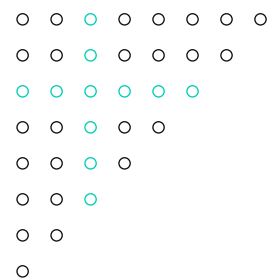


# DIGITAL STRATEGIES **IN PACIFIC ALLIANCE** COUNTRIES





#### TicTac

**Program Development Director**  
Adriana Ceballos López

**Project Coordinator:**  
Andrea Lucía Torres Arias

**Research Team:**  
Michael Sepulveda Castillo  
Andrea Lucía Torres Arias

**Acknowledgments:**  
Ashley Friedman

**Diseño y diagramación:**  
Paula Cruz Giraldo

#### About the TicTac

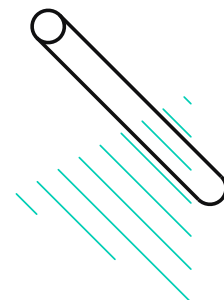
The TicTac is the first analysis and creativity tank of the ICT sector in Colombia, established by the CCIT in order to propose public policy initiatives oriented to the digital transformation of the country, with based on sustainability and economic competitiveness, social inclusion and government efficiency.



**Attribution-NonCommercial 4.0 International.**

**Copyright © TicTac 2021**

All rights reserved. Distribution and use of this non-commercial document is allowed without restrictions.



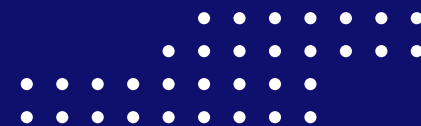
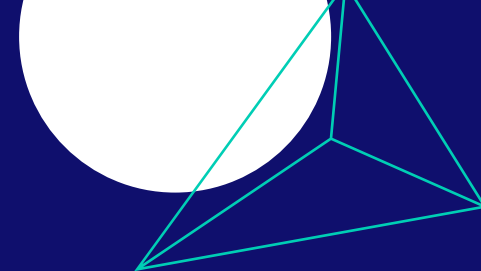
# DIGITAL STRATEGIES IN PACIFIC ALLIANCE COUNTRIES







# Contents



Introduction

06

1

Privacy

08

2

Cloud-based  
**services**

38

3

Broadband

54

4

Cybersecurity

64



Conclusions

86



References

106

# Introduction



The enormous challenges that have arisen in recent years have forced governments to act quickly in front of different circumstances, making use of the available technological tools, to ensure the well-being of the population. This has been one of the driving forces of change that has allowed countries to reach new levels of technological development.

Latin America has not been unaware to this situation, which has put it in a scenario of opportunity to adopt the necessary changes to support the advantages of digital transformation to the entire population. While this situation has been fundamental to mitigate certain impacts, for example, by allowing teleworking, virtual education, and the strengthening of e-commerce, among others, the region has shown the importance of reducing the digital gap among its population.

Precisely, the Pacific Alliance, formed by Chile, Colombia, Mexico, and Peru, with the intention of encouraging regional integration, growth, development and competitiveness of the countries. It has recently made a statement on the importance of promoting digital transformation to accelerate compliance with the Sustainable Development Goals set out in the 2030 Agenda of the United Nations.

In this sense, it is intended to show the digital strategies currently implemented by the governments of the Pacific Alliance countries, through a study of the context and results of each country, to identify best practices in the region. Hence the importance of knowing the actions taken before and after the crisis and analyzing their impact, to learn lessons and discover aspects to be considered around issues related to information technologies and telecommunications and their optimal use as enablers of other sectors of the economy.

This document is divided into four sections, reviewing first the legal and regulatory framework, followed by the actions taken before and during the pandemic and the analysis of each of the policy strategies implemented. The first section addresses the issue of privacy, followed by broadband, the third section discusses cloud-based services, and the final section is devoted to cybersecurity.



# 01

Privacy



The technological context refers to the interest that individuals have in exercising control over access to information about themselves and is most often referred to as "information privacy"<sup>1</sup>. For this reason, the governments have established data protection regimes in response to increasing levels of personal data processing.

For data protection, there has been enormous legal progress in granting users control over their privacy. Of the Pacific Alliance countries, Chile was the first country to adopt such a law in 1999. It took more than a decade for Mexico to adopt it in 2010, then Peru in 2011, and Colombia in 2012. The rapid advance of technology has made member countries respond to these challenges, primarily by referring to European legislation. Precisely with the General Data Protection Regulation of the European Union that came into force in 2016 (which as of 2018 is mandatory) and the granting of greater control of data owners, it has opened a space for a new generation of legislation on privacy protection.

<sup>1</sup> (Stanford, 2014)



The Peruvian regulatory framework is solid in terms of data protection granted through Law 29733 from 2013, amended in 2017. This modification arose from global trends in data protection, as for example in which communications protocols are considered facing data security incidents addressed to the affected holder and the regulatory body in the country. In addition, evaluations, and privacy impact analysis, which allow to guide more efficiently the implementation of controls to mitigate risks of leakage or loss of personal data information in companies.

This has left the country with a clear protection law, a control authority, provisions on data access in emergency cases, a mandate on data retention and allows the transfer of personal data<sup>2</sup> to other countries, if the receiving country maintains adequate levels of protection in accordance with Peruvian data protection law.

<sup>2</sup> Legislative Decree 1182 requires telecommunications companies to retain metadata for 12 months and to disclose the data by judicial authorization in real time.

<sup>3</sup> (Rodríguez & Alimonti 2020)

<sup>4</sup> Código Procesal Nacional, Article 303

<sup>5</sup> (Council of Europe, 1981)

<sup>6</sup> (Council of Europe, 2017)



Mexico, unlike the other countries analyzed, adopted a federal protection law for data held by private entities in 2010 and a related regulation in 2011. In 2017, it adopted a data protection law for information held by public entities, including law enforcement<sup>3</sup>. Likewise, the country has clear provisions for data access in cases of emergency<sup>4</sup>, the mandate on data retention issued by the Federal Telecommunications and Broadcasting Law in 2014.

Within this progressive line in data protection, the country is the only member of the Pacific Alliance that is part of Convention 108<sup>5</sup> and the additional protocol on control authorities and transborder data flows<sup>6</sup>. This implies the availability of shared international tools to achieve effective support and exchange of information for the defense of citizens' personal data and the right to respect for privacy.



