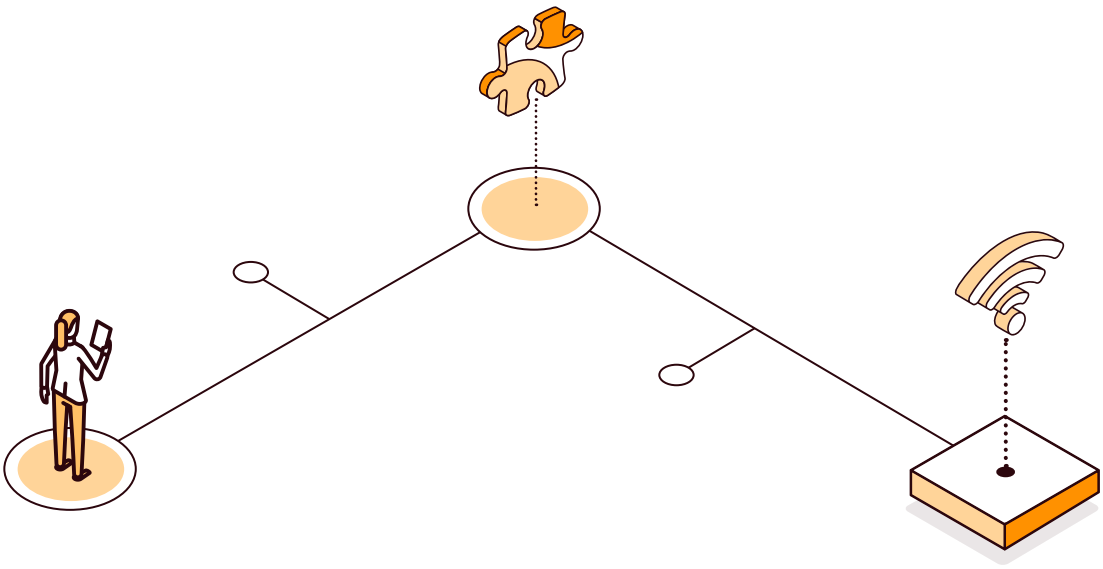
New digital processes and services





5.0

Introduction



The world is undergoing a major transformation: from the industrial society of the twentieth century to the digital society of the twenty-first century. In this era, the irruption of technology and digital technology has transformed the models of living, working, relating to others, etc. This change brings positive prospects for economic and social development, as it makes it possible to adapt the public services offered to the needs of citizens. This should be the goal: to benefit citizens.

A generalized challenge and objective of all public entities is to improve citizen service, as well as to increase the amount of digital services offered through the different electronic offices. Unfortunately, many of the problems that citizens have with the traditional administration are repeated in the digital world, which has even less justification than in the physical world, since technology provides tools that really bring institutions closer to the people.

The digital transformation of public administrations goes beyond the fact that a government has a web page, or that citizen attention is enabled through an email address. A restructuring and redefinition of all processes is needed, as well as training civil servants in this new perspective that seeks to bring the administration closer to the citizen—that is, to promote the electronic processing of administrative files from their beginning to their resolution, without conversion to paper at any stage of the chain.

To this end, it is important first to analyze and simplify work procedures prior to their digitalization, incorporating those functionalities that may be demanded (new forms of access, greater security, among others) and eliminating redundancies and duplications.

Technology should be understood as a tool that facilitates and enhances all these processes. For example, it cannot be said that e-health means having an appointment application, but rather that technology and the renewal of processes should facilitate all areas of the healthcare system: doctors should have their patients' medical records digitized and be able to consult data at any time, technicians who carry out tests should be able to prepare reports in the patient's record, patients should have easy access to reports, appointments can be managed through an appointment system to avoid queues and unnecessary waiting, etc. With digital transformation, the way citizens and states relate to each other is completely different. Therefore, not only the ICT units must be involved, but also the processing units, which are the necessary leverage to make the change a reality.

From the point of view of the administration, digital transformation involves the electronic processing of all activities and phases of administrative procedures. The digital work of public administrations will bring a new value, the generation of consistent and homogenized data, as well as associated information. Thus, it will be possible to monitor the activity of public services, in order to know and control the functioning of the administration, as well as the analysis of the results, with a view to facilitating government decision-making.

From the citizens' point of view, it completely changes the way they relate to public administrations, helping to bring public services closer to them. However, for citizens to use digital services in preference to traditional alternatives, it is important that they are simple and easy to use. In this way, it will be possible to forget the long queues of people outside public buildings to carry out a procedure, the people who have to go from window to window passing through three or four departments to obtain a certificate, the aid that does not reach the disadvantaged due to lack of easily accessible information, among other cases.

There must be multiple channels to provide services. In addition to face-to-face service, telephone service, and the web channel, citizens are increasingly inclined to use mobile platforms and social networks to access services or interact with providers, but the citizen's vision should not stop there. The language must be adapted for their understanding, since it is common for administrative procedures and documentation to have a "legal" language and operation, far removed from everyday language, which—once again—increases the gap between citizens and institutions, something that must be avoided.

The new digital public administration is open twenty-four hours a day, seven days a week. Services must be available at any time, from anywhere, and through any device (computer, digital tablet, cell phone). Thus, citizens will be able to start an administrative procedure easily, check the

status of their file, pay taxes and fees, download documentation (university degrees, medical certificates, etc.), manage appointments with the different public administrations and have all the information on available public services at their disposal.

The vision of the citizen as an individual must be respected, and this is achieved by avoiding asking for the same data in each case or in each interaction, or—also common—avoiding providing different information or services depending on the channel used (face-to-face, telephone, or digital). Therefore, it is worth considering the importance of multichanneling, or the need for issues that are currently simple, at least in the private sector, such as electronic payments or collections, to be simple in the public sector as well.

It is also essential that the digital public services provided are comprehensive, regardless of which public administration has responsibility for the parts of a service. While it is true that a country's administration is a large complex entity, with competencies divided into sectors or at the territorial level, the vocation of citizen service must insulate society from that complexity, so that citizens do not have to know the internal structure of the administration in order to access public services.

Given the above, once the lead institution has laid the foundations and has identified, designed, and implemented common services for the provision of digital services, each sector of the administration must be able to establish business models in conjunction with interested agents to provide a comprehensive service to the citizen. Thus, having a citizen folder that encompasses all the procedures carried out with the public administration is an essential milestone. With this vision, it is necessary to strengthen interadministrative collaboration with initiatives that exist in practically all countries, such as not requesting documents that are in the possession of the public administration or having the organizations in charge of collecting them—something that, by the way, is almost never done.

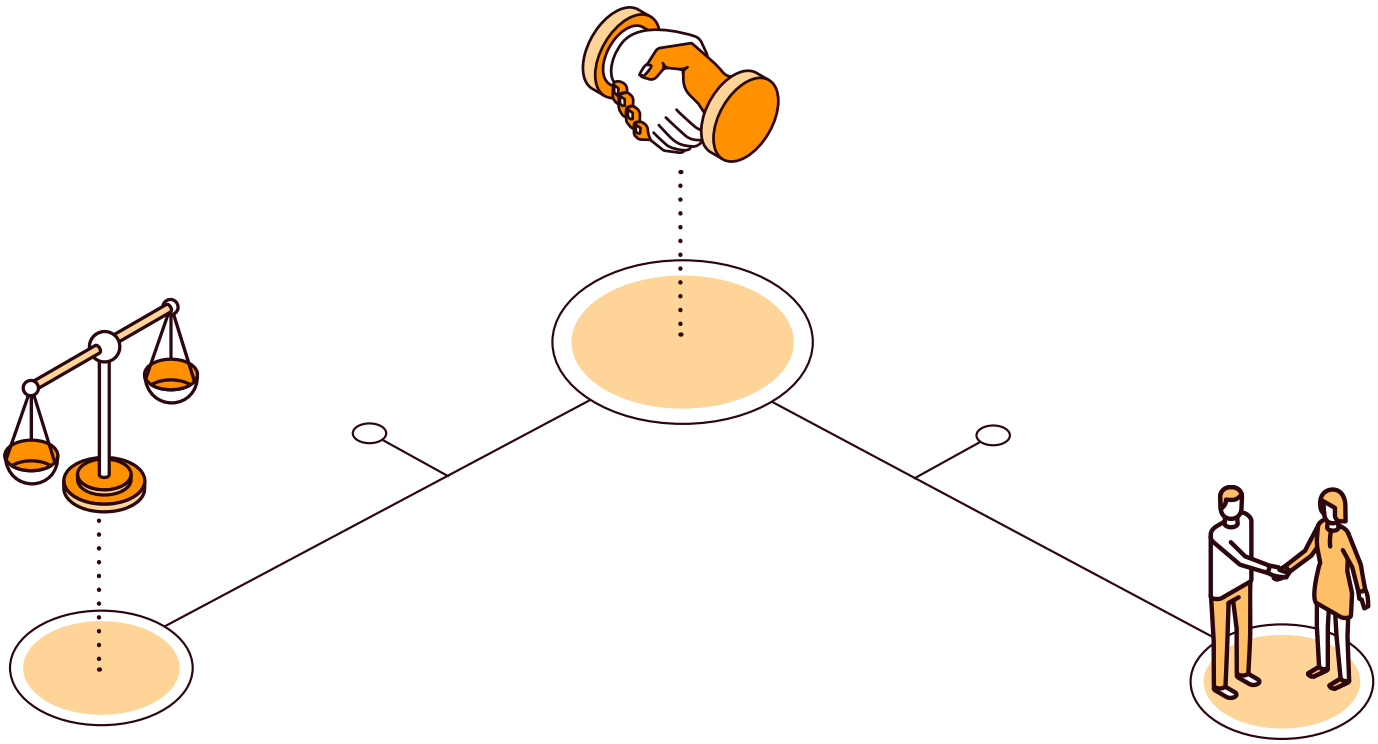
Likewise, something particularly valued by citizens is the unification of government information, the possibility of carrying out procedures online, monitoring the status of procedures and the consultation of data by citizens. For all these reasons, more and more frequently, and with good success stories, unified government information portal projects are being proposed, which improve the traditional model of ministerial and departmental websites that, rather than serving the citizen, seem to be oriented toward the promotion of the organization itself.

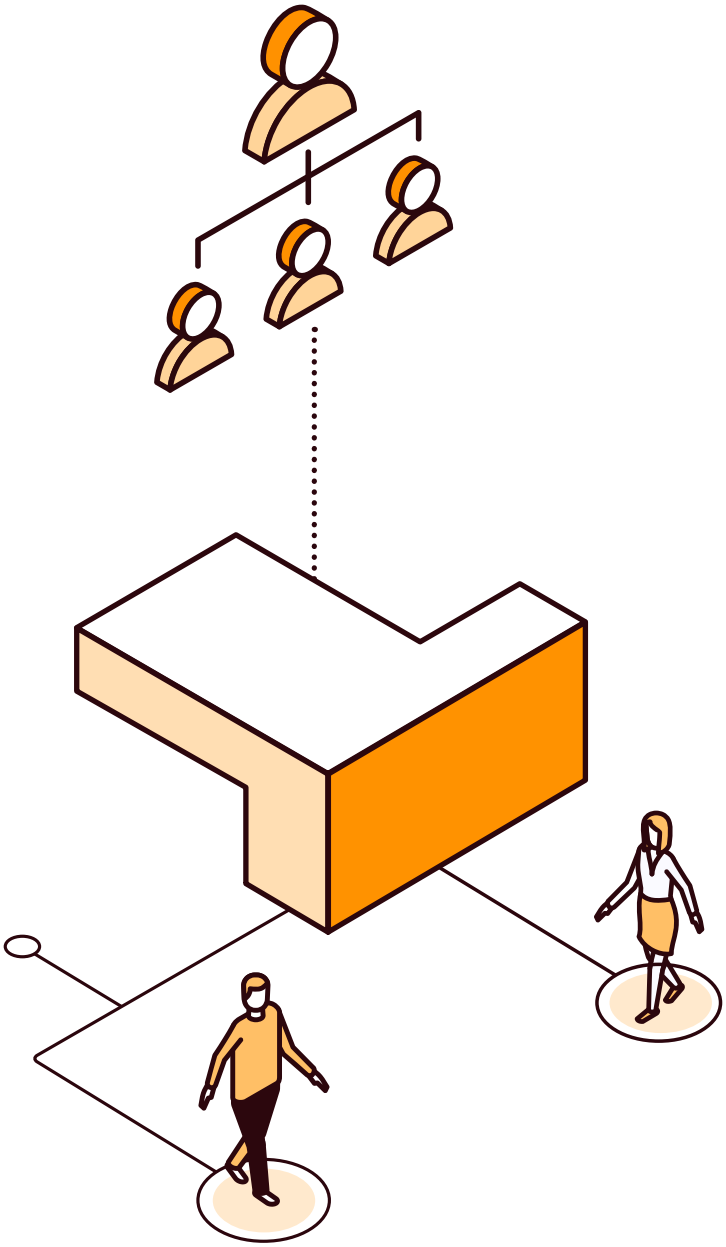
However, in order for citizens and businesses to prefer to use digital public services instead of going in person to government offices, as well as for public officials to prefer to use digital media to perform their functions, it is necessary to know their opinion of these tools and establish indicators to determine their level of satisfaction in order to provide adequate responses to their requirements.

Transparency, open data, and the principles of good governance, such as citizen participation, are

also part of this area, in which more and more countries are promoting an orientation of their digital services not to the unit that provides them, but to the citizen who receives them. In this way, they achieve the recognition of the latter in the valuations and use of information systems, something fundamental in the digital transformation project of a country and a government. This is true even though the main consumers of open government information are organized civil society, the press, the private sector, and academia, and not "ordinary" citizens.

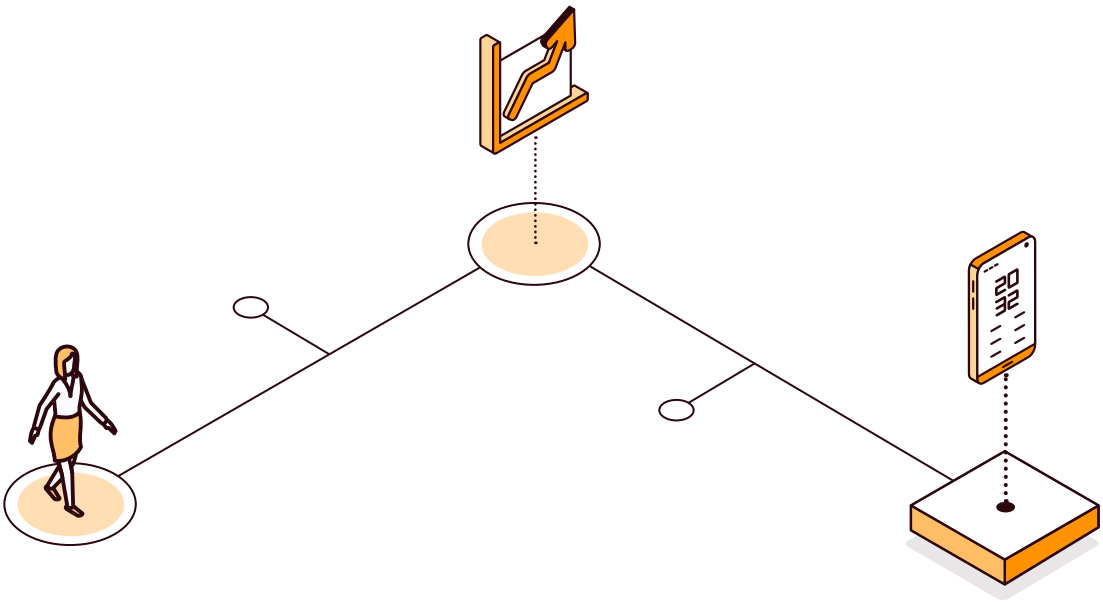
In line with this idea of measuring and evaluating digital transformation processes, there are various international organizations that carry out reports and surveys to identify whether these transformation processes are being carried out in the best possible way. In this regard, the United Nations has been conducting the United Nations E-Government Survey since 2001, the latest edition of which was published in 2020. This is the only report that reflects the state of development of digital government in all member countries of the United Nations, comparing them in their different stages of progress. The European Commission also produces a report, the eGovernment Benchmark study, that compares the progress in digital administration of the member states by measuring the availability of digital public services. The following section will go into more detail on this aspect.





5.1

From the point of view of the administration



The digital transformation of public administration must establish its foundations in a change of mentality, which must reach people, adapting behaviors and the way of working to the new realities and demands. In other words, it is no use trying to replicate in digital the same work in the same way as it was done before on paper.

It is necessary to promote this cultural change so that users are aware of the benefits of the transition from the paper world to the electronic world in their professional activity. Their participation is therefore essential, and their proposals must be taken into account by the institution in charge of the digital transformation when defining the new processes, encouraging their training and knowledge of the projects and the technological tools made available to them (i.e., promoting their complicity in the management of the change).

With the above in mind, a training plan must be designed for public administration personnel so that it contributes to the progressive adaptation to the needs and novelties of their new digital work, as well as the new organization and new digital processes. In turn, this instrument should provide the knowledge of computer applications and address the needs of an adequate attention to the public adapted to work in digital, with the aim of improving the skills and professional development of the staff in the service of public administrations. This is a key element to assimilate the continuous changes in tools and ways of working.

Once the digital transformation strategy has been defined, the new processes are already optimized and simplified. In this way, the civil servant of the national, regional, or local public administration that is going to start working in digital will obtain a higher performance in the work developed, eliminating tedious steps that have now been automated, achieving greater value, with less effort, thus generating greater efficiency and work capacity.