## Chile

Despite being one of the first countries to adopt a privacy regulation, Chile has manifested some fundamental challenges. The first and most discussed is the absence of an exclusive authority for data protection control. This situation has opened the door for personal information to circulate freely and legally in Chilean territory by multiple companies dedicated to massive personal data processing. The data are repeatedly exchanged by companies providing commercial, financial, health, telecommunications, and other services, thus violating the right to privacy and other rights protected by the Constitution. The second does not provide specific rules regarding the transfer of personal data to third countries.

Undoubtedly, the challenge facing the change of the Constitution that was approved in 2020 through the plebiscite, represents an opportunity to safeguard the right and protection of privacy. Precisely these issues have been strongly criticized and once again put under discussion with the pandemic by privacy experts<sup>7</sup>. For this reason, this historic milestone of drafting the Magna Carta, for the first time in a partisan way, is the opportune space for the strengthening of a regulatory framework that allows the use of information through data for the welfare of the majority, according to the challenges and trends that currently represent the technology and that we have highlighted above.

<sup>7</sup> (Álvarez Valenzuela, Daniel, 2016)

<sup>8</sup> (Donoso & Vega, 2020)

<sup>9</sup> The Constitutional Court of Colombia has pointed out that these exceptions are not excluded from the application of the data protection law, but are exempted from some of its provisions by virtue of their interest. (Rodríguez, Alimonti, & Castañeda, 2020)

<sup>10</sup> Decreto 1704 de 2012

## Colombia

The country has shown strong regulation during the last year, highlighting the Data Protection Law 1581 of 2012, which makes privacy a fundamental right, applies it to data held by the public sector, with a few exceptions<sup>9</sup>. Colombia has supervisory authority, provisions on access to data in case of emergency, and a data retention mandate<sup>10</sup>. Data may be transferred to other countries if the supervisory authority determines whether the receiving country complies with the same privacy legislation standards.



## 1.1. LEGAL AND REGULATORY FRAMEWORKS

Fast technological progress has made it necessary for countries to carefully review the laws and standards under which they operate, opening a whole new field for the regulations in which they operate. In this context, the Pacific Alliance countries have had a diverse reaction to the way they regulate privacy protection:

### Peru

In Peru, the data protection laws and regulations are:

- 1 Political Constitution
- 2 Law 29733 known as the Personal Data Protection Law <sup>11</sup>.
- 3 Supreme Decree 003-2013-JUS: Regulation of the Personal Data Protection Law.

The Political Constitution of Peru establishes that every person has the right that computer services, whether computerized or not, public or private, do not provide information that affects personal and family privacy<sup>12</sup>. The Personal Data Protection Law develops the rights of the holders of personal data, the principles and conditions that must be applied in its treatment.

<sup>11</sup> (Congreso de la República del Perú, 2011)

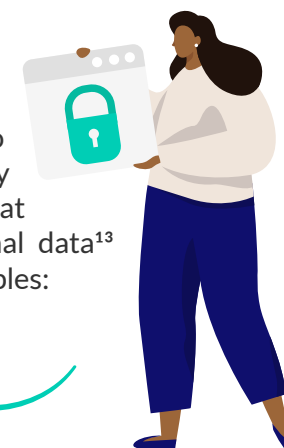
<sup>12</sup> Article 2, Numeral 6

<sup>13</sup> (Defensoría del Pueblo del Perú, 2019)

The Regulation of the Personal Data Protection Law regulates the registration in the National Registry of Personal Data Protection, as well as the sanctioning regime in case of non-compliance with the regulations on personal data protection.

### I. Guiding Principles for the Use of Personal Data in Peru

To provide a sufficient condition of protection to personal information, any natural or legal person that collects and processes personal data<sup>13</sup> must apply the following principles:







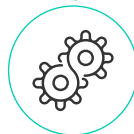
**Lawfulness:** The processing of personal data must be carried out in accordance with the requirements and provisions established by law.



**Consent:** The authorization of the holder is required to carry out the processing of personal data.



**Purpose:** Personal data must be collected and processed only for a specific and lawful purpose.



**Proportionality:** The processing of personal data should be in accordance with its purpose, avoiding any excess.



**Quality:** Personal data to be processed must be truthful, accurate and up to date.



**Provision for recourse:** There must be administrative and jurisdictional channels for the owners of personal data to complain against any irregular processing.



**Adequate level of protection:** A minimum level of protection must be guaranteed in the transborder flow of personal data.



**Security:** The owner of the personal data bank and the data processor must provide security and protection for the data they manage and process.

## II. Rights of the data subject

All holders of personal data have the following rights before data processors and data banks:



**Access:** Every person has the right to know what information about him/herself has been stored in a public or private data bank; how and why it was collected; as well as the transfers made or those that are planned to be made.



**Rectification:** Every person has the right to request the modification of data that was collected erroneously, incompletely, inaccurately, outdated or falsely, in a public or private data bank. In turn, it allows the updating and inclusion of new personal data.



**Cancellation:** Any person may request the cancellation or deletion of their data, when it no longer serves a purpose, when consent has been revoked or when the term for its processing has elapsed.



**Opposition:** Any person may oppose the processing of their personal data stored in public or private bank.

In addition, data subjects have the following rights:

### Right to information



The holder has the right to be informed about the processing of his/her data, as well as about the purpose, recipients, the bank in which they will be stored, the time of conservation and what is related to the processing.

### Right to protection



If the rights of the holder of personal data are totally or partially denied, the affected party may resort to the National Authority for the Protection of Personal Data or to the Judiciary, to exercise the defense of such rights.

### Right to prevent the provision



Personal data may be prevented from being supplied to third parties when the holder's fundamental rights are at risk.

### Right to compensation



In case the owner of personal data is affected because of a breach of the Personal Data Protection Law, he/she has the right to obtain the corresponding compensation.



### III. Duties of the banks and persons in charge of the processing of personal data

The owner of the personal data bank is the natural person, private legal entity or public entity that establishes the purpose for the collection and storage of personal data, as well as the processing and security measures that will be applicable. On the other hand, the person in charge of the processing of personal data is the natural or legal person, public or private, who carries out the processing of the data in the name and on behalf of the owner of the database. In case he/she carries out a processing outside the purpose of the assignment, he/she may assume responsibilities<sup>14</sup>.

Both the data bank owner and the processor have the following obligations:

- To carry out the processing of personal data only if the data subject has given valid consent.
- Not to collect personal data fraudulently, unfairly, or unlawfully.
- Collect only those data that are necessary to achieve the purpose previously informed to the holder.
- Not to use personal data for different purposes, except for anonymization or dissociation procedures.
- Not to limit the exercise of the rights of the holder of personal data.

- Replace or supplement personal data when they are inaccurate or incomplete.
- Delete those personal data that are no longer necessary or the term for their processing has expired.
- Provide the National Authority for the Protection of Personal Data with the information it requires on data processing and access to the banks.

### IV. Control and Surveillance Entities

The General Directorate for Transparency, Access to Public Information and Protection of Personal Data is the body that exercises the National Authority for the Protection of Personal Data, together with the National Authority for Transparency and Access to Public Information.

The National Authority for the Protection of Personal Data, which hierarchically reports to the Vice-Ministerial Office of Justice of the Ministry of Justice and Human Rights, has as its main function to guarantee the fundamental right of protection of personal data.

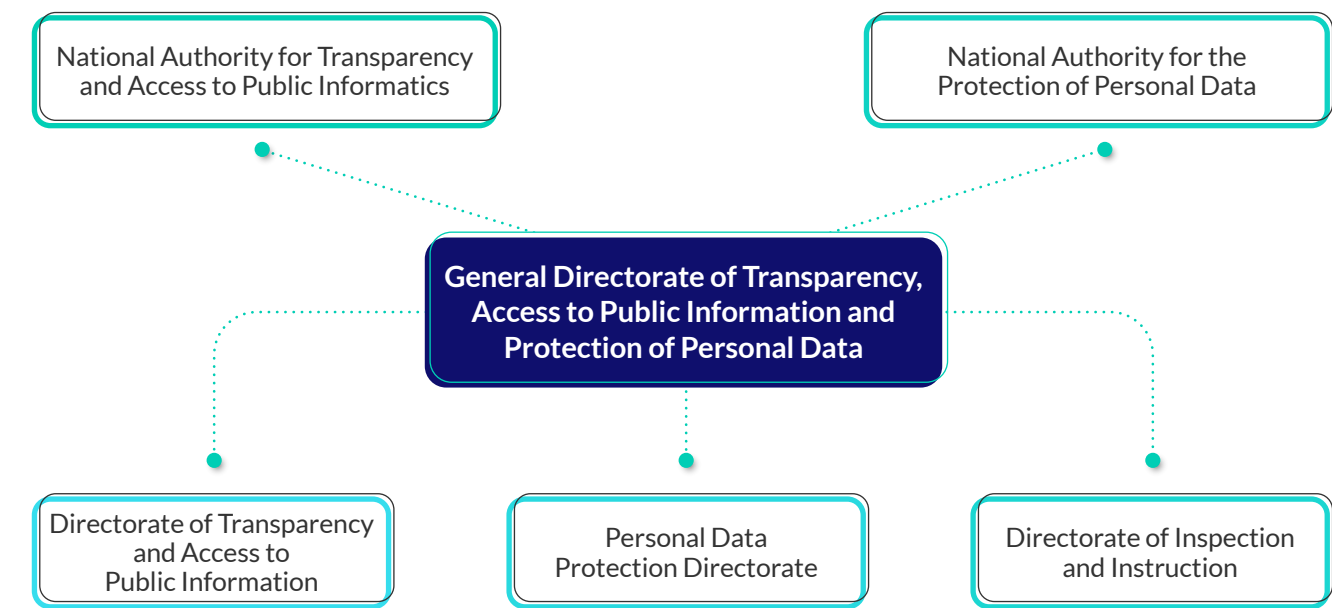


Figure 1: SUPERVISORY AUTHORITY IN PERU Source: Ombudsman's Office of Peru, 2019

## Mexico

In Mexico, the regulatory and legislative framework for data protection is:

- 1 The Political Constitution.
- 2 Federal Law for the Protection of Personal Data in Possession of Private Parties.
- 3 General Law for the Protection of Personal Data in Possession of Obligated Subjects.
- 4 State laws for the protection of personal data (one for each state).

<sup>14</sup> (Defensoría del Pueblo del Perú, 2019)

The Mexican Constitution<sup>15</sup> establishes that every person has the right to the protection of his or her personal data and to access, rectify and cancel them, as well as to express his or her opposition to their processing. In addition, it establishes the right to the protection of information related to the private life of individuals when this information is in the possession of the federal or state governments. The right to the protection of personal data of individuals is considered a fundamental right.

The Federal Law for the Protection of Personal Data in Possession of Private Parties (LFPDPP) establishes the protection of personal data in possession of private parties, with the purpose of regulating its legitimate, controlled and informed treatment, in

order to guarantee the privacy and the right to informative self-determination of individuals<sup>16</sup>.

The General Law for the Protection of Personal Data in Possession of Obligated Subjects issued in 2017, aims to establish the bases, principles, and procedures to guarantee the right that every person has to the protection of their personal data, in possession of obligated subjects. In other words, this law applies to the processing of data in the public sector and is understood as obligated subjects at the federal, state, and municipal level, any authority, entity, body and agency of the Executive, Legislative and Judicial Branches, autonomous bodies, political parties, trusts and public funds<sup>17</sup>.

## I. Guiding principles for the use of personal data in Mexico

As mentioned above, the protection of personal data in Mexico is governed by certain guiding principles, which are summarized in the LFPDPP:



**Lawfulness:** All data processing must be carried out in compliance with the provisions of Mexican and international law<sup>18</sup>.



**Consent:** Consent must be obtained from the owner of the data for its processing. Generally, this consent is tacit and is obtained after having placed the privacy notice<sup>19</sup>.

<sup>15</sup>Article 6

<sup>16</sup> (Congreso General de los Estados Unidos Mexicanos, 2011)

<sup>17</sup> (Congreso General de los Estados Unidos Mexicanos, 2017)

<sup>18</sup> LFPDPP, Article 7

<sup>19</sup> LFPDPP, Article 5



**Information:** Inform the owner of the data through the privacy notice the information regarding the existence and main characteristics of the treatment to which their personal data will be subjected<sup>20</sup>.