THE GOAL IS NOT STRICTLY TECHNOLOGY; THE GOAL IS TO MAKE THE PROCESSES DIGITAL

- Officials no longer have to deal with so many people coming to the service windows but work with digital inboxes where they can find the documentation submitted by citizens.
- Communication between public administrations and citizens and companies is mostly done electronically, with the efficiency and speed that this means.
- Documents that are still submitted on paper are digitized and incorporated into the electronic file in the administrations.
- In order to prepare the documentation and carry out the processing of files and other administrative procedures, the technological applications and tools designed for this purpose will be used.
- Support is provided for all the additional needs surrounding digital processing, such as consultation of files or citizen data, forwarding between administrative units or between public administrations, etc. The system is interoperable with all available applications and systems.
- The digital signature system is incorporated, with the appropriate authentication instruments.
- Unnecessary steps are eliminated, and tedious and repetitive tasks are automated, thus reducing administrative processing times.

All this results in a significant improvement in customer service by reducing and simplifying transactions, offering services in a proactive manner, providing greater options for access and participation, providing greater clarity and transparency, and acting more quickly.

In addition, the civil servant, by performing his work entirely in digital, can generate sufficient information and data necessary for the institution leading the digital transformation, in conjunction with the different vertical sectors, to make rational decisions, based on real figures and results, not on the perceptions of civil servants or citizens. The data can demonstrate the need to make changes in regulations, operations, personnel, or technological infrastructures and tools, with the aim of offering citizens more efficient, safer, and closer digital services.

ADMINISTRATIVE PROCEDURES: PAPER VS. DIGITAL

Beginning of the procedure

Procedure

Closing and notification of the proceeding

Beginning of the procedure

Paper-based administration

- In a paper-based administration, the official is at a counter, providing service to the citizen during specific business hours, with the limitations that this entails.
- When a citizen approaches a customer service window, he must take into account the opening hours, go to the corresponding building, and bring with him all the documentation he thinks he will need already prepared to present it.
- The officer has to review all the data and documentation submitted by the citizen, and manually stamp and record all the data in order to initiate the procedure.

New digital public administration

- The official can consult from his computer, at any time, his inbox. There he will find all the documents submitted by citizens. He does not have to do any manual registration, since the data is already registered. In addition, the systems themselves take care of putting the stamps to give the time and date of entry of the file. The time that the civil servant used to spend on these tasks can be used to study the documentation submitted to verify whether it meets all the requirements to be able to initiate the administrative procedure in question.
- The case of the citizen will be dealt with in more detail in the following point, but we can already advance that he will be able to initiate the procedure at any time, from any place, without the need to travel unnecessarily, or to adapt to limited opening hours.

Procedure

Paper-based administration

- The processing of the procedure is complex. The documentation that forms part of the administrative file has to be passed from one instance to another. The official who registers the file has to accumulate all the folders and transfer them to the offices of his colleagues who are going to carry out the processing of the procedure. The official often has to push a trolley with all the files, given the large volume of these. This movement of files through the administration's facilities is not safe, since it is relatively easy to lose documentation.

- In the information analysis carried out by the officials in charge of processing the administrative file, they may conclude that it is necessary to request information from other public administrations. In this case they would draft the request for information and prepare it for sending on paper to the other public administration. This documentation would go back to the official in charge of incoming and outgoing documentation, and he would issue the request for information.

- Once the request for information arrives at the destination public administration, a similar process would begin: registration of entry, transfer of the physical file to the unit in charge of providing the requested documentation, analysis of the information and preparation of all the necessary documents to be sent to the public administration that requested it. Then, again, the entry registration process would be repeated at the administration that made the request. The civil servant would have to manually register the receipt of the documentation and again distribute the files to his colleagues who are in charge of processing them.

HOW DOES IT LOOK? CUMBERSOME? THIS IS THE CASE TODAY IN MANY PUBLIC ADMINISTRATIONS, AND THIS MANUAL AND COMPLEX PROCESS CAUSES DELAYS IN THE PROCESSING OF ADMINISTRATIVE FILES.

New digital public administration

- The process is much shorter and simpler. The officer who initiated the procedure transfers it to the responsible unit for processing with a single click.

- The processing of the file and the analysis of the information could begin immediately, since the officer would have all the documentation submitted by the citizen at that very moment.

- If, after the information analysis, the official in charge of the processing needs additional information from another public administration, he can request it with a single click, and receive it quickly and easily in his inbox. No paperwork, no need for the original documentation to go from one place to another with the risk of loss and deterioration, but the information is stored in a secure way.

CAN YOU SEE THE DIFFERENCES? THE DIGITAL PROCESSING OF ADMINISTRATIVE FILES IS AGILE, EFFICIENT, AND SECURE.

Closure and notifications of the transaction

Administración en papel

- Once the official has resolved the file and has the final resolution already prepared, the citizen who initiated the file must be notified. However, for the resolution to be valid, it must first be signed by the person in charge of the administration.

- There is a high-ranking official who must spend several hours a day reviewing paper documents and manually signing them one by one.

- The official who has resolved the file has to transfer the resolution, with all the associated paper documentation, to the offices of the civil servant who is in charge of making the notifications.

- The officer receiving the documentation has to manually record the necessary information to generate the output of the notification and prepare the mailing to the citizen.

- The citizen will receive the documentation by mail several days, even weeks, later.

- In the meantime, the official has to take the entire file folder, with all the documentation that has been generated during the processing, to the physical archiving unit. Again, one sees

a civil servant pushing a cart full of folders with the files to the archiving units to look for a space to store the files, with all the time and effort that this entails. Sometimes, given the lack of physical space in public administration buildings, it is necessary to have a physical archive in another building, public or private, hire or arrange a transport service, and store the documentation in the facilities where the physical archive is located.

ONCE AGAIN, IT CAN BE SEEN THAT THE PAPER PROCESS OF RESOLVING AND CLOSING AN ADMINISTRATIVE FILE ON PAPER IS TEDIOUS AND INEFFICIENT.

Nueva administración pública digital

- The official has processed the file in the processing system and has drawn up the resolution that ends the procedure. He gives legal validity to this resolution by digitally signing the document; in fact, the person responsible for signing resolutions, with the digital signature system, can select several resolutions and sign them at the same time, in a single step.

- Once the resolution is digitally signed, the official, at the click of a button, notifies the citizen in a simple and fast way.

- The citizen, from his device with internet connection (a computer, a tablet, or even his cell phone), immediately has available the notification of the resolution of the administrative file that he initiated.

- The official in charge of resolving the file, once notified, can easily archive the file from the processing system itself.

ONCE AGAIN, THE DIFFERENCES ARE EVIDENT, AND IT CAN BE SEEN HOW THE WORK OF CIVIL SERVANTS IN THE SERVICE OF THE PUBLIC ADMINISTRATION IS SIMPLIFIED AND STREAMLINED.

TANGIBLE BENEFITS OF DIGITIZATION

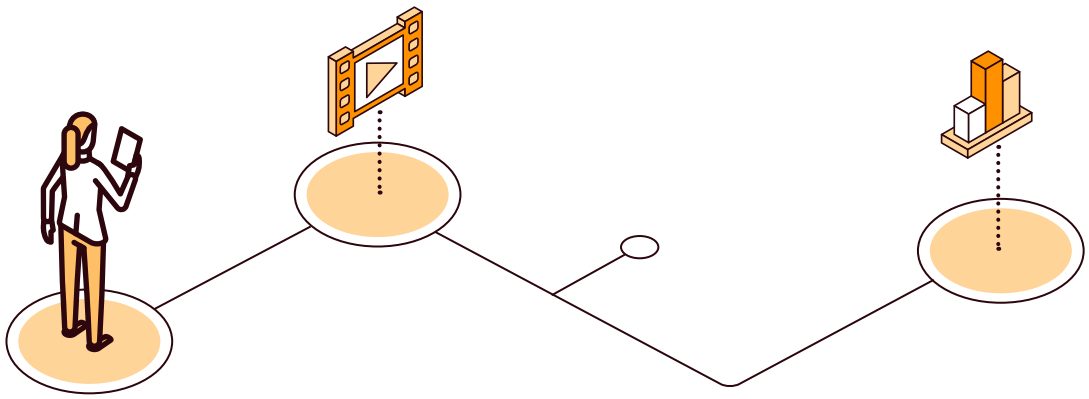
- It represents a breakthrough in energy efficiency, derived from the reduction of paper.
- It allows a more agile processing, reducing human errors, simplifying tasks, and avoiding undue delays.
- It offers real-time monitoring of the processing of files, which facilitates consultation for both interested citizens and the officials involved in the files, who can easily find out the status of a file.
- It reduces paper transit between public offices and storage space, which also means greater security, since loss and deterioration of paper files is avoided.
- It provides greater security through the use of electronic signatures, since the confidentiality, integrity, and authenticity of the information is guaranteed at all times.
- It achieves a more efficient public service, with a significant reduction in processing times and management of files, and with greater efficiency in the use of public resources.
- It makes it possible to improve existing public services and generate new services that bring the public administration even closer to the citizens as a whole.
- It replaces manual tasks, allowing civil servants to focus on tasks that require more human input. This increases the satisfaction of civil servants with their work, as they feel that they contribute value.
- It enables something that has become more valuable than ever in times of the global pandemic caused by the COVID-19 virus: teleworking. This is made possible to a greater or lesser extent depending on the degree of progress of the digital transformation of public administrations; at the time when work processes are done digitally, it opens the possibility of working from anywhere, at any time, and also gaining access to digital public services with security and guarantees. Telework is here to stay, in a digitally transformed public administration, offering digital services to a permanently connected society. It is essential to ensure that even in the event of force majeure such as natural disasters, pandemics, terrorism, etc., public services will not stop. The benefits of implementing online medical consultation in public healthcare in this pandemic year can be taken as an example: the possibility of avoiding citizens having to go to medical centers and hospitals for small consultations or routine check-ups would have relieved the pressure on first-level healthcare.

A CLOSE LOOK AT DIGITIZATION

The digital transformation is so important that organizations around the world are elaborating indexes that periodically measure its advancement in different countries. These indexes, through certain previously defined indicators, collect the degree of progress and evolution of the digital transformation, in order to know the current situation and to anticipate the challenges to be faced in the future.

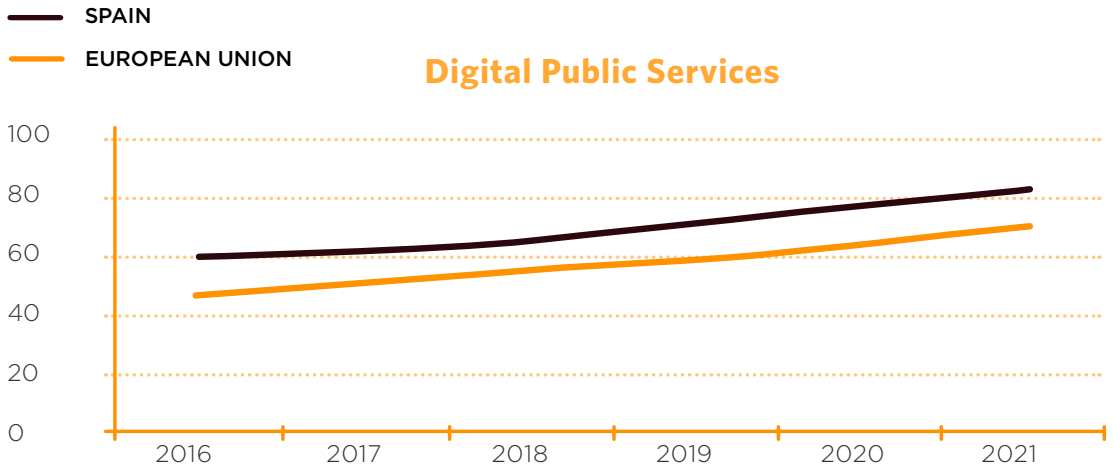
For example, in Europe there is the DESI report (Digital Economy and Society Index)[42], which monitors the evolution of the European Union member states in digital competitiveness through five indicators:

- Connectivity
- Human capital
- Internet use
- Integration of digital technology
- Digital public services



42. In the DESI 2020 report (https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi), Spain ranks second in digital public services, above the EU average.

Digital Public Services	SPAIN		EU
	Rank	Score	Score
DESI 2021	7	80,7	68,1
DESI 2020	2	87,3	72,0
DESI 2019	4	80,9	67,0
DESI 2018	4	76,6	61,8

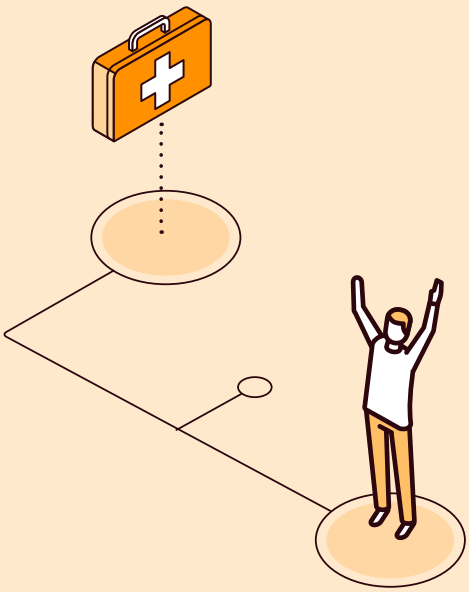


Another organization that analyzes digitization is the United Nations, which annually surveys all 193 member states to determine the scope and quality of online public service.[43] In 2020 it concluded that the leading states in telecommunications infrastructure and human capacity are Denmark, Republic of Korea, and Estonia, followed by Finland. Also, the OECD (Organisation for Economic Co-operation and Development) annually presents a digital government index, in which it provides an analysis of the results of its own digital government policies[44].

43. https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey
44. https://www.oecd.org/gov/digital-government-index-4de9f5bb-en.htm

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

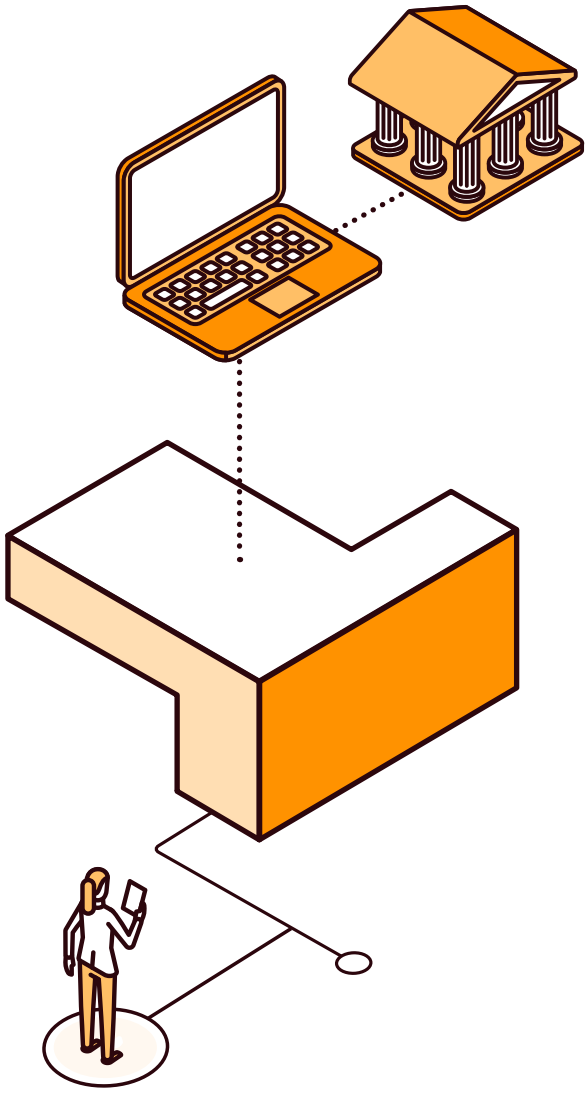


Citizen
Camilo

Camilo wants to apply for one of the social health programs offered in his country. He works two jobs and takes care of a young daughter, so his free time does not coincide with the opening hours of the organization that processes the aid. He goes online and checks that, among the services offered by the Single government portal of the public administration, is the procedure to apply for access to the social health program. Once he has checked the documents to be submitted, Camilo enters his citizen folder and can quickly download the certificates required to qualify for the health program. After downloading all the information onto his computer, he proceeds to complete the application process for access to the social health program and writes down the application number given to him by the program, which he can use to check the status of his application at any time. The next day he notices that the official who is processing the application asks for a certificate that he was missing. At that very moment, Camilo accesses the citizen folder again and downloads the requested certificate, so that he can correct his application that same day. Camilo is satisfied with the simplicity and speed with which he has been able to complete the procedure with his public administration.

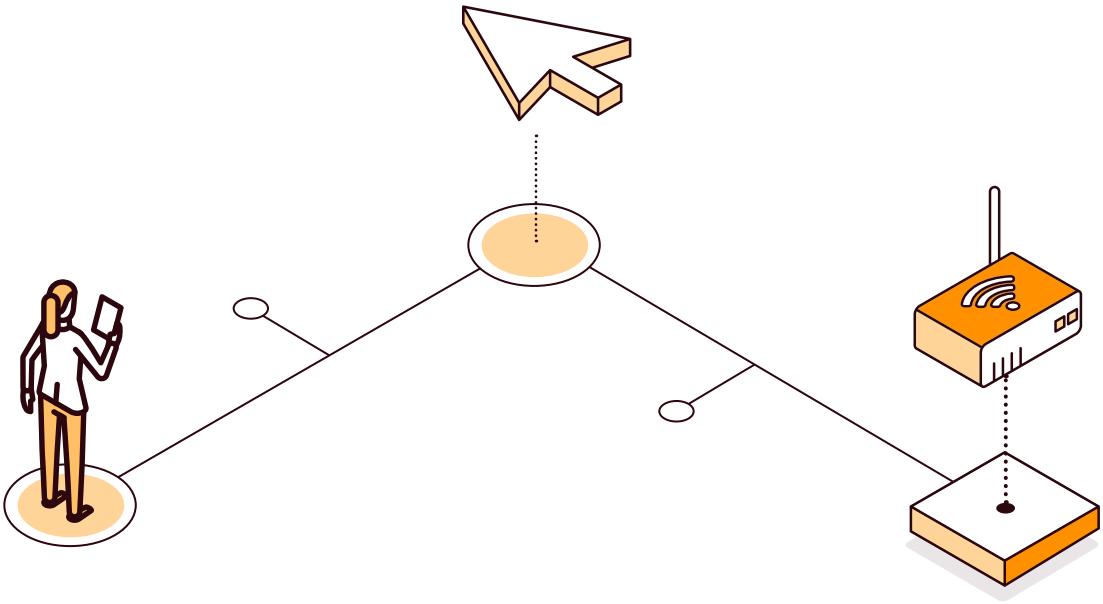
Vice minister of health
Sara

Sara came to the health sector knowing that in other sectors, such as education, applications for scholarships have been available online for years through the single government portal. Although she knows that the process of accessing the public health program is more complex, she intends to digitize it and include it in the catalog of procedures offered by her ministry. She is satisfied with the result, because in the first year the number of successful procedures has increased, and processing times have been reduced by 25 percent.



5.2

Citizen access to digital services



At a time when citizens are accustomed to obtaining anything at the click of a button, digital public services make it possible to provide more agile solutions with the immediacy that twenty-first-century society demands. The digital transformation of public administration contributes to modernizing work processes, institutional communication mechanisms, and the relationship with citizens, to provide a higher quality digital public service, increasing people's satisfaction. Therefore, in the process of digital transformation, technology is not the goal, but the lever to improve the perceived quality, effectiveness, and efficiency of public service.

Improving citizen service is a challenge, and in turn is the goal of all public entities. Therefore, the provision of quality public digital services should be an overall objective that the institution leading the digital transformation should constitute as the backbone and coordinate with all vertical sectors to take advantage of synergies.

In this order of ideas, it is necessary to change the vision of silos that exists in the provision of public services, the "go to the other window" has to become history. Citizens do not care about competencies, levels of administration, or internal differences between entities or departments of the same institution; what they want is to receive quality service and to carry out as few procedures as possible, without being suffocated by bureaucracy.

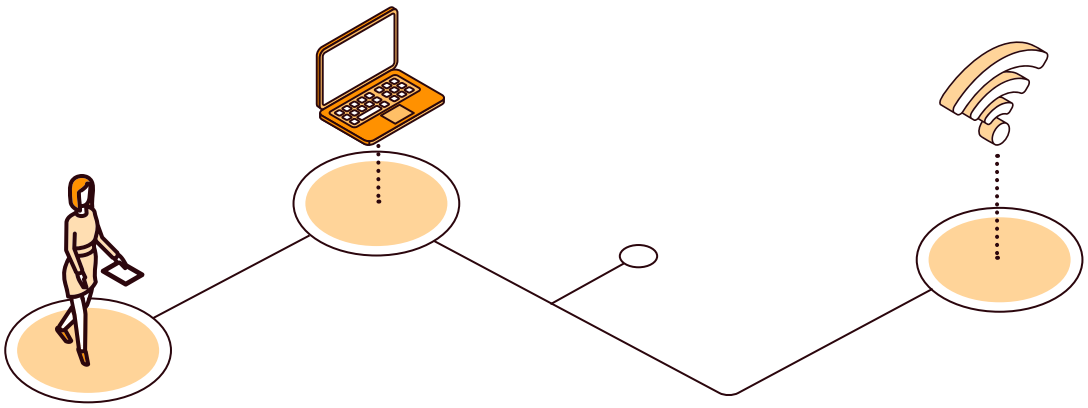
With this vision, it is necessary to strengthen interadministrative collaboration with initiatives that exist in practically all countries, such as not requesting documents that are in the possession of the public administration and leaving it to the organizations themselves to collect them whenever possible.

- *Example:* When a citizen applies for a scholarship, he can give his consent for the education department in charge of processing the application to ask the tax information officer for data on his annual income level, in order to check whether or not he meets the established scales for the granting of the scholarship.

Public administrations must prevent citizens from bearing administrative burdens that are not strictly necessary, improving their productivity, avoiding travel as much as possible, and making administrative procedures as agile and simple as possible. The digital transformation of public administration makes it possible to meet these objectives, and profoundly changes the way in which citizens and administrations relate to each other.

In today's age, citizens use the internet to manage a large part of their social relations, information, exchanges, and business. This is not a matter of fashion, but rather citizens see advantages in digital management over doing the same things in the traditional physical world.

- *Example:* A citizen has to apply for unemployment benefits. In a traditional administration, he would have to physically go to the unemployment office at a specific time that is determined for him, and he cannot choose. Once there, he would have to face a long wait. Images of citizens queuing outside a building are well known, as everyone accumulates at the same opening hours. However, in the new digital administration, the citizen could apply for unemployment benefits using a cell phone with a simple internet connection, something that is accessible to a big part of the population (66.6 percent of the world's population has a cell phone by 2021).



NEW SERVICES

Digital public administration changes the life of citizens and produces an explosion of public services, which can be adapted to the needs of these people, and which can be accessed easily. Thus, they can count on services that are just a click away, an administration open twenty-four hours a day and seven days a week, geographical and physical independence in accessing public services, and a public service close to them and at low cost.

Among these new basic services for the digital world are the following:

Multichannel system

Single government portal

Citizen's folder

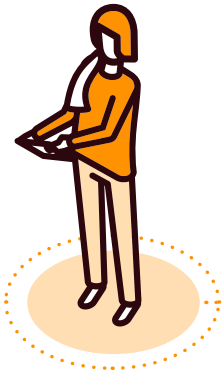
Agenda system

Procedures catalog

Transparency

Payment gateway

Sectorial services



- **Multichannel system:** It is essential to respect the right of citizens to choose the means of interacting with the public administration. It is therefore necessary for citizens to be able to contact the administration through various channels and to choose which channel is their priority, both for sending and receiving information.

- **Single government portal:** This service is related to the centralization of information and easy access to it. It is a website designed to offer citizens a solution to the great dispersion of public administration information in different portals and web pages, which caused difficulties in citizens' access to administrative procedures and services, duplicated information, and lack of adequate coordination. More and more frequently, and with good success stories, unified government information portals are being proposed, which improve the traditional model of ministerial and departmental websites that, rather than serving the citizen, seemed to be oriented toward the promotion of the organization itself.

- **Citizen's folder:** Something that is especially valued by citizens is the unification of government information, the possibility of carrying out procedures online and tracking the status of procedures and data consultation. With digital administration, a citizen folder can be built, with secure access, where citizens can have all their public information centralized, such as certificates of studies or civil status, tax payments or collections, or health data. Likewise, this would be the ideal way to communicate with the children's school, access the processing status of the procedures in which they are interested, etc.

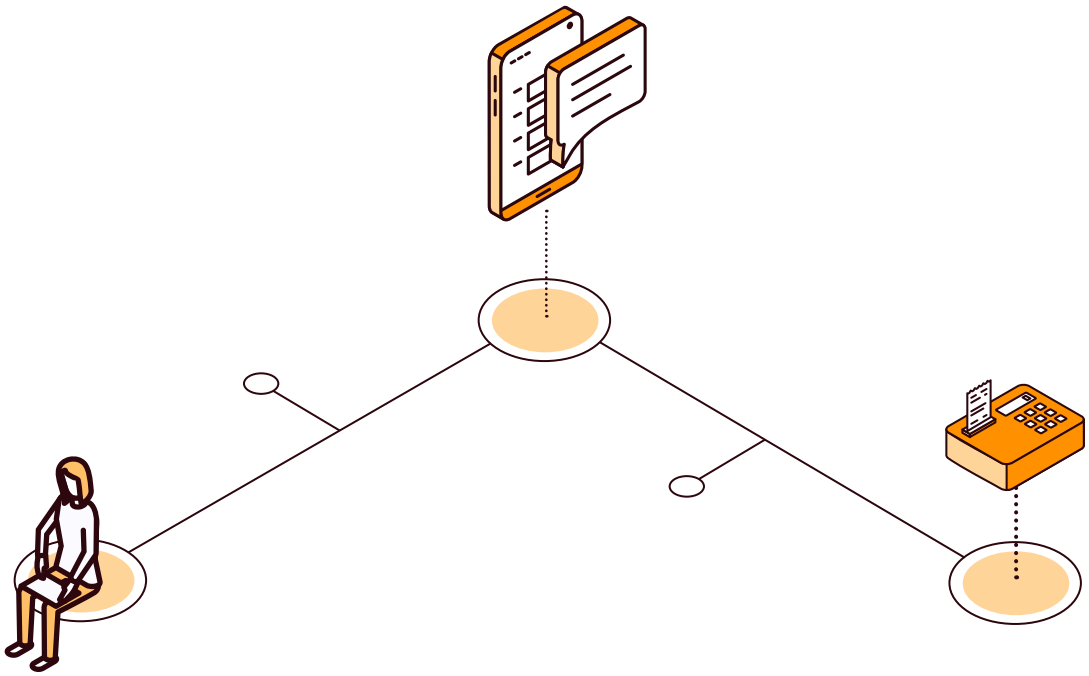
- **Agenda system:** This is an aspect that should also be included in the citizen's folder. Consider the multitude of appointments with the public administration that occur from birth: birth registrations, medical consultations and check-ups, obtaining an identity card, driver's license, marriage registration, and so on. In this context, it is essential to have a system that allows centralizing and simplifying all the appointments that citizens may have with the administration in a single point. To this end, it is necessary to provide the possibility of registering new appointments, modifying them, consulting, and even creating alerts so that citizens can be sure that they will not miss any of them.

- **Procedures catalog:** Given the multitude of services and administrative procedures that exist in the public administrations of a country, it is essential to have the possibility of consulting, from the Single government portal, the catalog of procedures and services that the public administration makes available to citizens. The catalog should inform, for each procedure, the characteristics, the way to carry it out, the deadlines, the necessary documentation, and reference regulations. This is one of the contents that arouse the greatest interest among citizens.

- **Transparency:** As mentioned above, one of the benefits of the digital transformation of public administration is transparency. Therefore, it is necessary to have an information system that reinforces the transparency of public activity and serves to guarantee citizens' right of access to information. The system must also establish the obligations of good governance that public administrations must comply with.

- **Payment gateway:** One of the most difficult procedures with the public administration for citizens are payments. Public services have a multitude of fees, taxes, and other types of payments that, if made in person, force people to travel both to the public administration and to banks. It is therefore essential to have a single payment gateway for the entire public administration—firstly, to make it easier for citizens, together with the electronic procedure, to pay the associated fees and taxes, and secondly, to facilitate transparency and control of the accounting situation of public administrations.

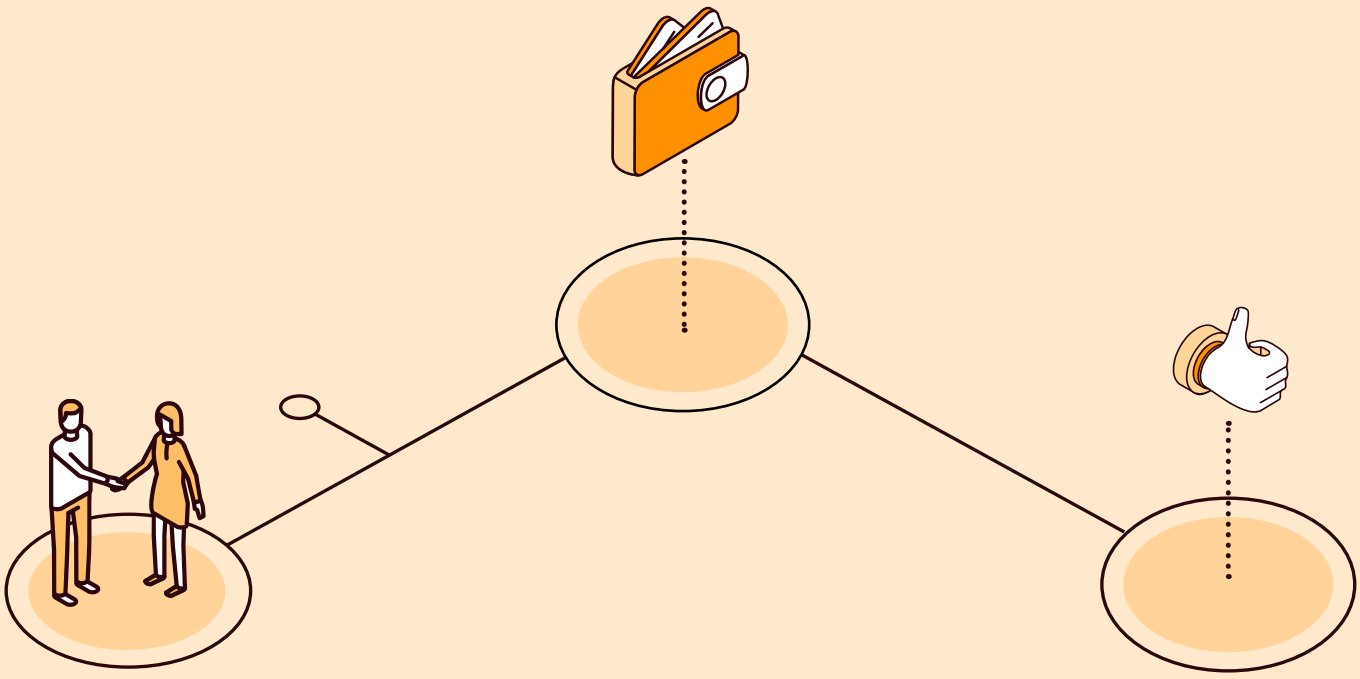
- **Sectorial services:** Once all the common public services have been defined, the last step is to make them available to the different sectorial administrations, so that they can incorporate their own electronic services to the catalog of public administration procedures.



SUCCESS STORIES

Estonians can access 99 percent of their administration services via the internet, thanks to a digital ID card containing their digital signature and an electronic chip containing all their data, which cannot be shared without their consent. Registering a company, renewing a driver's license, consulting medical prescriptions and accessing medical records, checking children's grades or communicating with teachers, and voting are all procedures that can be carried out *online*.

Spanish public administrations have digital government elements such as a unified folder for citizens, where even the different autonomous communities are integrated. It is also worth mentioning a unified mailbox for notifications or an identification and digital signature platform common to all administrations.



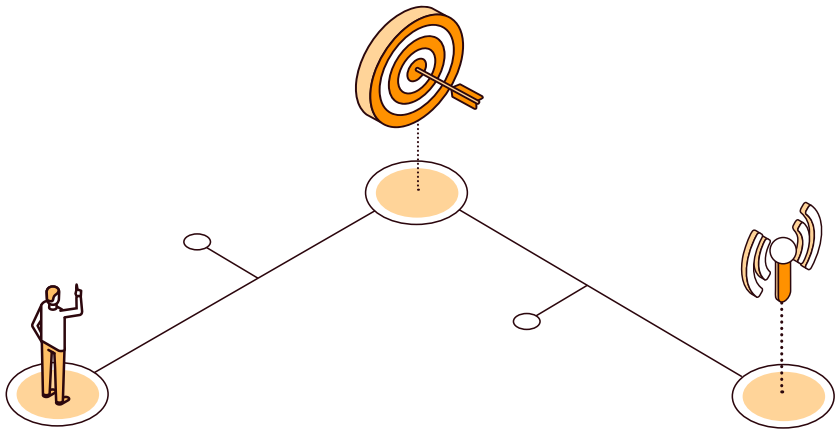
5.2.1 MULTICHANNEL SYSTEM

The digital channel, when properly implemented—following all the principles of human-centered design and based on precepts such as "only once"—is clearly the most efficient and can provide the best service to citizens, even if it cannot always be used, as may be the case if there is no internet connection or if there are disabilities that prevent its use. Sometimes, a web page or web or mobile application is not the appropriate channel due to lack of digital literacy, access costs, characteristics of a particular procedure, or any other reason. For this reason, public entities usually have citizen service offices, as well as an information and/or telephone processing service.

Common services can be developed for use by all institutions in their face-to-face or telephone service. Citizen service must be multichannel (web, telephone, face to face), which often leads to the need to create service centers. The idea is that everything should be integrated, so that if someone initiates a procedure on the internet, they can find out its status by making a call, and if they visit a physical office for any reason, a civil servant should be able to inform them, for example, that the procedure has already been completed and give them the corresponding resolution.

The multichannel system is defined, then, as the set of services and information systems that allow citizen service, not only by electronic means, through the internet, but also by telephone or in person, in an integrated and useful way, both for citizens and public entities.

THE MULTICHANNEL SYSTEM SHOULD BE ACCOMPANIED BY INDIVIDUALIZED AND PROACTIVE ATTENTION.