**Quality:** Treat the personal data accurate, complete, relevant, correct and updated according to the purposes for which they were obtained. When the data are provided by the owners, it is understood that the data controller follows this principle<sup>21</sup>.



**Purpose:** Personal data may only be obtained and processed to fulfill the purposes established in the corresponding privacy notice<sup>22</sup>. Thus, if there is another purpose that is not established in the privacy notice, the consent of the owners must be obtained, and the privacy notice must be modified to inform about the new purposes<sup>23</sup>.



**Loyalty:** All personal data must be treated giving priority to the protection of the owner's interests and the reasonable expectation of privacy; therefore, under no circumstances must personal data be obtained through deceitful or fraudulent means<sup>24</sup>.



**Proportionality:** Only those personal data that are necessary, adequate, and relevant in relation to the purposes for which they have been obtained shall be processed<sup>25</sup>.



**Responsibility:** You must ensure and be responsible for the processing of personal data held in your possession, and for those that you have communicated to a third party, whether these third parties are in Mexico or abroad<sup>26</sup>.

<sup>20</sup> LFPDPP, Article 3 and 23

<sup>21</sup> LFPDPP, Article 36

<sup>22</sup> LFDPP, Article 12

<sup>23</sup> (Equipo Legal Amazon México, 2019)

<sup>24</sup> LFPDPPP, Article 7

<sup>25</sup> LFPDPPP, Article 45

<sup>26</sup> LFPDPPP, Article 6 and 12



# Rights of the data owner

# ARCO RIGHTS

The owner of the information has the right to:

## Right of Access:

To obtain and know your:

- Possession.
- Category.
- Elaboration.
- Utilization.
- Provision.
- Divuligation.
- Organization.
- Conservation.
- Communication.
- Transfers.
- Storage.
- Utilisation.
- Use.
- Purposes.
- Register.
- Diffusion.
- Driving.
- Access.

## Right to Rectify

When they are:

- Inaccurate.
- Incomplete.
- Wrong.
- Outdated.

## Right to Cancel

When:

- Not fit for purpose.
- They do not conform to the law.
- Consent is revoked.
- The treatment is illegal.
- Spread without consent.

## Right of Opposition

Reasons:

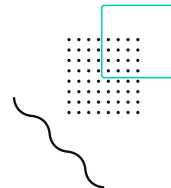
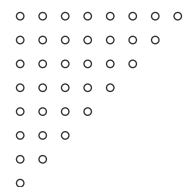
- The automated treatment.
- The automated treatment produces unwanted effects.
- That significantly affect their interests, rights and liberators.

Figure 2: ARCO RIGHTS Source: (National legal regime for the protection of personal data)

## II. Duties of data controllers and processors of personal data

The following are the duties of data controllers and data processors<sup>27</sup>:

- Keep strict confidentiality regarding the personal data provided to them by individuals..
- Implement physical, managing, and technical security measures to protect the personal data they process against damage, loss, alteration, destruction or unauthorized use, access or processing.
- Prevent unauthorized access, damage or interference to physical facilities, critical areas of the organization, equipment, and information.
- Protect mobile, portable, or easily removable equipment located inside or outside of the facilities.
- Provide equipment containing or storing personal data with maintenance to ensure its availability, functionality, and integrity.
- Ensure secure disposal of personal data.



<sup>27</sup> (Congreso General de los Estados Unidos Mexicanos, 2011)

## III. Control and Surveillance Entities

The National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) is the authority responsible for promoting and monitoring compliance with the right to protection of personal data in Mexico.

### Chile



In Chile, the data protection laws and regulations are:

- 1 The 1980 Constitution.
- 2 Law 19.628 on the protection of private life of 1999.
- 3 Law 19.812 of 2002.
- 4 Law 20.463 of 2010.
- 5 Law 20.575 of 2012.

The 1980 Constitution establishes the respect and protection of the private life of the individual and his family<sup>28</sup>, the inviolability of the home and all forms of private communication<sup>29</sup>. Although the Chilean Magna Carta does not regulate the right to privacy, those interests linked to it are present in the constitutional regulations.

With Law 19.812 of 1999, Chile became the first country in South America to adopt a regulatory framework on privacy. The law specifically regulates the processing of personal data, the operation of databases, the rights, and duties of those involved and a dispute resolution mechanism. However, the law left gaps in the treatment of data by third parties and has been criticized as follows<sup>30</sup>.

### I. Guiding Principles for the use of personal data in Chile



**Freedom in the processing of personal data:** Establishes that any person may carry out the processing of personal data. Provided that the processing is carried out according to the law, for purposes allowed by the legal system, and the full exercise of the fundamental rights of the data owners and the powers recognized by law must be respected<sup>31</sup>.



**Information and consent of the owner:** Protects the right of individuals to control the information that concerns them, the law establishes that the processing of personal data can only be carried out with the express authorization of the law -understood as Law 19.628 itself, or other- or of the owner of the data.

<sup>28</sup> Article 19 No.4

<sup>29</sup> Article 19 No.5

<sup>30</sup> (Viollier, 2017)

<sup>31</sup> (Ministerio Secretaría General de la Presidencia, 1999)



**Purpose:** It mandates that personal data may only be used and processed for the purposes for which they were collected. This principle is closely related to the principle of information and consent of the owner, since it would be illegitimate for the data to be used for purposes other than those consented to by the owner<sup>32</sup>.



**Quality of the data:** It requires that the personal data must be accurate, updated and truthfully respond to the real situation of its owner. Failure to comply with this duty gives rise to the holder requesting that the data be modified, blocked, or deleted<sup>33</sup>.



**Special protection of sensitive data:** In the first instance, the processing of sensitive data is prohibited, unless authorized by law, with the consent of the owner, or if such data is necessary for the determination or granting of health benefits that correspond to their owners<sup>34</sup>.



**Data security:** It establishes the duty of the person responsible for the records or bases where personal data are stored, to take care of them. However, no specific measures are established for this purpose with due diligence, being responsible for the damages caused.