AREAS OF FACE-TO-FACE CARE WHERE MULTICHANNEL SERVICES ARE USEFUL

- **Integrated citizen services offices:** It is common to set up single points of face-to-face contact where multiple procedures can be carried out, including those of different agencies. For these offices, it will be necessary to have an information system that facilitates the completion of procedures of several public agencies, as well as obtaining information and the possibility of carrying out general procedures (collecting documentation, submitting documentation for any entity, registering, or modifying data of the identification service or national electronic signature, and so on). Therefore, it will be necessary to provide these offices with the possibility of using all the general common services that appear in this document, plus those specific to the management of these offices.

- **Specific face-to-face service offices:** These areas should offer one or more of these multichannel services so that, to the extent of their capabilities, they can facilitate the citizen's management, even in procedures that do not fall within their field of action, and also in the general procedures mentioned above, to be offered, if possible, also through these offices. This can be achieved by allowing certain officials access to common services that integrate citizen information, and even by providing the possibility for officials of a given office to carry out procedures of other entities.

RELATIONSHIPS WITH OTHER SYSTEMS

- **For civil servants:** In order to access the systems that have citizen information, or for civil servants to be able to act on their behalf, they must be identified and know the role they play, for which they must be integrated with the system of roles and profiles of civil servants. All this will allow the multichannel service system to provide maximum value to citizens, and this will result in integration with almost all services, so that citizens can use them in any channel.

- **For citizens:** The multichannel system must be connected to other systems that have information about the citizen, to facilitate access to information from a single point. Thus, the information published in the government's single point should also be accessible by telephone or in an office. Citizen-specific information should also be accessible from the data in the citizen folder, which can be accessed both from the telephone channel and in person through a civil servant. This will include all digital services, such as the collection of notifications and communications, submission of documents, access to files, management of authorizations, etc.

SERVICES TO BE OFFERED IN AS MANY OFFICES AS POSSIBLE

- Digital identity management
- Digital signature management
- Agenda and appointment management for citizens
- Sending documents to any public entity
- Collection of information or documents from any agency
- Access to files of any organization
- Management of authorizations and representations
- Consultation of citizen data, obtaining certificates .

SOME USEFUL SUPPORT TOOLS

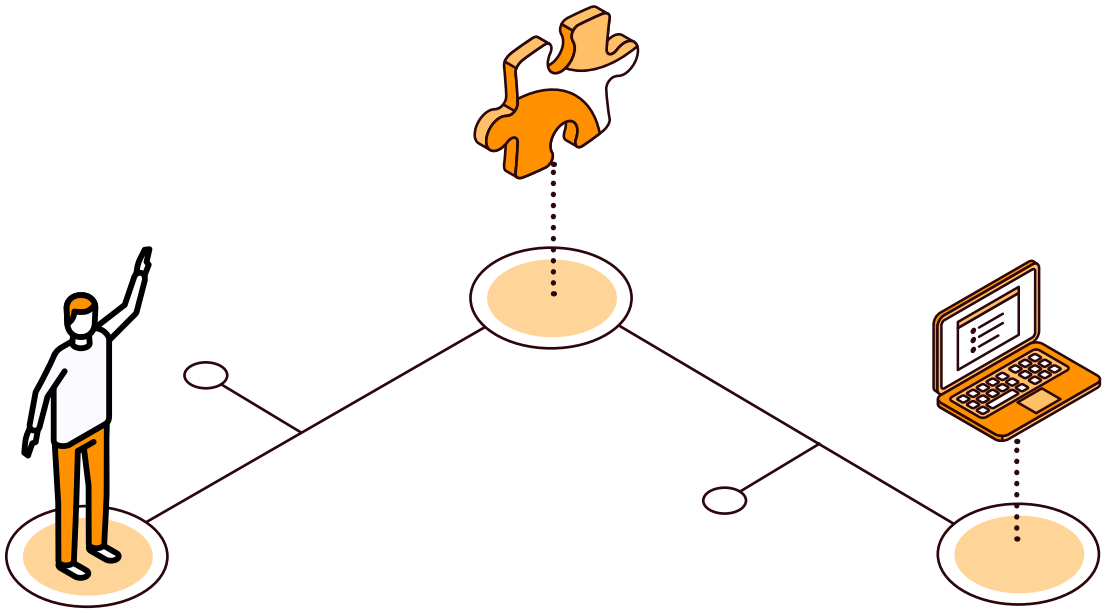
- **Telephone service:** It is of particular interest that a single intelligent voice service number can be used (with a virtual assistant for everything but the most complex, and people for the rest), and that all the associated services are offered to all institutions. This is especially important given the cost and complexity of these services. In any case, one must consider the level of satisfaction that citizens may have with virtual assistants. It is not unusual to have a certain level of frustration with call centers (long waits, cases being referred from one assistant to another, and having to repeat the same details or explanations, etc.).

  The idea is not to eliminate specific customer service numbers, since this is compatible with a general system; the idea is that the intelligent voice system (voice-based customer service, automatic customer service based on artificial intelligence or natural language recognition, IVR [interactive voice response] or menu-based identification and signature systems via telephone) should be used solely to increase synergies, save costs, and offer advanced services. Ideally, many of these services can be provided to entities that, due to complexity and cost, had never considered an advanced telephone customer service system.

- **Totems:** : It is becoming increasingly common to find totems for citizen attention in face-to-face offices. These can offer different services depending on the hardware and software elements they incorporate; in fact, they range from simple totem dispensers to totems that incorporate biometric identification capabilities through fingerprint, facial recognition, and iris reading.

Depending on the services to be offered and, therefore, the security of the information to be protected, the identification elements will have to be increased until the appropriate level of protection is achieved. The most advanced elements, such as facial recognition or iris reading, can be used in combination with preconcerted keys or keys known to the citizen to offer high-level information services, such as access to certificates of personal and sensitive information, as well as for the collection of information or access to files, or as an identification element for the accreditation of physical presence.

- **Quality management:** Knowledge of the citizen experience is key to planning actions aimed at improving the quality of services. In this regard, it is recommended that decision-making be based on inputs generated through both process indicators (service and resolution times, number of steps, etc.) and citizen experience.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo wants to check the status of his administrative file. He has friends who have told him that this can be done conveniently over the internet, but he does not feel comfortable with the computer. He would love to be able to call a phone number to find out the status of his file, without having to go to the office that manages it, which is very far from his home.

Mayor's advisor
Daniel

Daniel, the mayor's advisor, is talking to Adriana, who works in a customer service office. Adriana knows that she can get a lot of information through the internet, as well as certificates, and even carry out national government procedures. What she does not understand is how these procedures are not available in person at the municipal office, to facilitate the attention of the citizens she receives in her office, who are particularly disadvantaged.

EXAMPLES

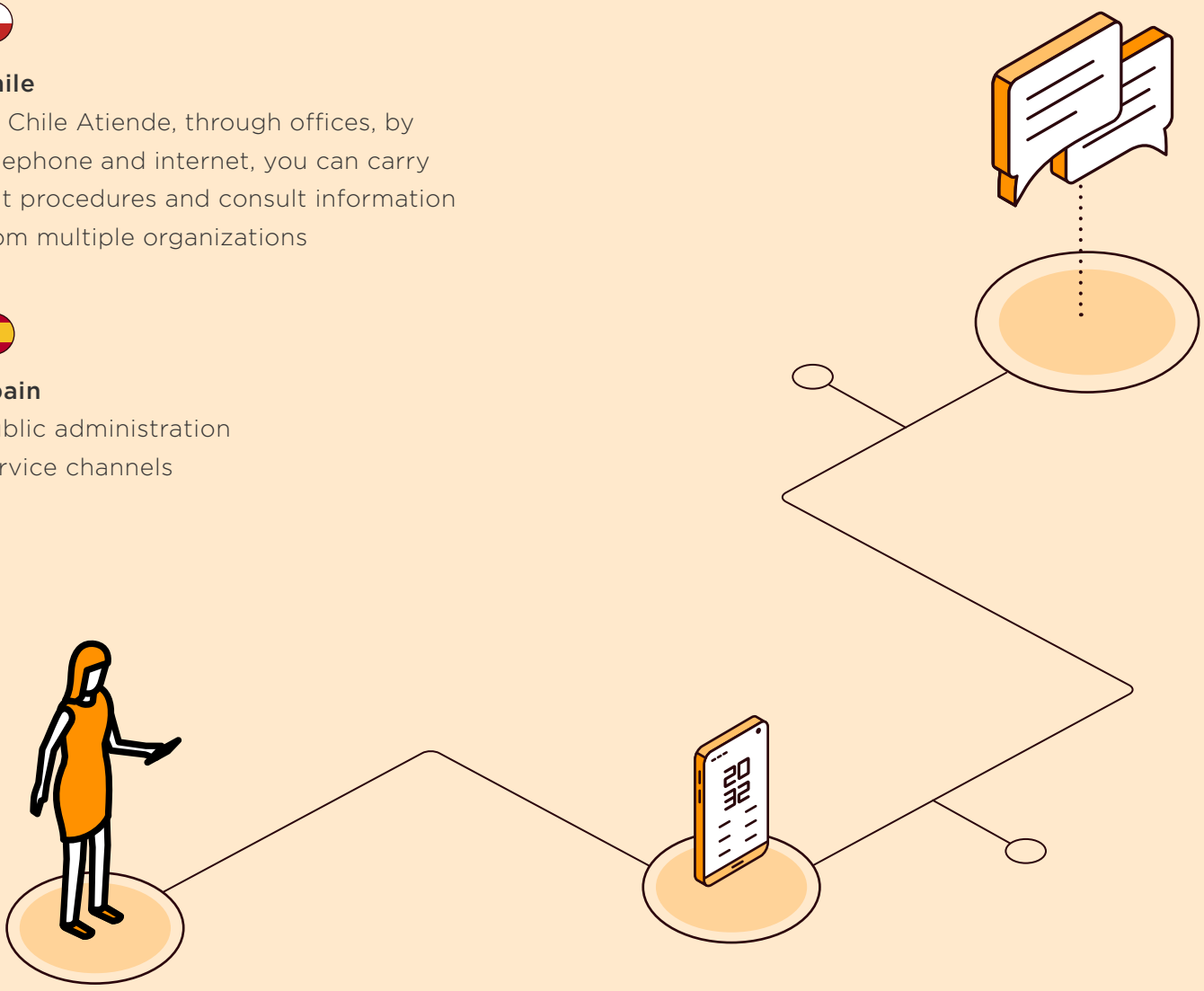
Click on each flag or icon to go deeper.

Chile

At Chile Atiende, through offices, by telephone and internet, you can carry out procedures and consult information from multiple organizations

Spain

Public administration service channels



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there an integrated citizen hotline?
- Are there offices where the offer of public services from multiple entities is integrated?
- Can a citizen or a company start a procedure in one channel and continue it in another (e.g., start on the internet and continue in person)?
- Is it possible to consult more than half of the central government procedures in the multichannel system?
- Can all central government procedures be consulted in the multichannel system?
- Can more than half of the procedures of the entire government (including states and municipalities) be consulted in the multichannel system?
- Is it possible to consult all the procedures of the entire government (including states and municipalities) in the multichannel system?
- Is it possible to handle more than half of the central government procedures in the multichannel system from start to finish?
- Can all central government procedures be handled in the multichannel system from start to finish?
- Is it possible to handle more than half of the paperwork of the entire government (including states and municipalities) in the multichannel system from start to finish?
- Is it possible to manage all the procedures of the entire government (including states and municipalities) in the multichannel system from start to finish?

5.2.2 SINGLE GOVERNMENT PORTAL

In general, administrative and governmental information is organized from the perspective of the producer. This means that there are hundreds or even thousands of websites with information that may be of interest to citizens and businesses. Moreover, in these websites the information is arranged according to a structure that corresponds to the agency itself, with a language that is usually legal or sectorial, and in many cases oriented more to what the agency wants to publish than to what may be of interest to the citizen or the company.

From the citizen's perspective, the above causes confusion and difficulty in obtaining information, and—finally—when accessing the place where the information is found, it is not understood; all this without achieving the objectives of the agency and its brand-new website. An example of this is that, in general, citizens use Google or other search engines more than administrative websites to find the information they are interested in.

The Single government portal is the web space that allows citizens to access the information of the administration and/or a public entity at a single point, in a simple, easy-to-navigate manner and with the possibility of having a search engine to easily find what each person needs. This Single government portal integrates all the information that may be of interest to the citizen—in particular that which refers to services, with its language and perspective, as opposed to information in general disaggregated into ministries, agencies, or administrative units, which is often more focused on these agencies than on the citizen himself.

In the event that there is a single transactional point with the citizen/citizen folder, this should be included in the single government portal, with a common image and operation, so as to eliminate for the citizen the difficulty of having to relate to different information systems. However, since technologically the solution for the information portal usually differs from the transactional one, this section deals with the single information point and the single transactional point with the citizen folder.

CHANGING THE FOCUS

The first thing to do is to shift the focus from the agencies to the citizen, so that the portal is created with the citizen's perspective and interests in mind. Now, as the focus must be unique, someone in the government is required to ensure the service and establish the focal point for the different ministries and agencies, so that they provide the information that is of interest to citizens. All of this requires strong coordination of public entities.

It is worth considering that this change of focus not only implies a framework to which public entities are not usually accustomed, but also leads them to lose their image or promotional capacity. Many institutions and agencies use their web page to promote and strengthen themselves, but citizens are not interested in the structure of the government, the conflicts of competencies, or the way in which services are provided; what they want is to have the information and get to the resolution of their problems, without caring which agency is the one that provides the former or solves the latter.

This is especially relevant if the Single government portal includes not only the central government and its agencies, but also subnational governments. Again, the citizen is not interested in whether the municipality, the state, or the federal government is involved in a given social service; what he wants is the solution to his problem.

KEYS TO A SINGLE GOVERNMENT PORTAL

- **Change the language:** Usually, government websites, for legal security or trend, use a legal or sectorial language that is incomprehensible to citizens. In many cases, a linguistic, usability, and navigation study must be carried out, so that the portal is really oriented toward the citizen and he can understand it.

- **Link the Single government portal with the citizen's folder:** It should even be possible to reach one easily from the other, promoting a common and simple navigation between systems, so that in the open part (government portal) there is public information that does not require identification, and in the folder, that which is specific to the identified citizen.

    - *Example:* In the single government portal, the citizen can view the information of an administrative procedure. To find out the status of this procedure, he can enter his folder and access it directly, or initiate it, as the case may be.

- **Comply with usability and accessibility strategies and regulations:** The government portal must comply with all these regulations, facilitating use through clear language, simple and citizen-oriented navigation, and a modality accessible to all people with disabilities. This makes the service particularly relevant to the strategy of eliminating digital divides**.**

- **Integrate or easily refer to open data and statistical or analytical information portals:** In this way, it should provide access to the state's dashboard and analytical information system.

- **To be integrated with the georeferencing system** to display the information in the most useful way possible for the citizen.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo is trying to find information about jobs in the public sector and is completely lost. He wants to work in a public entity, but he sees that he has no aggregated information on the positions offered. He knows some websites of some institutions, but he would like to be able to find all the public job offers in a single portal.

Entrepreneur
Ana

Ana is the head of a company that is going to open an office in another country. She would like to know the different procedures to be carried out in the different regions in relation to her activity, but she does not know of any place where she can see these procedures in a single portal. She has to search entity by entity, and it is difficult for her to find the information. She is sure that if she had all this information integrated in a single page, she could find the best place to locate the new subsidiary of her company in the country.

EXAMPLES

Click on each flag or icon to go deeper.

United Kingdom
GOV.UK

Colombia
Trámites, servicios e información

Argentina
Argentina unida

Panama
Digital Panama

Peru
Procedures, services and information

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Does the country have a Single government portal?
- Are more than half of the public institutions of the central government integrated to the Single government portal?
- Are all public institutions of the central government integrated to the Single government portal?
- Are more than half of the public institutions of the entire government integrated to the Single government portal?
- Are all public institutions across the government integrated to the Single government portal?
- Is the procedure portal or similar integrated to the Single government portal?
- Does the Single government portal incorporate usability and accessibility standards?
- Are there design standards for content published on the Single government portal?
- Does all content appearing in the Single government portal meet usability, accessibility, and design standards?
- Is the Single government portal integrated to the open data portal?

5.2.3 CITIZEN FOLDER

The citizen folder is the web space (connected to the government's Single government portal) where the citizen, once identified, can find all his data, certificates, records, communications and notifications, services, files, and other relations with public entities, and ideally with the private sector, in an integrated and organized manner according to the citizen's perspective (not that of the public institutions).

The citizen is not interested in the distribution of the competencies of public entities, or the different government structures, or the separate responsibility of each body in a procedure. The citizen wants to see in an intelligible and unified way his information and data, the status of his files, and to be able to carry out procedures with full control in a simple way. For this reason, the citizen folder is a project of general use, not limited to a single sector or only to the central level of government. If it were sectoral, multiple citizen folders would be created, and this is not what is expected, since it would render the multiple advantages of the project ineffective.

It is necessary to create a web space, a single country folder, from where it is possible to access the a single point of notification or registration that should exist for relations with the institutions, but not limited to this. The space should cover everything from the consolidated consultation of all files in all entities to the citizen's own data and certificates, or the initiation of administrative procedures.

Everything must be consolidated in a single point and under the citizen's perspective. This includes the wording and usability of the folder, so that it does not follow a competence or administrative criterion, even in the wording of the texts, but a functional, colloquial one, close to the image of the citizen.

Ideally, and if the forums with the private sector and the transformation strategy allow it, the citizen will not only be able to see in an integrated and simple way his information from all public entities (it is important to emphasize again that this is "his" information, oriented to the identified citizen, not general information), but also that of the private sector. Thus, just as you can access your work history, your university degrees, your real estate, etc., you can also access your telephone company, your bank, your electricity supplier, etc., from your folder. All this with a smooth and simple navigation, and without the need to reidentify between environments (taking advantage of the capabilities of national identification).

It should be noted that the term "citizens" refers to individuals and legal entities, as the latter should not be forgotten. Citizens have a small number of interactions with public entities every year, but companies have hundreds or thousands. Therefore, the fact that they have a comprehensive portfolio of relations with public institutions is remarkably effective for the state.

THE CITIZEN'S FOLDER IS THE CITIZEN'S PRIVATE AREA, SO THE FIRST THING TO DO IS TO AUTHENTICATE HIM. THUS, THE ELECTRONIC IDENTIFICATION AND SIGNATURE ARE RELATED TO THE FOLDER FROM THE VERY BEGINNING.

WHAT SHOULD YOU BE ABLE TO DO THROUGH THE CITIZEN'S FOLDER?

All citizen services, in general, should be in a folder, so this should be the single and common interface for the management of services related to the citizen. Thus, through the folder, it will be possible to

- Access the system of notifications and communications (output from the institutions to the citizen);
- Submit documents to public entities;
- Access electronic file systems or documents, in order to be able to know your own;
- Manage authorizations;
- Access one's own personal data through the interoperability platform;
- Obtain certificates through the same platform;
- Know the transactions and exchanges of information carried out by the entities;
- Know about appointments or events planned with the agencies.

IN ORDER FOR SERVICES NOT TO BE OFFERED ONLY THROUGH THE WEB CHANNEL, THERE MUST BE A RELATIONSHIP WITH THE STATE'S MULTICHANNEL SYSTEM.

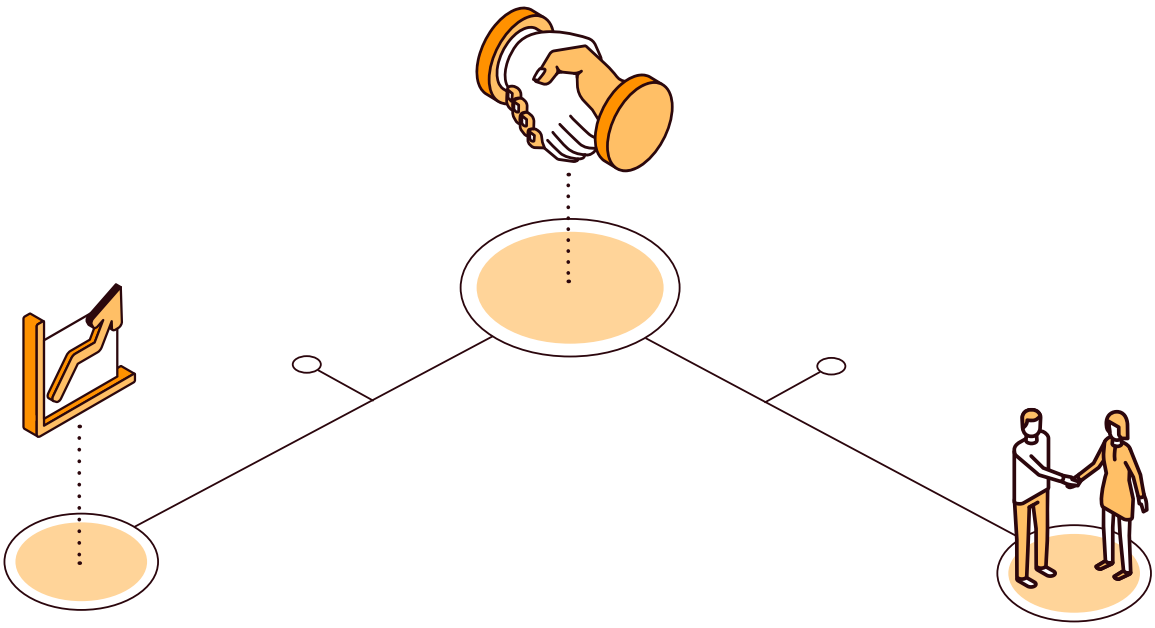
KEYS TO A SUCCESSFUL CITIZEN'S FOLDER

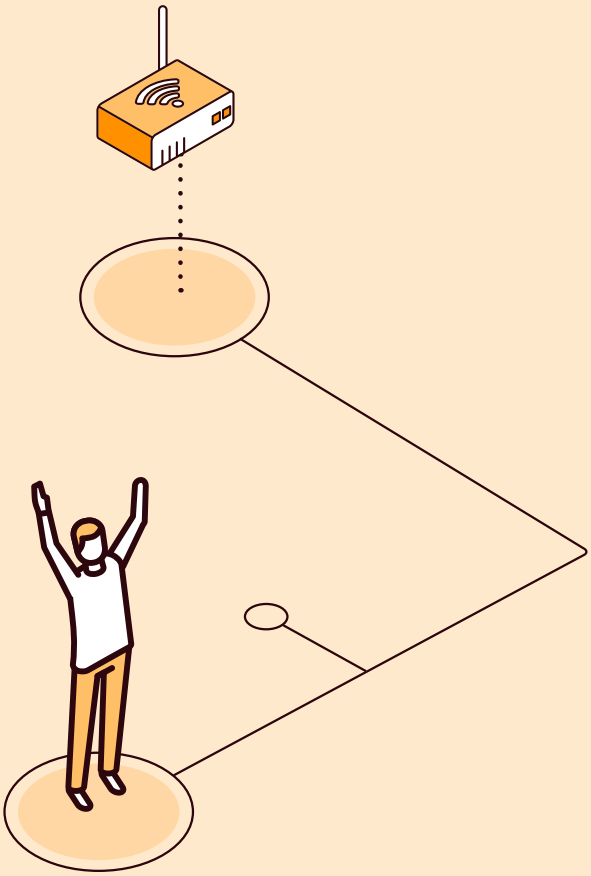
- **Electronic documents and records:** Precisely because of the wide range of integrated services on offer, these two concepts are particularly important. Only through a holistic and well-structured definition of electronic records will the citizen folder be able to interoperate with all types of systems and services. For this reason, the definition of nodes and metadata associated with documents and electronic records requires a great deal of attention, not only so that they cover as many services as possible, but also so that they can facilitate the adoption of new services in a simple manner.

- **Usability and accessibility strategies and regulations:** The folder must comply with all of these precepts, facilitating use through clear language, simple citizen-oriented navigation, and a system accessible to all people with disabilities. This means that the citizen folder has a special relationship with the strategy of eliminating digital divides.

- **Regulatory guarantee:** As sensitive personal data is handled, the folder must ensure that the use and access to such information is regulated. For the same reason, it is essential that all cybersecurity measures are implemented, because not only are there personal data, but the citizen can perform actions, so that a failure in the security of this system can damage people's trust in digital media.

- **Authorizations:** It is essential that the folder be integrated with the systems of authorizations, so that a citizen with the capacity to know the status of a procedure or to manage on behalf of another can effectively exercise these rights.





STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo does not understand how the physical counters have been replicated in the digital world. He finds it difficult to go to a different website each time to find out his data, depending on the entity, or to check the status of his file. He would like to go to a single site that has all his information integrated, regardless of its origin.

Entrepreneur
Ana

Ana is a digital native and is very happy that her country, thanks to the intermediation platform, does not need to ask her for data she already has to do her company's government procedures. However, she would like to really know what data, for what purpose, and to where it is exchanged on the platform, through a single point of entry, and to see the exchanges of her data between public entities.

EXAMPLES

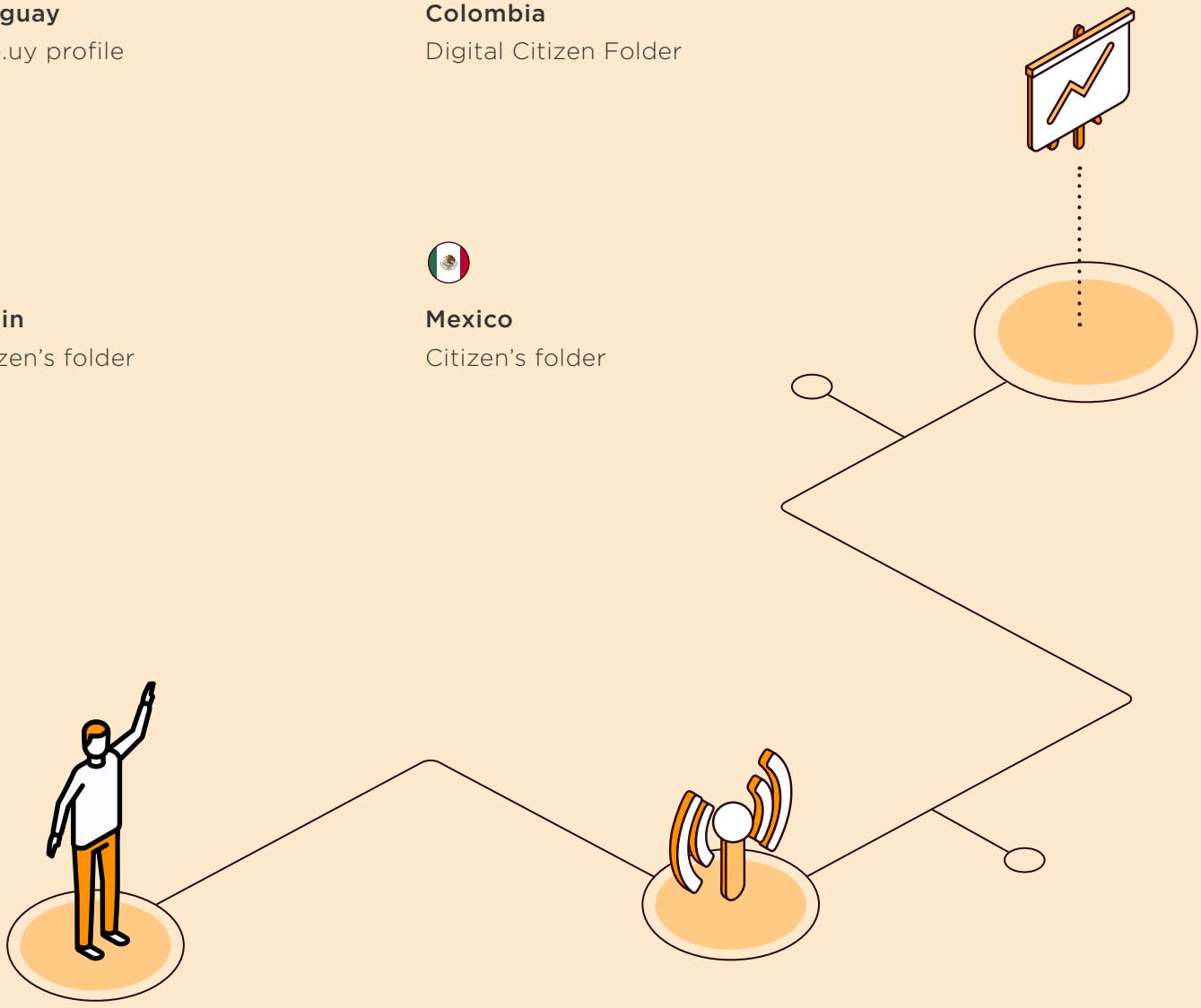
Click on each flag or icon to go deeper.

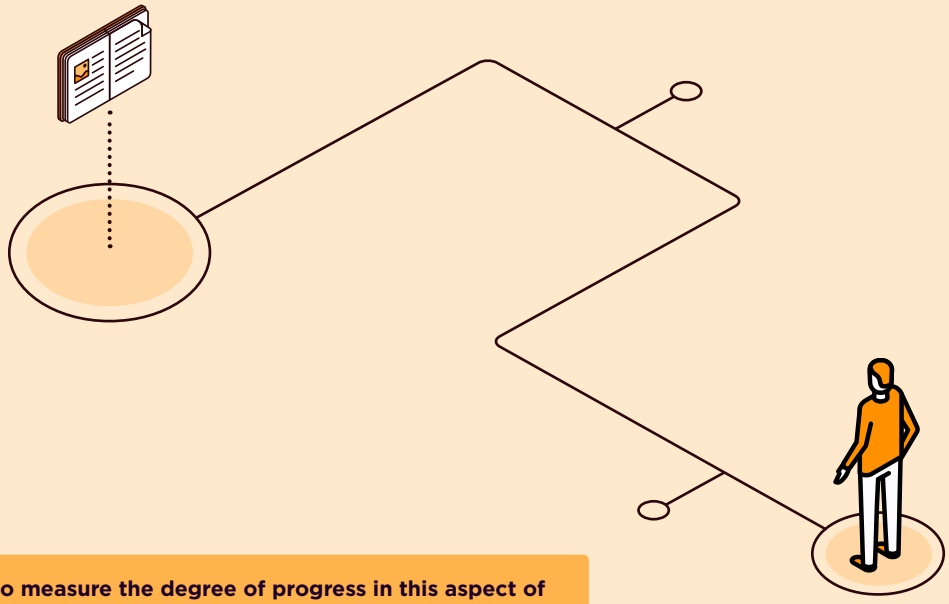
Uruguay
gub.uy profile

Colombia
Digital Citizen Folder

Spain
Citizen's folder

Mexico
Citizen's folder





INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a citizen's folder or similar tool? If so:
  - Are all public entities of the central government incorporated?
  - Are all public entities incorporated?
  - Can the citizen know the status of all his procedures with the different entities?
  - Can the files and documents of the different public institutions be accessed through this single point?
  - Can citizens access their data?
  - Can the citizen obtain and store valid administrative certificates through the single point?
  - Can the citizen receive notifications and communications from multiple entities through the single point?
  - Does the citizen have access to the information exchanges of his personal data carried out by the different entities through this information system?
  - Is there, through the single point service, access to a unified agenda of future appointments and procedures to be carried out by the citizen in multiple agencies?

5.2.4 SCHEDULING SYSTEM

The scheduling system manages citizens' appointment requests and reservations for all the entities that provide them. This is another of the services that multiple entities usually need, so once again there is the possibility of providing it as a common service. In this way, two advantages would be obtained:

- Each and every institution that needs it would not have to develop the service and maintain it.
- The quality of service and the citizen's perception would be improved.

In many areas (meetings with the children's teacher, medical appointments, renewal of documents, social assistance, etc.) a personal or direct relationship with the citizen is still required. In many cases, some entities have set up an appointment system to organize the demand according to the offer that can be given and improve the service to the citizen, but it is not common for these systems to be unique or interoperable.

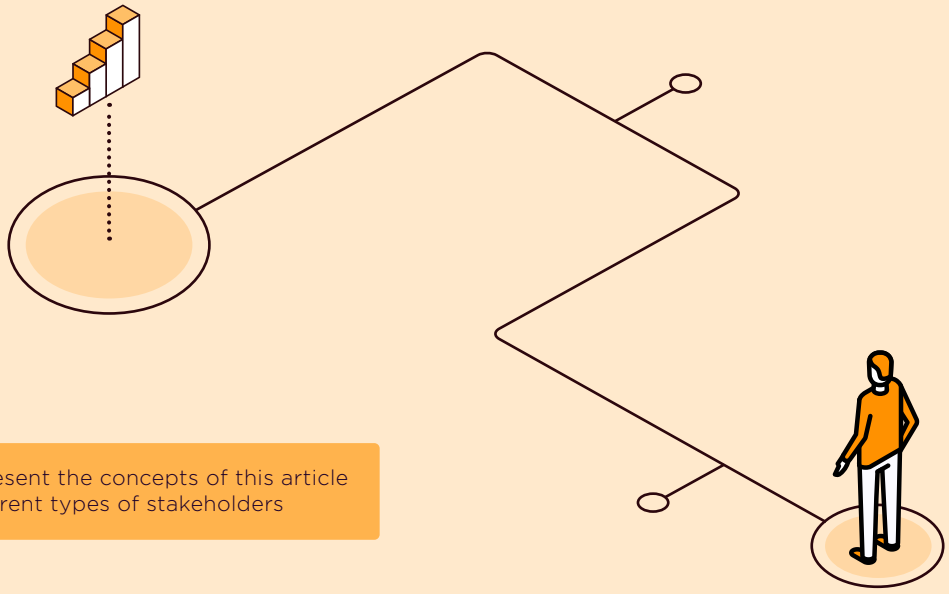
From the citizen's perspective, having multiple systems leads to the known consequences: complexity of use, confusion, and forgetting appointments. Thus, having a single system that the citizen could integrate or use as his personal schedule at will would improve the quality of service. This information system is particularly related to queue management, which is discussed below. It can also be oriented to proactive processing, so that the system alerts the citizen not only when he has an appointment already made, but also to indicate when he should make one—for example, to renew a document that is about to expire soon.

KEYS TO AN SCHEDULING SYSTEM

- **A single information system:** The available services and appointments generated by the various public entities should be loaded into a single information system, to which citizens have access through multichannel care or the single point on the web (or, in less advanced contexts, as a common service integrated into separate pages), to sign up for what they need or are interested in.

THERE ARE MULTIPLE SCHEDULING SYSTEMS IN FREE OR PROPRIETARY SOFTWARE THAT COULD BE ADAPTED TO SERVE AS THE BASIS FOR THE COUNTRY'S SCHEDULING SYSTEM.