**Duty of secrecy:** It is established that the persons in charge of the registers or data banks have the obligation to keep secret the personal data recorded therein, to the extent that they come from or have been collected from sources not accessible to the public. Said obligation is not extinguished by the cessation of their activity as database manager, and therefore the obligation is extended<sup>35</sup>.

<sup>32</sup> (Viollier, 2017)

<sup>33</sup> Ley 19.628, Article 9

<sup>34</sup> Ley 19.628, Article 10

<sup>35</sup> Ley 19.628, Article 7

<sup>36, 37</sup> Ley 19.628, Article 12

<sup>38</sup> Ley 19.628, Article 6

## II. Rights of the data owner



### Right of information or access.

Gives the holder of personal data the right to request the data controller to provide information about the data concerning him/her, its origin and recipient, the purpose or purpose of storage and the individualization of the persons or organizations to which his/her data are regularly transmitted<sup>36</sup>.

### Right to modification or rectification.

Allows the owner of the data to request its modification, and the correlative obligation of the person in charge of the database to carry out such modification, when the data is erroneous, inaccurate, misleading, or incomplete, and this is proven<sup>37</sup>.



### Right of cancellation or deletion

The cancellation shall correspond, and may be requested by the holder, when their storage lacks legal basis or when they are outdated.

### Right of blocking.

It is the temporary suspension of any processing operation of the stored data. Those responsible for personal data banks must block personal data whose accuracy cannot be established or whose validity is doubtful and in respect of which cancellation does not correspond<sup>38</sup>.



### III. Control and oversight entities

One of the main criticisms of the Chilean regulatory and legislative framework on privacy is that there is no established control authority. This implies that all matters concerning data protection are brought before the ordinary courts of justice.

## Colombia

In Colombia, the regulatory framework contains several provisions concerning data protection, the following being fundamental:

- 1 Political Constitution.
- 2 Statutory Law 1581 of 2012.
- 3 Law 1712 of 2014.
- 4 Decree 1008 of 2018.

Article 15 of the Political Constitution of Colombia states that all persons have the right to personal and family privacy and to a good name, and the State must

respect them and ensure that they are respected. Similarly, Article 74 determines that it is a fundamental right to access public information, except for the exceptions established by law.

For its part, Law 1581 of 2012 constitutes the general framework for the protection of personal data in Colombia. Law 1712 of 2014, which regulates access to public information, provided that all information in the possession, control or custody of a State entity is public, and may not be reserved except as provided by law. Likewise, it defined that the information in possession of a public entity that belongs to the own private or semi-private sphere of a natural or legal person shall be considered as classified and shall be protected.

### I. Guiding principles for the use of personal data in Colombia



**Legality:** The processing of data must be subject to the provisions of the law and other provisions that develop it.



**Purpose:** The processing must obey a legitimate purpose in accordance with the Constitution and the Law, which must be informed to the owner.



**Freedom:** Processing may only be carried out with the prior, express, and informed consent of the owner. Personal data may not be obtained or disclosed without prior authorization, or in the absence of legal or judicial mandate that relieves the consent.



**Truthfulness or quality:** The information subject to processing must be truthful, complete, accurate, updated, verifiable and understandable. The processing of partial, incomplete, fractioned, or misleading data is prohibited.



**Transparency:** Processing must guarantee the right of the owner to obtain from the data controller or data processor, at any time and without restrictions, information about the existence of data concerning him/her.



**Restricted access and circulation:** Processing may only be carried out by persons authorized by the Data Controller and/or by the persons provided for in this law. Personal data, except for public information, may not be available on the Internet or other means of mass dissemination or communication, unless access is technically controllable to provide restricted knowledge only to the Data Controller or third parties authorized in accordance with this law.



**Security:** The information subject to processing by the data controller or data processor shall be handled with the technical, human, and administrative measures necessary to provide security to the records avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access<sup>39</sup>.



**Confidentiality:** All persons involved in the processing of personal data that are not of a public nature are obliged to guarantee the confidentiality of the information, even after the end of their relationship with any of the tasks involved in the processing and may only provide or communicate personal data when this corresponds to the development of the activities authorized by law.

### Rights of the data owner



To know, update and rectify their personal data against the data controllers or data processors. This right may be exercised, among others, against partial, inaccurate, incomplete, fractioned, misleading data, or data whose processing is expressly prohibited or has not been authorized.



To request proof of the authorization granted to the data controller, except when expressly exempted as a requirement for the processing.



To be informed by the data controller or data processor, upon request, regarding the use given to their personal data.



File complaints before the Superintendency of Industry and Commerce for violations of the provisions of this law and other rules that modify, add or supplement it.

<sup>39</sup> During the term of the health emergency declared by the Colombian government by COVID-19, management will be limited to the technical, human and administrative safety measures available to health service providers, provided that the purpose is to protect the fundamental rights to life with dignity and health of patients.



To revoke the authorization and/or request the deletion of the data when the treatment does not respect the principles, rights and constitutional and legal guarantees. The revocation and/or deletion will proceed when the Superintendence of Industry and Commerce has determined that in the processing the data controller or processor has incurred in conduct contrary to this law 1581 of 2012 and the Constitution.



Access free of charge to your personal data that have been subject to processing.

## II. Duties of those responsible and in charge of the processing of personal data

Those in charge of the processing shall comply with the following duties, without prejudice to the other provisions provided for in this law and others governing their activity:

- Guarantee the holder, always, the full and effective exercise of the right of habeas data.
- Keep the information under the security conditions necessary to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
- Timely update, rectification, or deletion of data under the terms of this law.