- **Agree and define the following:**
  - System governance (the owner can be the lead institution of the digital government)
  - The operation of the entities in relation to the system
  - Identification requirements (which may not always be necessary)
- **Be connected to the nation's notification or message management system:** It will be possible to send notifications or appointment reminders to citizens, through the channel and data they have indicated as preferred. In addition, it is one of the star systems in the integration of the citizen folder, so that citizens have a unified view of all their appointments with government institutions and can make the appropriate arrangements.
- **Connection to a telephone interface:** Precisely because it facilitates face-to-face appointments, the system may be used by people without digital skills, so it would be particularly interesting to connect the service, via multichannel, to a telephone interface. To make the telephone channel as operational as possible, it is important that the electronic national identification system is also operational via the telephone channel.
- **Store metadata for each service or procedure for which appointments are managed:** As part of the metadata, data should be stored on aspects such as:
  - The average time of attention for the resolution of the procedure;
  - The place where the face-to-face service will be provided;
  - The number of simultaneous service counters at the physical location for that procedure.
- **Be related to the unit directory:** To facilitate, in a univocal way and without margin of error, the management in the indicated unit, as well as the updated contacts.
- **Be related to the registration of procedures:** To associate appointments or appointments with the specific administrative procedure.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Vice minister of health
Sara

Sara is meeting with Elena, the person in charge of the shift service at a health center. Elena understands perfectly well the complaints of patients because they cannot take appointments through the internet or modify them. She would like there to be a system that would allow her to do this easily and that would not cost her much.

Citizen
Camilo

Camilo wonders why he does not have a site where he can see in a unified way his appointments for government procedures. He has recently done several of them (renewing his ID card, enrolling his daughter in school, inheritance procedures), and in each case the appointment has been handled differently, often on paper, and he has no place to see them all in an integrated way, so he is afraid he might forget one of them.

EXAMPLES

Click on each flag or icon to go deeper.

Uruguay

gub.uy profile, where citizens can access the unified schedule of "my appointments" in public agencies

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there an ascheduling system as a common service that can be used by any public institution? If so:
  - Are more than half of the central government institutions that offer appointments to the public integrated?
  - Are all central government institutions that offer appointments to the public integrated?
  - Can appointments be made for more than half of the central government procedures that require it through the system?
  - Can appointments be made for all central government procedures that require it through the system?
  - Is the system effectively used to schedule more than half of the appointments for central government procedures?
  - Is the system integrated with the directory of administrative units?

5.2.5 SERVICE CATALOGUE

The procedures catalog is the set of formalities or procedures carried out by public entities that have been classified and tagged with metadata. In general, this service ends up becoming a key part of the ecosystem, since it not only has the list, but also all the information associated with the procedures, from the regulation related to each one to the associated and necessary documentation for each case, including the characteristics of the file archive linked to the procedure, the certificates that interoperate, the volume of use, its access options (in person, online, by telephone), etc.

In some countries, the procedures catalog ends up being the citizens' entry point to the government procedures. Technologically, it can be the same information system or different systems; what is important is the abstract concept of a procedures information system, for statistical purposes for management, related to the steps of the processes and associated legislation, etc. In addition to the catalog as such, it can be part of or feed into the citizen folder or the single point of government.

USEFUL FOR CITIZENS AND PUBLIC MANAGERS

- **For public managers:** In the case of new authorities, it is useful to know what each administration does. Once the catalog is available, the natural step is to include the associated statistical information, so that the corresponding public entity can exploit the information: how many procedures of each type it carries out, if there are peaks or seasonality, how many in electronic format, what is the average time for each phase of the procedure, etc. This provides the entity with important information to improve its performance.

WHAT DOES THIS CATALOG ALLOW?

- Facilitate the interoperability of required documents.
- Classify administrative files in the document manager.
- Automatically manage the archiving of documentation.
- Enable access to files.
- Stipulate the management of the business process that follows an administrative procedure or process, so that the agency's electronic managers can read and implement it automatically.

KEYS TO A SERVICE CATALOGUE

- **General for the whole nation:** There must be a centralized repository with the basic and public information of all procedures. In many cases, the nature of the catalog is binding or a basic registry of the state; that is, whatever is processed must be in the catalog, and this can be, in fact, the key to interoperability, the consultation of the status of the procedures, the initiation of them, etc. Therefore, in some regulations the catalog is expressly named, even with the rank of law.

- **Cloud system for certain cases:** The above repository will load the information in a federated manner, in the event that the public entity has its own catalog system. However, municipalities or small organizations may not have their own catalog, so there must be a cloud system so that these entities, simply with an authorized user and a web browser, can manage their catalog.

- **Access:** It is important that the catalog is published and available in a format that allows automatic processing in the Single government portal, since its information is very useful for citizens, companies, and the rest of the public entities.

- **Procedure code provided by the catalogue:** This becomes really important, as it is the equivalent of the citizen identification code or unit identification code in the unit directory. This code ends up being important information included in the electronic file -and similar documents- metadata. For example, it must be part of the metadata of the notifications or communications to citizens, automatically processable, so that the company or the citizen knows what he is being notified about. It is the metadata that identifies the procedure in the input information.

- **Back-office and front-office:** It is interesting that both the back-office aspects of the catalog (for use by officials) and the front-office (for use by citizens), usually called "portal," are the responsibility of the same institution, in order to avoid duplicate work and inconsistencies of information between sources.

- **Relationship with the registry of administrative units as an entry system:** Thus, each of the procedures can be linked to the administrative unit that manages it.

- **Relationship with the registry of officials:** Similarly, the management and modification of procedures can only be done by authorized users, so the catalog must be related to the registry of authorized officials, and only those who have a role that allows them to access the instrument will be able to do so.

SOME OF THE MOST SIGNIFICANT IMPACTS OF THE SERVICE CATALOGUE

- Integration with the single point of government, communicating to citizens and companies all the procedures and public information associated with each one of them.

- Integration with the citizen folder for the presentation of procedures to citizens.

- Integration with the interoperability system, since the procedures registry stores information about the data needed and is the one that enables requesting them from the platform, so that everything is public and in accordance with regulations.

- Integration with the nation's electronic archive, so that each type of administrative procedure is associated with the document series to which it belongs and its archiving characteristics, access, possibility of public consultation, etc.

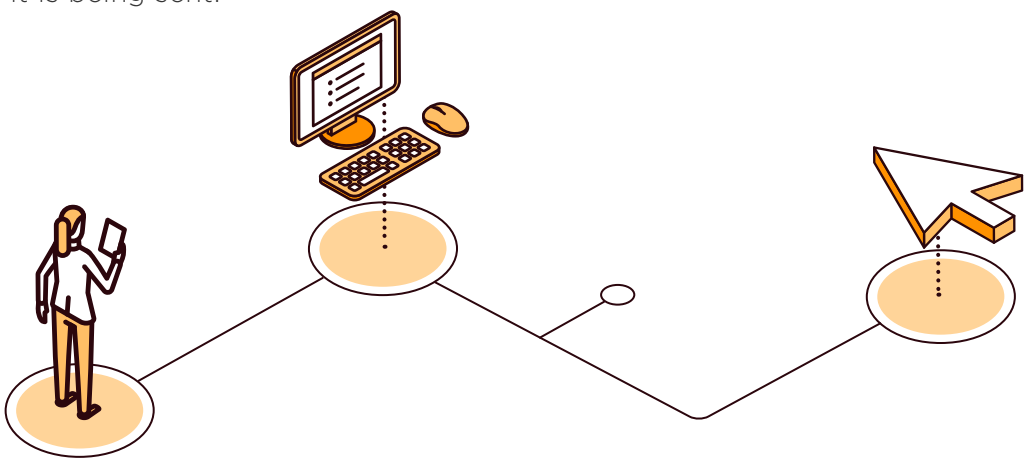
- The code of the procedure registry is used, like that of the unit directory, as a basic metadata of the nation. Thus, it is included in

  - Notifications and communications from public entities, so that the citizen and the company know to which process they correspond;

  - Electronic documents and files, so that they are associated with the process to which they belong;

  - Authorizations, to indicate that citizen a can carry out on behalf of b (company or citizen) the procedure according to the registry code.

- The code allows marking incoming documents. Thus, the citizen or company, when sending a communication to the corresponding public entity, can univocally indicate for which procedure it is being sent.



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo's cousin, Marcos, is doing a study for a university on electronic procedures in public institutions. However, it is very difficult for him to get information because there is no published catalog of procedures. Marcos believes that this is problematic from the point of view of transparency and gives discretion to the public entity in relation to its work.

Camilo is applying for a food subsidy for his family and is confused about the requirements and steps to be taken, as they vary depending on the official who attends him. He is surprised that for this or any other procedure the information he needs to know is not published on the internet, such as what documents are required, what the deadlines are, or what steps must be taken to complete the procedure.

Vice minister of health
Sara

When Sara was appointed vice minister, her first task was to find out how much paperwork there was related to health services. When she asked ministry officials, she found only partial answers. It seems that no one knows for sure what procedures her ministry does, how many times it does them, or how they are done. Sara would love to have this information so that she can improve her ministry's management.

EXAMPLES

Click on each flag or icon to go deeper.

Mexico

National Commission for Regulatory Improvement.

Spain

The system evolved from a catalog to a complete administrative information

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Are more than half of the central government entities included in the catalog?
- Are all central government entities integrated in the catalog?
- Are more than half of all government-wide public entities included in the catalog?
- Are all government-wide entities integrated into the catalog?
- Are more than half of the procedures of central government entities included in the catalog?
- Are all the procedures of all central government entities integrated in the catalog?
- Are more than half of the procedures of all public entities of the entire government integrated in the catalog?

- Are all the procedures of all the entities of the entire government integrated in the catalog?
- Is the following information about the procedures included?
  - For citizens:
    - The legal support that gives meaning to the process or procedure
    - Where to do it
    - Hours of operation
    - Eligibility requirements and conditions
    - Data protection
    - Steps to follow
  - For civil servants:
    - Statistics regarding number of uses, types, location of procedures, etc.
    - Documents required to perform the procedure, in a standardized manner, to be the "key" that allows access to the interoperability platform.
    - Process diagram, expressed in such a way that a machine can implement it automatically.
    - Archiving (i.e., what are the archival characteristics in relation to each of the steps or procedures). For example, if the information is destroyed after five years or if it is kept in whole or in part, which documentary series it belongs to, etc.
    - Transparency and access rules for making decisions regarding citizen requests or the publication of information.
    - Interoperability and relationships of the procedure with other entities, other data, or other agencies. For example, map of relationships, what data does not have to be provided because it is obtained from the interoperability platform, or if there is a proactive approach to vital events in which this procedure triggers others in a chain.

5.2.6 TRANSPARENCY AND GOOD GOVERNANCE INFORMATION SYSTEM

Regulation related to transparency and good governance has to work effectively, with a view to achieving its objectives and for citizens to regain or improve their trust in institutions. Therefore, information systems that favor transparency and good governance are essential for legal regulations to become an effective right on the part of citizens.

NEEDS COVERED BY A TRANSPARENCY SYSTEM

- **Access to and understanding of data:** It is not only necessary that web pages exist, but that they are useful and allow information to be found in an effective and simple manner, which in turn must undoubtedly be understandable. In many cases, institutions flood websites with data—for example, budgetary data—which is not automatically processable and it is hard to know if it is being put to good use. Therefore, it is helpful to have graphs, studies, and processing to make data useful.

- **Requesting data and filing complaints:** With little or no administrative cost for the citizen, it should be possible to request from the institutions data that is not published in the portal, as well as to complain to the authority that oversees compliance with the provisions of the regulation. If this information system does not exist to channel requests for information or to raise complaints about unattended requests, the regulation will be reduced to a legal text with no enforcement in practice.

- **Contribute to good governance:** For the principles of good governance to be implemented, it is necessary to have the information systems that make them feasible. In this field, it should be noted that in daily life, citizens interact a lot with municipalities, and these, in general, except for large cities, are not able to meet their needs. It is therefore important that the country's system offers these solutions to those entities that, due to their small size or lack of technical capacity, would not be able to offer these services to the civil society on their own. In this way, citizen participation is facilitated, both in the processes of legislative development and hearing procedures, when so regulated, and in participation through surveys, referendums, consultations, and the like. The participatory budget system is also included in this area, as well as tools that allow for improved interaction and contact between citizens and public entities, such as mobile applications that facilitate notifications or the relationship between citizens and institutions.

A TRANSPARENCY AND GOOD GOVERNANCE INFORMATION SYSTEM FACILITATES COMPLIANCE WITH THE REGULATIONS ASSOCIATED WITH THIS MATTER, BOTH BY THE CENTRAL GOVERNMENT AND BY THE REST OF THE PUBLIC INSTITUTIONS.

MODULES THAT SHOULD MAKE UP THE NATIONAL TRANSPARENCY AND GOOD GOVERNANCE SYSTEM

- **Transparency web:** This is the best known and most common. It is the point where agencies, subject to accountability regulations, publish information in a proactive and direct way. It is important that the web is easy to use, has a clear language, and eliminates administrative complexities so that the available information can be easily found and used. Within this, in turn, it would be convenient to have the following:

  - A search engine that, given a term, allows you to find all the related information available. Ideally, this information should be ready to be downloaded and processed automatically.

  - Everything associated with public procurement. Because of its special relevance, it is essential that all information in this regard is available, so that it is easy to detect malpractice, corruption, or any other type of improper behavior in the use of public funds.

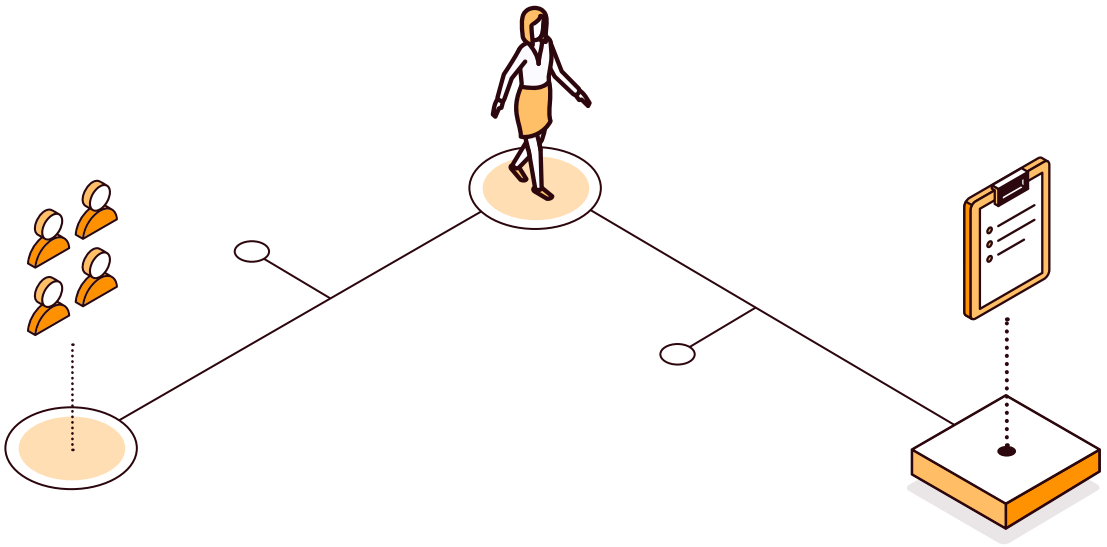
- **Data integration module:** The publication portal needs the data to be uploaded, so it is important that the country's transparency system has such a module. Ideally, it should integrate this data automatically from public information systems (e.g., from the government procurement platform). This ensures that all information is published in real time and without manual processes that can hide or modify it. However, it is not possible in all cases to connect an automated information system with the transparency information system. It is therefore essential that the information that needs to be uploaded manually can be processed in a simple way, and that this can be done by all institutions or agencies that have to publish transparency information.

- **Channeling of citizen requests:** Another technical module that is required is the one in charge of channeling citizen requests for information related to those aspects that are not published on the portal but which they have the right to access. There must be an information system that fulfills this task, and it is key to ensure compliance with deadlines, as well as the traceability of all requests, to ensure the effective fulfillment of citizens' rights. Traceability information on

the request and response process is fundamental for the body that must ensure compliance with the law to be able to resolve possible complaints and appeals from citizens in the event of what they consider to be noncompliance with their rights. Likewise, the system for submitting complaints to the control body must also be contemplated.

- **Participatory modules:** The system should also have modules for the creation of participatory budgets and the promotion of citizen participation in the creation of value and public service: the collection of initiatives and comments to laws or relevant projects, electronic voting systems, and consultations on issues in which citizens can participate. For transparency and good governance to become a reality in the country, and to be perceived as such by the citizens, it is necessary that some agency, generally from the central government, provides these information systems to all those public agencies that, due to lack of capacity, cannot have them on their own.

GIVEN THE PHILOSOPHY OF THE PROJECTS, IT IS COMMON TO FIND OPEN-SOURCE SOLUTIONS THAT HAVE BEEN TESTED AND ARE WORKING FOR EACH OF THE MODULES.