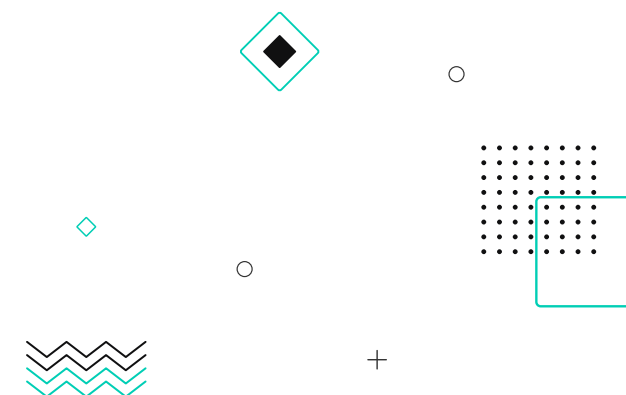
- Update the information reported by the data controllers within five (5) business days from its receipt.
- Process queries and claims made by data owners under the terms set forth in this law.
- Adopt an internal manual of policies and procedures to ensure proper compliance with this law and, in particular, for the attention of queries and claims by the owners.
- Register in the database the legend "claim in process" in the manner regulated by this law.
- Insert in the database the legend "information under judicial discussion" once notified by the competent authority about judicial proceedings related to the quality of the personal data.
- Refrain from circulating information that is being disputed by the holder and whose blocking has been ordered by the Superintendence of Industry and Commerce.
- Allow access to information only to persons who may have access to it.
- Inform the Superintendence of Industry and Commerce when there are violations to the security codes and there are risks in the administration of the information of the holders.
- Comply with the instructions and requirements given by the Superintendence of Industry and Commerce.



Those responsible for the treatment must comply with the following duties, without prejudice to the other provisions set forth in this law and in others that govern their activity:

- Guarantee the holder, at all times, the full and effective exercise of the right to habeas data.
- Request and keep, under the conditions set forth in this law, a copy of the respective authorization granted by the owner.
- Properly inform the owner about the purpose of the collection and the rights that assist him by virtue of the authorization granted.
- Keep the information under the security conditions necessary to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
- Guarantee that the information provided to the person in charge of the treatment is truthful, complete, exact, updated, verifiable and understandable.
- Update the information, communicating in a timely manner to the person in charge of the treatment, all the news regarding the data that you have previously provided and adopt the other necessary measures so that the information provided to it is kept up-to-date.
- Rectify the information when it is incorrect and communicate the pertinent to the person in charge of the treatment.
- Provide the person in charge of the treatment, as the case may be, only data whose treatment is previously authorized in accordance with the provisions of this law.

- Require the person in charge of the treatment, at all times, to respect the security and privacy conditions of the owner's information.
- Process inquiries and claims formulated in the terms indicated in this law.
- Adopt an internal manual of policies and procedures to guarantee adequate compliance with this law and, in particular, for the attention of queries and complaints.
- Inform the person in charge of the treatment when certain information is under discussion by the owner, once the claim has been submitted and the respective process has not been completed.
- Inform at the request of the owner about the use given to his data.
- Inform the data protection authority when there are violations of the security codes and there are risks in the management of the information of the holders.
- Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.





### III. Control and Surveillance Entities

The Superintendence of Industry and Commerce, through a Delegation for the Protection of Personal Data, shall exercise oversight to ensure that the principles, rights, guarantees, and procedures set forth in this law are respected in the processing of personal data.



#### 1.2. CURRENT PUBLIC POLICIES



There is a difference between information security and privacy<sup>40</sup>. Privacy refers to the way in which data is collected, processed, and shared, according to specific guidelines and standards. Security refers to the way in which data is protected from internal or external attacks. With this clear, there are three actors to consider when talking about information privacy: users, data processors and governments, i.e., regulation.

**Users** are the ones who provide their information when entering a website or accessing a service. From this perspective, three mistakes are made, consciously or not:

- Underestimating the amount of information generated every day.
- Underestimating the value of this information.
- Believing that there is total privacy with the information generated.

**Data processors** are the institutions or people who receive the information provided by users and are obliged to handle it according to the rules established and previously informed to the user.

Internet access and mobile devices that have become widespread, all the time signals are sent to the installed antennas, which allow to identify each movement. But why is all this information so valuable? They are algorithms that make it possible to detect behaviors and identify trends, which can be used for advertising, economic, commercial, or political purposes, depending on the interest of those who have access to them. There are great debates about how to attract the attention of users, who, without the correct monitoring, tend to be treated as extractable resources and not as human beings subject to rights, against the idea of an economic system in which the data generated by the crowd are the fundamental product for the creation of value<sup>41</sup>.

Therefore, the **governments** of the countries have acted on the matter through regulation. The intention is, of course, to guarantee the protection of users' rights and not to hinder the benefits of the use of information if the rules are respected according to each territory.



### Peru



If a user contracted a banking or telecommunications service and sometime later received calls from another company of the same economic group trying to sell him another service, he can file a complaint under the



Personal Data Protection Law or Law 29733 of 2011<sup>42</sup>. In this country, according to the National Authority for the Protection of Personal Data, the financial, insurance and telecommunications sectors are the ones that have received the most complaints for violating the law. The use of personal information without the owner's consent, lack of security measures, failure to respect confidentiality or incomplete and/or incorrect communication of data processing conditions, are some of these complaints.

Peruvian law establishes the guidelines on the treatment of personal data in the country, clarifying the supremacy of the fundamental rights of citizens and the need for prior authorization to access them, with full right to revoke such consent at any time. According to this, the holder of the personal data bank and all those who intervene in the processing of the information must respect confidentiality, with some exceptions<sup>43</sup>.

The owner of the data has the right to be informed about the use of his data and any update or rectification of his information, to refuse to provide it, to oppose the processing of his data and, in case of authorizing it, to have it processed in an objective manner.

In this order of ideas, to guarantee transparency, the person in charge of processing the information must dispose of it, only with the prior consent of the owner, use the data for the exposed purposes and not collect it by fraudulent means and use the data for the exposed purposes.

<sup>42</sup> (Ley de protección de datos personales en Perú, 2011)

<sup>43</sup> In case of explicit judicial requirement or when national security is at risk.

<sup>44</sup> (Reglamento De La Ley Federal De Protección De Datos Personales En Posesión De Particulares, 2011)



### Mexico



There is the Federal Law for the Protection of Personal Data in Possession of Individuals<sup>44</sup> that applies to the processing of personal data that have physical or electronic media. This law obliges to obtain consent for the processing of personal data, clarifying the purpose, prior to the processing. Unless the data is obtained personally, tacit consent is valid as a rule.