KEYS TO A SYSTEM OF TRANSPARENCY AND GOOD GOVERNANCE

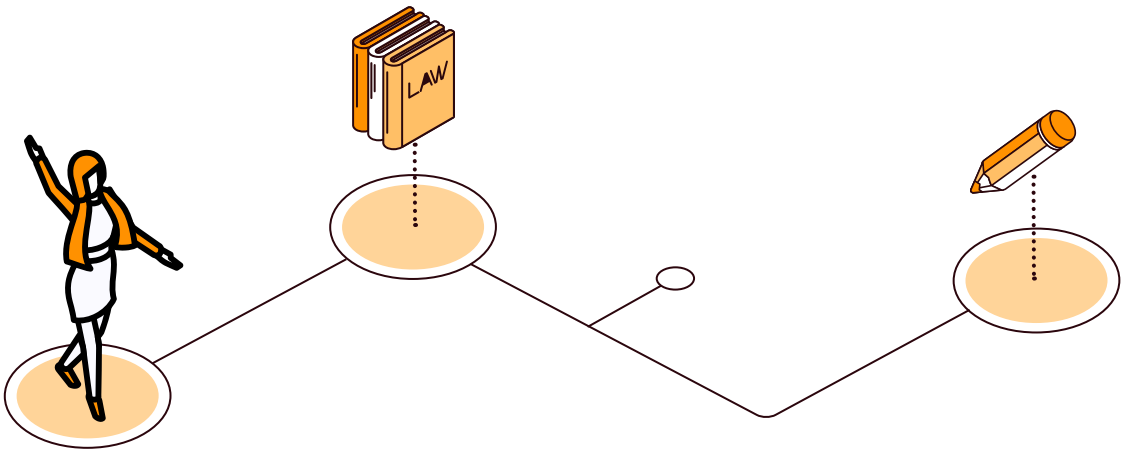
- **Relationship with regulations related to transparency and good governance:** The system must cover all aspects defined in the regulations related to these areas.

- **Linkage to open data policy and strategy:** Transparency datasets should be made available as open data.

- **Accessibility and usability:** It is necessary to ensure that these specifications are applied, especially in a system that is widely used by citizens, such as the transparency and good governance system. In addition, since it is a key information system of massive use, it must be within the government's Single government portal or have a coherent relationship, a similar interface, and other guidelines provided by the government.

- **Relation with identification and electronic signature systems:** This is relevant if, apart from the publication of information, other services are offered (request for information by citizens, public participation, etc.). Similarly, if there are parts that are specific to citizens, the system should be related to the citizen folder.

- **Compliance with established standards and semantic systems:** In order to provide information in the most useful and actionable way possible, the system must follow the guidelines that are established in this regard. This ranges from the document or electronic file standard to the obligation to mark the information with the directory of units or procedures, when applicable, or to show useful information from these systems (such as the volume of procedures carried out or the organization chart of the administrative units).



STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo is very concerned about the fight against corruption, and he is a citizen quite involved in this issue. For this reason, he has used the information and transparency system a couple of times. Thanks to it, he was able to consult with the competent body about a concern he had about the misuse of resources in his neighborhood, and it has answered him by giving him a logical explanation for these expenditures. Moreover, as Camilo was apparently not the only concerned citizen, his municipality decided to start publishing this data on a regular basis.

Vice minister of health
Sara

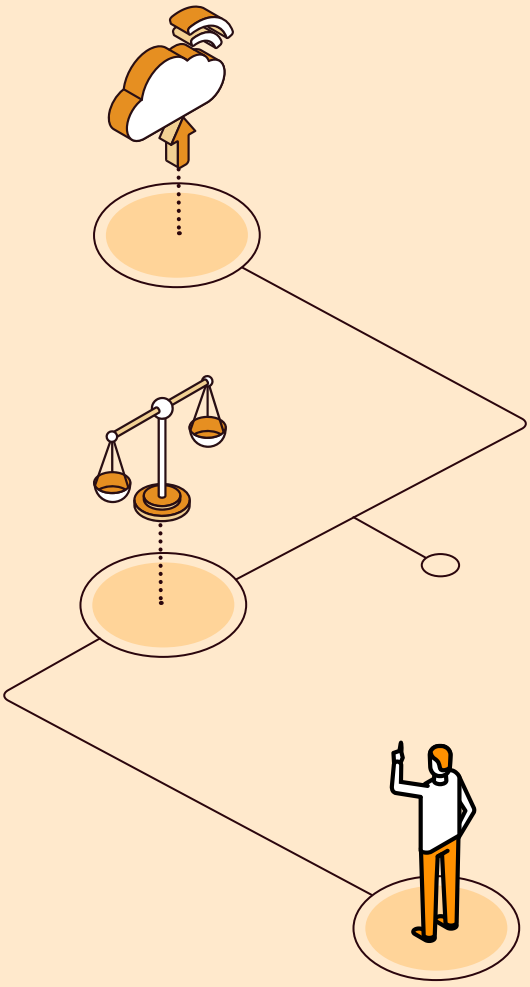
Sara is aware that health is one of the most sensitive issues for citizens, so she has appointed a person in charge of transparency and citizen participation. This person will not only ensure that legal obligations are met, but also that questions from citizens and companies are answered within specific deadlines. In addition, the ministry's strategy must be published and shared—all this, of course, by electronic means, thanks to the country's transparency and good governance system.

Mayor's advisor
Daniel

Daniel has encouraged his municipality to use the country's transparency and citizen participation system. Thus, transparency information is published in a single site where it can be compared with other municipalities (from public salaries to tenders), which gives greater added value to the information. In addition, it means that his municipality does not have to create their own transparency portal.

EXAMPLES

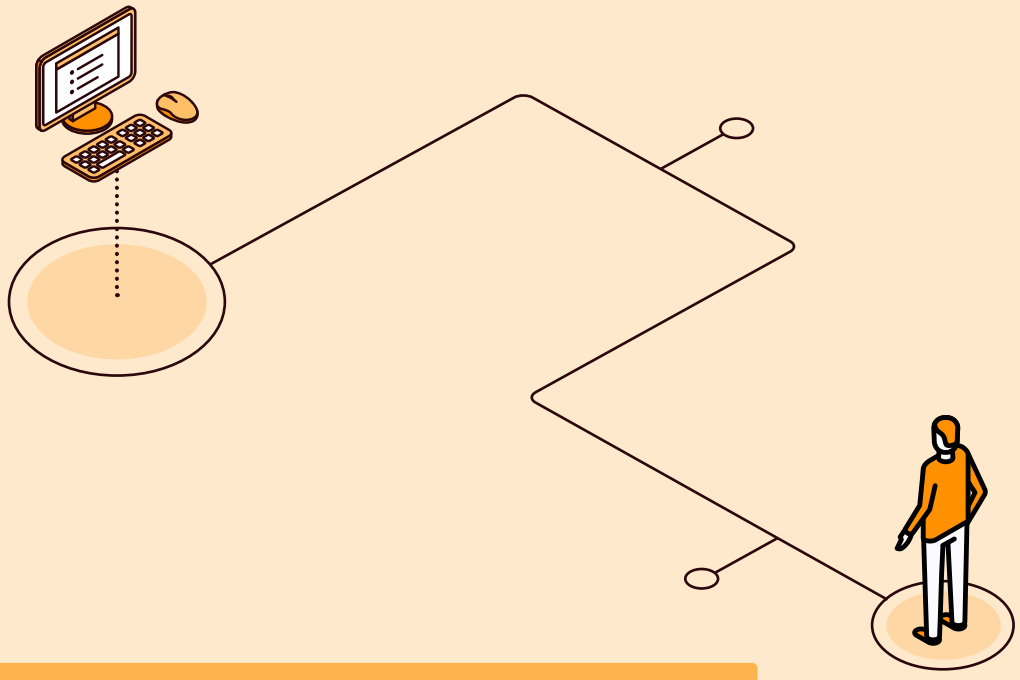
Click on each flag or icon to go deeper.



Spain
Portal of transparency in the cloud for local entities

Mexico
Portal of Transparency Obligations (POT))

Chile
Portal of Transparency



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a transparency portal? If so:
  - Is it integrated in an automated way with the state's computerized procurement system?
  - Is it integrated to the open data portal?
  - Does it have a search engine?
  - Is it governed by usability and accessibility standards?
  - Does it facilitate the creation of participatory budgets, the promotion of citizen participation, and/or other similar initiatives?
  - Does it allow for receiving and channeling citizens' requests for access to information?

5.2.7 PAYMENT GATEWAY

Many administrative procedures involve some kind of payment, which is often small in amount but is frequently a serious problem for many entities due to the strict audit control conditions of the public sector and the ability to perform them by digital means. Moreover, in many digitized procedures, payment is not digitized, so that, even if it is a small amount, it implies an extra transaction cost for the citizen. It is sometimes necessary to switch to a paper-based procedure, go to a specific institution (such as a bank or public office) and return with proof of payment, which is a setback on the improvements that the digital procedure entails.

On the other hand, in many small agencies it is costly to have agreements with banks and credit or debit card issuers for the management of electronic payments, so a larger agency should provide payment solutions to these entities. This need for economies of scale and negotiation with the financial sector makes it important to offer the system as a common service, either from the digital government, the tax collection agency, the central bank, or the Ministry of Finance. In the event that the technical solution comes from the e-government side (as in Spain, for example), it is important to coordinate with the state's financial agencies in order to achieve the greatest economies of scale and the greatest possible negotiating capacity to avoid or reduce commissions.

The payment gateway is the information system that manages payments and collections, with their associated accounting, by multiple electronic means, so that when the administrative process requires it, these payments do not have to be made by traditional means. For economic and accounting reasons, as well as for technical and usability reasons for citizens, it is important that this service be reusable by any public entity, thus improving accounting management and providing citizens with a clear and common reference for making state payments, facilitating its use, generating trust, and avoiding the technical and administrative complexity of each unit developing its own system for payments.

THE AGGREGATION OF DEMAND MAKES IT POSSIBLE TO SUBSTANTIALLY REDUCE BANK FEES, OR EVEN ELIMINATE THEM, SO IT IS PARTICULARLY INTERESTING THAT THE PAYMENT SERVICE IS COMMON AND OFFERED TO ALL ENTITIES THAT NEED IT.

KEYS TO A PAYMENT SYSTEM

- **A good agreement with banks and/or credit card issuers:** One of the first necessary issues is to establish agreements with the means that citizens will use to make payments, so that there are no fees charged on payments, or that these fees are minimized. Likewise, flexibility should be provided so that any public institution can use the system.

- **Having a powerful user and user entity management system, and being highly protected against attacks:** These issues are key because of the sensitivity involved in handling money.

- **Provide interfaces:** This is key so that the different applications and web pages of the institutions can use the system, facilitating its integration. In this sense, it is important to provide two alternatives:

  - Manual interfaces that can be integrated into web applications.

    - *Example:* An online process being carried out by the citizen on an agency's website is passed to the payment gateway when a payment needs to be made. Once the payment is made, the system returns the information to the entity's website, and the flow continues.

  - Automated interfaces.

    - *Example:* If a license fee for the use of public space has to be paid every quarter, the citizen or company can authorize the public entity in question to collect the fees automatically. It is therefore important that the system, in addition to an interface that can be integrated into web applications, also has automated interfaces.

  - It is also important to take into account the counter officers, who must have a virtual point of sale so that they can collect payments from citizens.

- **Consider the management and audit module:** This will enable the accounting and treasury monitoring obligations of the system's users and auditors, for the easy detection of strange behavior. To establish this module, it is necessary to take into account:

  - The need to show a relationship between each charge made and the procedure associated with it, plus the institution responsible;

  - The need for a tool that is accessible to users of different entities, their managers, and control bodies;

  - The need to provide sufficient configurability so that each unit or user can manage exclusively its own area of competence, without being able to access the information of the rest;

- The need to offer different payment mechanisms, such as credit cards, debit cards, and other types of electronic payments;
- The need to have interfaces for access from websites, mobile devices, and social networks.

- **The final technological solution:** In this sense, procedures have been carried out with public software, and ideally this should be offered as a cloud service for direct consumption by any public entity. The service can also be contracted with a private company, although in this case it is necessary to highlight the needs with respect to the interoperability that must be kept with the rest of the systems of the different user entities.

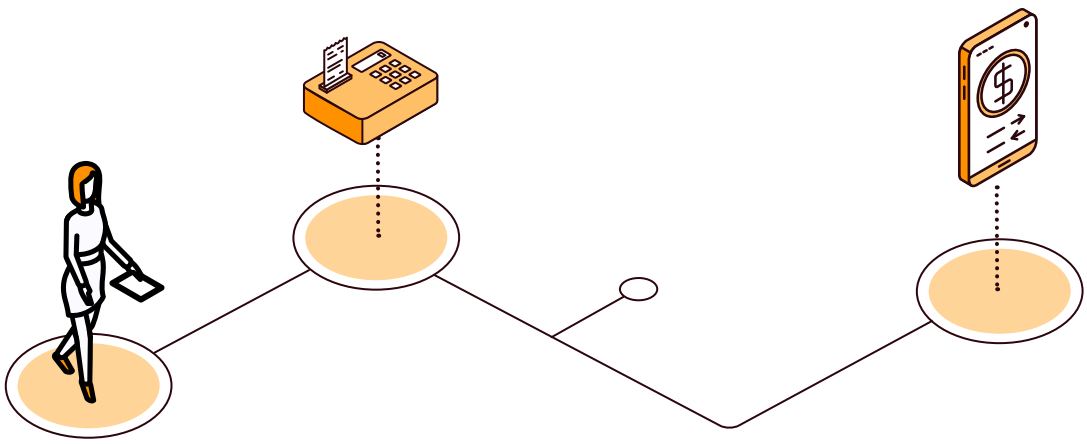
- **Use of electronic identification and signature systems:** The payment gateway will typically use these for citizen identification and signing of transactions and related documents.

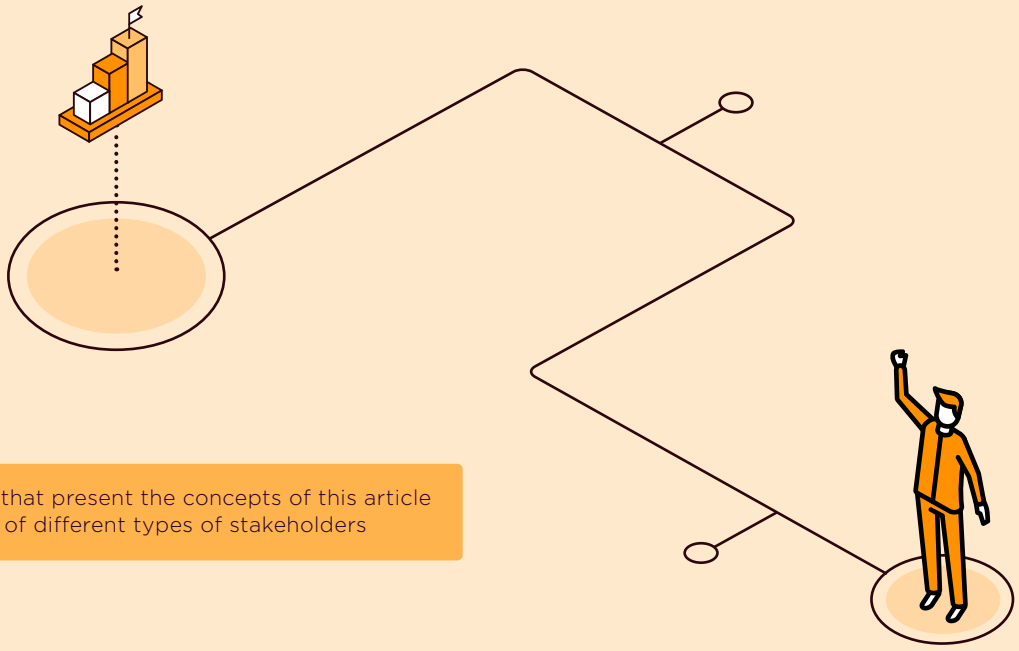
- **Relationship with the registry of authorized officials:** For use by citizens, the gateway will be linked to this information system to facilitate the work of those officials who have permission to collect or make payments, according to their role.

AREAS IN WHICH THE PAYMENT GATEWAY MAY BE USED

- Citizen folder and other possible processing systems that need to manage payments from citizens, facilitating payments by electronic means. Also from the folder it will be possible to see the history of payments made or obtain receipts of these.

- Multichannel customer service system, allowing payments to be made by telephone and in offices, through authorized officers.





STORIES

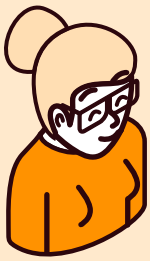
Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Given his activity as a cab driver, Camilo has to make payments for municipal and state licenses, as well as taxes, on a quarterly basis. Until now, the process could be done electronically, but the payment could not, so he had to go to his bank branch to complete the process. Now, thanks to the new payment gateway, he can do the complete process without leaving his home.

Entrepreneur
Ana

Ana was already a user of the electronic payment system for tax and social security procedures, and now she is delighted with the new platform that allows her to make all government related payments through a single system. Not only because she has all the payment information centralized, but also because she can now pay in a single place for all the procedures with all the government institutions.



Vice minister of health
Sara

Sara has pushed for her ministry to be one of the first to join the new state payment platform, and she is delighted with the results, not only because it makes life easier for citizens by allowing them to pay for health-related procedures online, but also because it is used in reverse: it centralizes all payments for health subsidies and social services. The gateway also allows payments to be made over the counter for face-to-face procedures, which has led to better management and the virtual elimination of cash payments at health facilities.

Mayor's advisor
Daniel

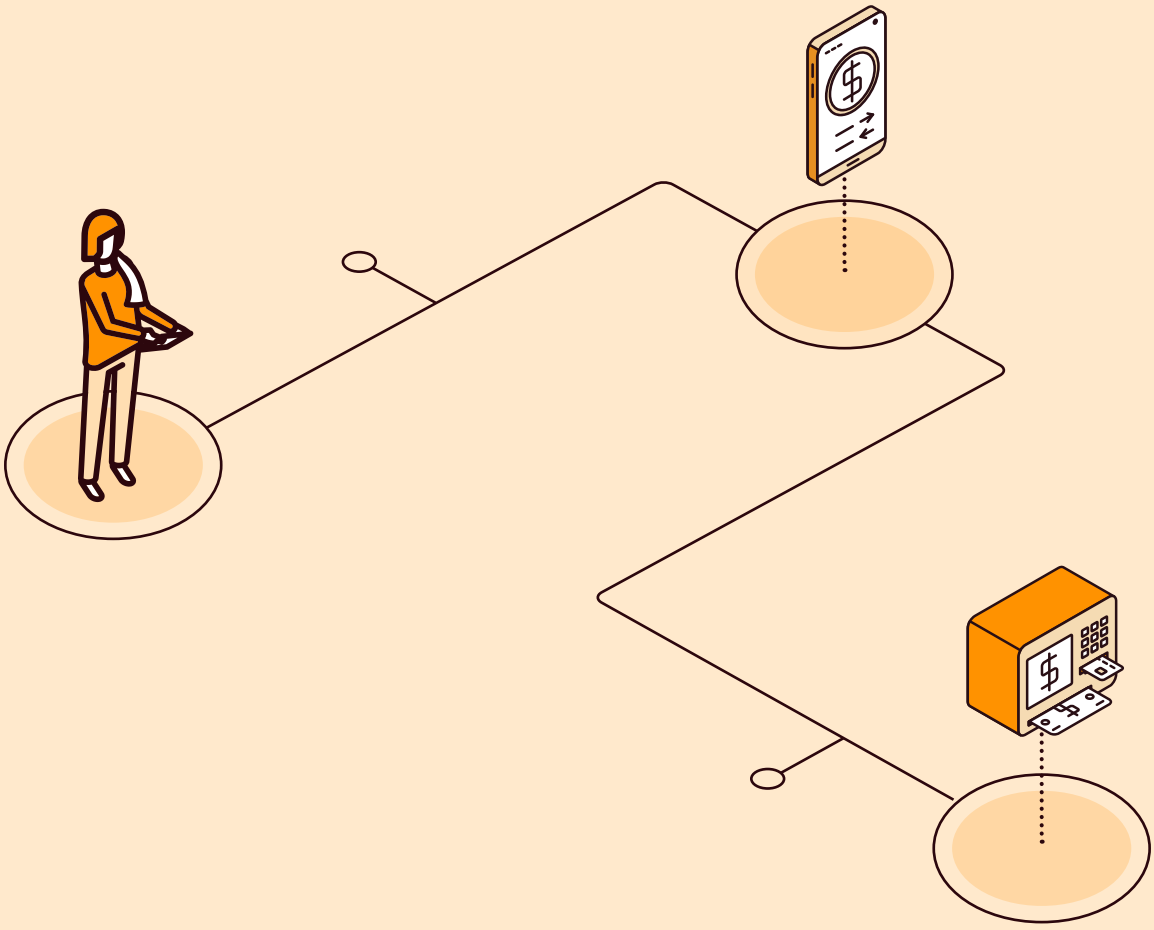
Daniel was frustrated because his municipality enabled digital processing, but payments could not be made. This was because the banks were charging him abusive fees to make online payments, which was not fair to impose on citizens or to be borne by the municipality. Now, thanks to the state's gateway, all payments can be made through this point, at no cost to the municipality.

EXAMPLES

Click on each flag or icon to go deeper.

United Kingdom
GOV.UK Pay

Spain
Payment platform



INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- Is there a payment gateway as a common service that can be used by any public institution?
- Of the central government procedures that require payments, do more than half use the payment gateway?
- Of the government-wide procedures that require payments, do more than half use the payment gateway?

5.2.8 SECTOR SERVICES

The institution in charge of the digital transformation is responsible for making the common services described above available to the different sectoral administrations: the multichannel system, the Single government portal, the citizen folder, the scheduling system, the payment gateway, etc. However, the common services themselves have no content if they are not fed by the sectoral services of each of the existing areas in a country, such as health, justice, employment, etc. Therefore, the last step in order to offer a comprehensive service to the citizen is for each sector to activate and offer its services to citizens through the infrastructure and common services that the governing body has made available. Only each of the sectors knows the vertical specifications of their services and must add to the catalog of procedures those that can be carried out digitally and that benefit both the administration and the citizens.

Digital public services must be comprehensive, regardless of which public administration (Ministries of Justice, Education, Health, Finance, Interior, etc.) has responsibility for such services.

› For example, if the Ministry of Education is responsible for processing the application for a scholarship, but the Ministry of Finance is responsible for verifying compliance with the income level and payment of the scholarship amount, the fact that the application can only be made through the citizen folder would not be of value to the citizen if the rest of the procedures had to be done on paper, going from window to window. That is why it is necessary to implement complete services, so that the digital transformation process is seen by citizens as something positive.

On the other hand, the complexity of the administrative structure of countries must be considered: the public sector is divided into multiple spheres; there is also sometimes complexity from the territorial point of view, with territories having more or less autonomy by sector and with different levels of management (national, regional, local). However, this complexity cannot be transferred to citizens, who have the right to access quality public services, regardless of the administration in charge of providing them.

The following procedure can be assumed when a government activates the citizen folder:

1. A pilot is conducted in which citizens can access their education data: university degrees, enrollment, grades, etc.

2. Once the correct functioning and the good reception by the citizens is verified, new services from other sectors should be incorporated to offer a global service to the citizens.

It is important that after the governing entity has defined its strategy, vertical sectors or other administrations and agencies articulate their own strategies with the principles and objectives of

the national strategy. In this sense, it will be convenient to set milestones and define projects aimed at advancing in an aligned and homogeneous way in the digital transformation, in order to make progress in the provision of digital public services to citizens.

A GLOBAL VISION CAN ONLY BE DRAWN FROM THE CENTER OF THE ORGANIZATION, JUST AS THE PROPER VISION OF EACH SECTOR CAN ONLY BE OBTAINED WITH THE KNOWLEDGE OF EACH AREA.

All public sectors of an administration must understand that digital transformation is everyone's job and that all sectors must contribute to the ecosystem of digital public services. Within this framework, it is essential to promote the reuse of existing systems and solutions to:

- Avoid duplication of efforts;
- Take advantage of interoperability;
- Exchange information and knowledge.

In this way, it is possible to establish a scenario of efficiency that facilitates the provision of digital public services in the most appropriate way possible. In this sense, a strong collaboration of all public administrations and units involved is necessary to obtain an efficient administration that provides homogeneous public services.

SOME EXAMPLES THAT ILLUSTRATE THE IMPORTANCE OF SECTORAL SERVICES

- In the healthcare sector:
  - The public administration itself that manages this area must decide which of the services it provides would be beneficial to make digital: the electronic prescription, the digital health record, telediagnosis, the appointment management system, the waiting management system, etc.

- *Examples:*

  - During the pandemic it has been very important to find on the health ministry's websites information related to the COVID-19 situation, health recommendations, instructions for protection, etc. At a time when citizens could not leave their homes, what better official means to inform than through the internet, which has been the greatest refuge in times of pandemic?

  - Some countries, such as Spain, specifically in the city of Madrid, have implemented a system of health warnings via citizens' cell phones. Thanks to the cross-referencing of health data with the postal address of each person, a message was sent to them informing them of health restrictions in their area.

  - The green passport,[45] developed in Europe during the COVID-19 pandemic, will make it possible to prove whether a person has had the disease, has been vaccinated, or has undergone PCR or other tests. It is accompanied by other documents such as the *Guidelines on Verifiable Vaccination Certificates—Basic Interoperability Elements*.[46]

› In the justice sector:

- The procedures are no longer administrative, but are judicial procedures, with different legislation and regulations. The challenge is similar to that of other public administrations, but with certain particularities as it is a differentiated branch of government.

  - *Example:* the responsible administration, which has sufficient knowledge of the functioning of justice, must define:

    - The requirements to be able to admit a lawsuit filed by a lawyer through digital services;

    - How electronic communications must be configured so that they can start the computation of procedural deadlines and comply with the principles of integrity and nonrepudiation.

- Although citizens do not directly consume the services of this sector, but rather the administration of justice puts them at the service of the state's security forces and corps, the ultimate benefit is for citizens, who will have greater security in the streets.

---

45. https://ec.europa.eu/health/sites/health/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf
46. https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

- *Examples:*

  - A police officer who stops a person on the street can check a database for the existence of a criminal record, restraining orders, or precautionary measures and make an arrest at the same time, if applicable.

  - In Spain, the Central Registry of Sex Offenders, a centralized database where all convictions for a crime of a sexual nature are recorded, was set up. This has led to the formulation of a law for the protection of minors that establishes the obligation for all professionals and volunteers who work in regular contact with minors to provide negative certificates from the Central Registry of Sex Offenders. The way to apply for the certificate is simple and free, and anyone who wants to opt for a job with minors can obtain their certificate through the electronic headquarters.

- In social security:

  - *Example:* In Spain, when accessing the electronic headquarters, a notice appears so that any citizen can find out if he meets the requirements to benefit from the minimum living income benefit, as well as other economic aid to which people at risk of social exclusion can have access. Other procedures that can be carried out at the electronic office include requesting certificates of employment, applying for the European health card, and paying social security debts.

THE IMPORTANCE OF ACCOMPANYING

IT SHOULD NOT BE FORGOTTEN THAT THE VARIOUS VERTICAL SECTORS—OR TERRITORIES—MUST DECISIVELY ACCOMPANY A COUNTRY'S DIGITAL TRANSFORMATION.

No matter how much the leading institution of a country's digital transformation puts in place the transformation strategy, governance, regulatory framework development, talent-based cultural change strategy, and a multitude of common tools and services, there will not be many complete digital services to offer to citizens if the vertical sectors are not involved in this effort. In short, everyone involved in public administration, both horizontally and vertically, is called to be part of an exquisite coordination, to make the digital transformation of a country's public sector a reality.

STORIES

Fictitious anecdotes that present the concepts of this article from the perspective of different types of stakeholders

Citizen
Camilo

Camilo has obtained his electronic signature certificate, and now he is happy because he can use it to carry out procedures in all the administrations that have services in the citizen folder.

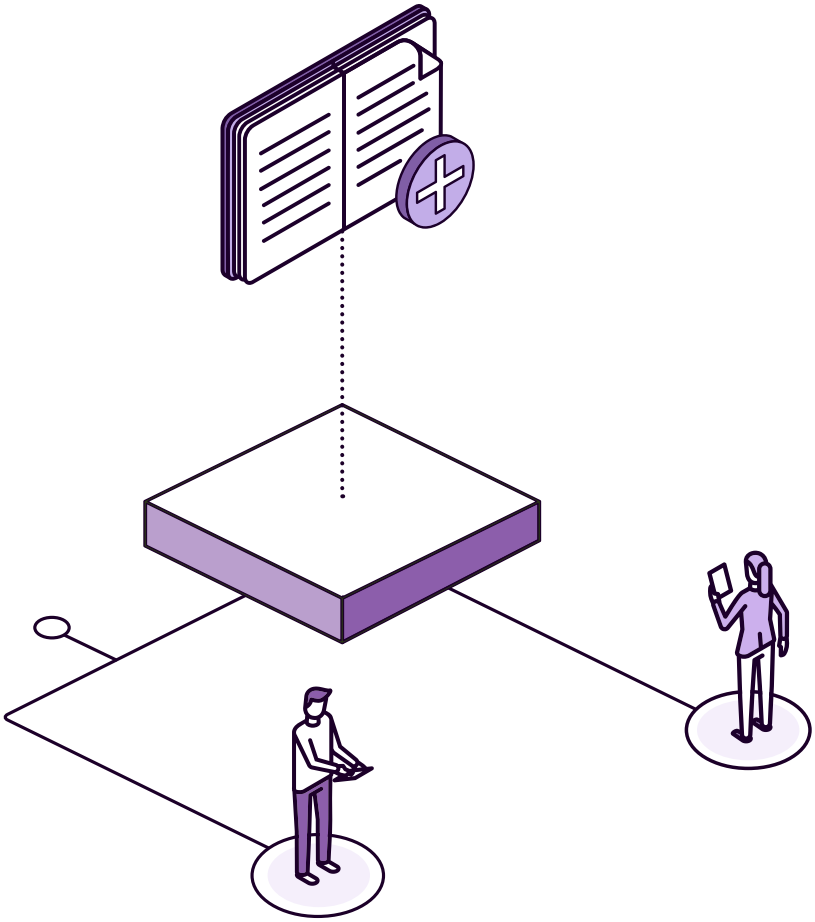
Vice minister of health
Sara

At a meeting with the directors of all the public hospitals, Sara is approached about the need for a centralized system for purchasing equipment. From her previous experience, Sara knows that the central administration has such a system, so she arranges a meeting to see what adaptations need to be made for its use in the health sector.

INDICATORS

These questions can be used to measure the degree of progress in this aspect of digital government. They are all yes or no, where "yes" indicates greater progress.

- What percentage of public administrations use any of the common services?
- How much was saved by using common services?



APPENDIXES

Throughout the guide, short fictional stories are presented that illustrate different aspects of the government's digital transformation. These stories are told from the perspective of four invented people: Camilo, a citizen; Ana, a businesswoman; Sara, the vice minister of health; and Daniel, an advisor to the mayor.

Citizen
Camilo

Camilo is thirty-six years old and lives in a large city. He works in a clothing store and drives a cab two nights a week to supplement his income. He has a five-year old daughter and lives with his grandmother in a downtown apartment. He completed high school and is saving for a degree at a technical university. He has a computer at home, which only uses for emailing, consulting social media and helping with his daughter with her schoolwork. He meets the criteria to be eligible for several government food and health subsidies.

Entrepreneur
Ana

Ana is the owner of a company that produces microchips. The firm has grown significantly in the past years and currently has more than two hundred employees with offices in several countries in the region. She is a systems engineer and strives to keep up to date with the latest technological developments in order to increase her company's productivity.

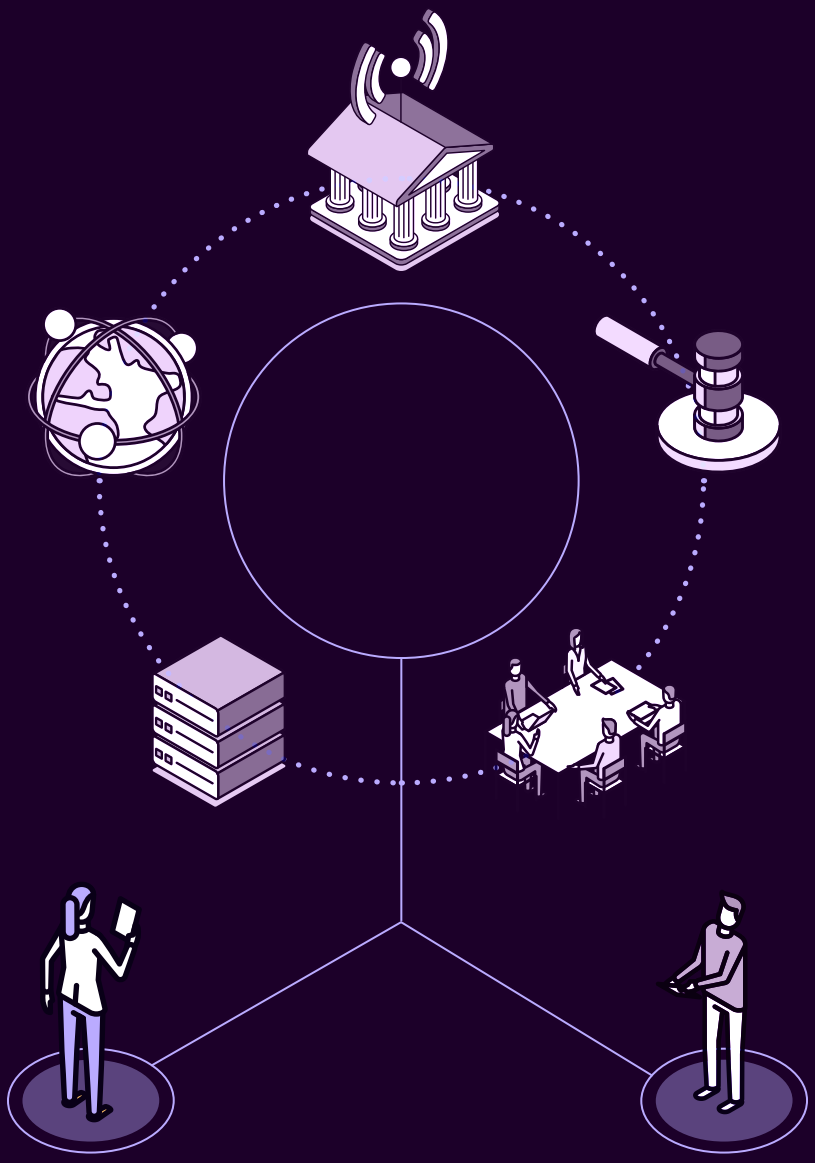
Vice minister of health
Sara

Sara is the Vice minister Health and is in charge of, among other things, the public health and disease prevention policy agenda. She previously worked in the digital government authority and brings to the ministry several ideas to transform the most inefficient processes.

Advisor to the mayor
Daniel

Daniel is the advisor to the mayor of a small city of about five thousand inhabitants. He deals with a wide range of issues, from environmental regulatory reform to district education programs to the city's innovation agenda.

IDB
Improving lives



Government digital transformation guide