Mexican law clarifies that the personal data processed must be accurate, complete, pertinent, correct, and authorized. It is expressed that it must be guaranteed that the information complies with the **Principle of quality** when provided directly by the owner and until he/she does not manifest and prove otherwise. It is not possible to use the data for purposes other than those for which it was provided, unless required by law. The owner's interests prevail, and the data processed must be the minimum necessary. They comply with the **Principle of proportionality**, i.e., only the strictly necessary data are processed, and the **Principle of accountability**, i.e., the data controller is accountable and can make use of international standards and practices of supervision and security. For the use of cloud services, data protection regulations are complied with, with transparency, the privacy of the owner is respected, and the security of the information is guaranteed.

<sup>40</sup> (VARONIS)

<sup>41</sup> (Buitrago & George, 2017)





In Chile there is law 19628 of 1999 on the protection of private life<sup>45</sup>, according to which, personal data are defined as those relating to any information concerning natural persons, identified or identifiable. The treatment of this data by public bodies is subject to a special regime, supervised by the Civil Registry and Identification Service, the administration of the registry of personal data banks of public bodies.

In the Chilean case, there is no public agency with powers to sanction or intervene in private entities that process data. The owner of the data has the right to access, modify or rectify, cancel, and block his information. There is the National Consumer Service (in charge of watching over the protection of consumers' rights) and the Council for Transparency (CPLT). Regarding the processing of personal data by public agencies, according to Law No. 20285<sup>46</sup> on access to public information, there is the CPLT, to ensure proper compliance with the law on the protection of personal data by the organs of State Administration.

Chilean law does not expressly contemplate the figure of the "person in charge" of data processing, but there are: the person responsible for the registry or data bank and the owner of the data. In this case, any person may process data if he/she respects the law and has the consent of the data owner. In this country, unlike other legislations, there is no legal obligation to register personal databases, except in the case of public bodies.

<sup>45</sup> (Régimen Legal nacional de protección de datos personales)

<sup>46</sup> (Congreso Nacional de Chile, Información Pública, Ley no. 20.285)

<sup>47</sup> (Ley 1581 de 2012)

The Chilean case has the particularity that its current constitution has not changed since the military regime of General Augusto Pinochet in 1980. On November 2, 2020, the drafting of a new constitution was approved, where it is very likely that several of the rules described here will be reconsidered.



In Colombia there is Law 1581 of 2012<sup>47</sup>. According to this law, the collection of personal data must be limited to those personal data relevant to the purpose for which they are collected, and such purposes must be clearly informed at the time of collection. The data controller must request the owner's authorization.

The Superintendence of Industry and Commerce is in charge of protecting the fundamental right of Habeas Data (to know, update and rectify the users' data). As for the authorization, it must be given orally, in writing or through unequivocal conduct (silence is not an unequivocal conduct) and those responsible must keep the proof of such authorization. The holder has the right to revoke his/her authorization by means of a claim.

When it comes to the processing of personal data of children and adolescents is prohibited, except if it is data of a public nature and it is to protect their rights. It is their legal representative who gives the authorization.

### 1.3. PRIVACY PROTECTION MANAGEMENT FACING THE COVID-19 PANDEMIC

For most countries, information related to the health status of their citizens corresponds to sensitive data that must be treated under special guidelines in accordance with the legislation of each country. As mentioned above, the states analyzed have a mandate that allows them to act in emergency situations regarding data processing.

The Covid-19 outbreak has caused transformations in several areas. As a result, many people have had to adapt to the change. Several governments have chosen to decree general isolation, others, on the contrary, have preferred to interfere to a lesser extent in the normal development of economic and socio-cultural activities, trusting that the population will acquire the necessary level of immunity to counteract the negative effects of the virus<sup>48</sup>. Several international examples show that there is great potential for supporting the detection and monitoring of cases of infection, forecasting the possible evolution of the health situation, as well as developing and evaluating policies aimed at containing and mitigating the spread of the virus. However, there are countries whose laws restrict certain data processing procedures.



<sup>48</sup> (Acosta, 2020)

<sup>49</sup> (Ministerio de Justicia y Derechos humanos Perú, 2020)

<sup>50</sup> (Gobierno de Perú, 2020)



In Peru, sharing information about a person's health, identifying them without their consent, is a violation of Law N°29733, Personal Data Protection Law, which can be punished with a fine of between 21,500 and 215,000 soles. (Almost 60USD)<sup>49</sup>. In health aspects, it seeks to protect the patient's identity, limiting public access to such information. Confidential data should not be disclosed to maintain doctor-patient trust, even after the professional relationship has ended.

Health facilities should implement the necessary security measures to prevent patient data from reaching unauthorized persons. The only official institution allowed to provide information on confirmed cases is the Ministry of Health and only the patient's sensitive data can be disclosed with the patient's consent, which must be free, prior, express, unequivocal, and unequivocal and informed. This consent must be given in writing.

In Peru, in June 2020, "*Perú en tus manos*", a mobile application, was implemented as part of the digital strategy to confront Covid-19 designed by the group "*Te Cuido Perú*"<sup>50</sup>. The application was created to warn citizens about areas with a higher probability of contagion, seeking to be used as a tool to manage the progressive return of citizens to economic activity after confinement. The application's Privacy Policy covers the processing of personal data collected, concerning personal data and health information. The purpose of the treatment of this data is to provide information on issues related to symptoms for prevention, guide patients, keep a statistical record and provide attention to citizen's doubts, ensuring the corresponding security and confidentiality.

## Mexico

For Mexico, in the context of the pandemic, the collection and processing of employee health-related data (Covid19) by employers - for the purpose of prevention and follow-up of diagnosed cases, - does not require the authorization of individuals because it is understood that the collection of this information is intended to<sup>51</sup>:

- ▶ Ensuring safety and hygiene in the workplace.
- ▶ To maintain the labor relationship
- ▶ To avoid harm to the individual and third parties.

However, health data is considered sensitive information, so the pertinent security measures must be taken. For such reason, the Mexican Government issued a Comprehensive Privacy Notice<sup>52</sup> where it is clarified that personal data will be used for the purpose of providing attention through social networks, online chat, SMS and by telephone to those persons requesting the services of locating missing persons, reporting missing vehicles, attention to drug use, medical or psychological assistance or information on procedures and services of the Public Administration. There is the Covid19 mobile application where the user, voluntarily and unilaterally, can delete the location record of the mobile device at any time. On the other hand, in case of having received support with public resources through some technological mechanism, the information must be kept in the application (except for the location of the mobile device).

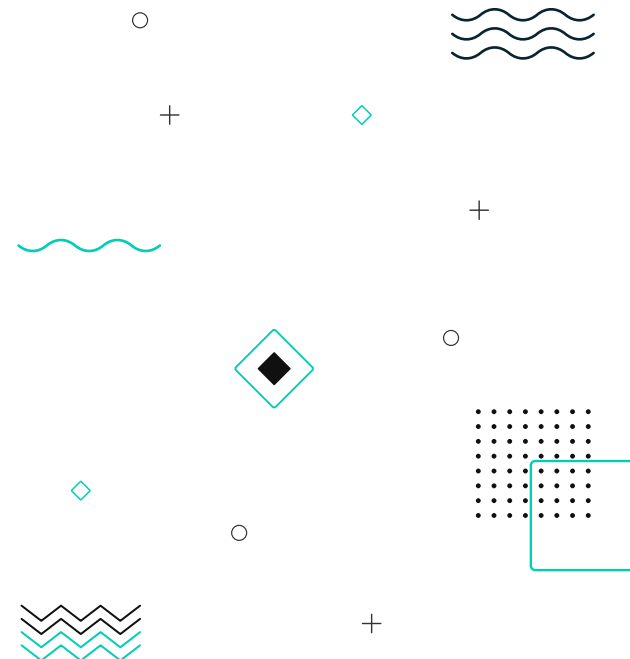
<sup>51</sup> (Mogollón González, 2020)

<sup>52</sup> (AVISO DE PRIVACIDAD INTEGRAL, 2020)

<sup>53</sup> (INFOCDMX, 2020)

In Mexico, information campaigns on data protection were carried out<sup>53</sup>. Emphasis is placed on the ownership of the information and the rights it confers, clarifying that:

- > Health Sector authorities must inform by means of the Privacy Notice, among others, the use, and purposes they will give to your personal data and the site where you can consult its terms.
- > Before providing the data, verify that the person requesting the data is an authority, entity or public body authorized to collect them, when the health emergency.
- > Avoid providing personal health-related data by misleading or unofficial electronic means.
- > Take into consideration that the technology used in relation to this pandemic should privilege the protection of sensitive personal data.



## Chile

In Chile there is the Superintendence of Health<sup>54</sup>, which ensures the confidentiality of the personal data of users who register on its website according to law 19.628. The personal data of users will be used for the fulfillment of the purposes indicated in the corresponding form and always within the competence and powers of this entity.

The user can:



Request information regarding the data banks for which the Superintendence of Health is responsible, i.e. the legal basis for their existence, their purpose, types of data stored and description of the universe of persons they comprise.



Request information about the data related to your person, its origin and recipient, the purpose of storage and the individualization of the persons or organizations to which your data is regularly transmitted.



Request the modification of your personal data when they are not correct or not up to date, if necessary.



Request the deletion or cancellation of the data provided when so desired, if applicable.

<sup>54</sup> (Superintendencia de Salud Chile)

<sup>55</sup> (CIPER CHILE, 2020)



Request, in accordance with the provisions of Law 19.628, a copy of the modified registry in the pertinent part, if applicable.



Oppose the use of your personal data for advertising purposes, market research or opinion polls.

In Chile, the CoronApp mobile application was not very well received<sup>55</sup>, for fear of biases and prejudices of those who have access to the information. Gaps and the use of imprecise language have been detected when setting the rules of the mobile application and the rights of users. This could allow data to be used for purposes that their owners do not fully understand.

The Privacy Policy states that eventually the Chilean Ministry of Health could be required to "provide access or disclose the data to third parties, by virtue of a judicial or administrative order", but it is not specified, for example, whether this could only occur in the context of an order given by an authority authorized by law to require certain data, or whether, as the user's authorization is the source of legality of the processing, his consent would be expanding the hypotheses under which administrative authorities could access and process personal data.

In addition, in the terms and conditions of service of the mobile application, it is stated that "it may be necessary to collect and process certain information, which will be obtained from the mobile device where the application has been installed", adding a new purpose: "to make improvements to the application that optimize and strengthen it, tending to achieve a satisfactory user experience". Although the Terms announce that the processing conditions will be described in the Privacy



Policy, the latter not only omits such new purpose, but also does not specify what is the "certain information" that is vaguely announced. This type of announcements that are not clear enough for citizens, generate distrust.

# Colombia

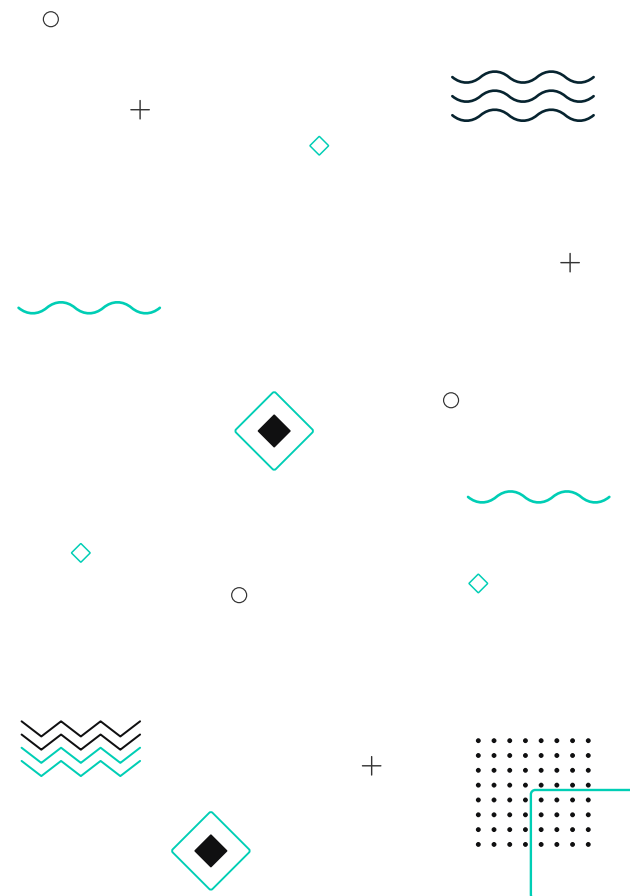
In Colombia, there is a Privacy and Confidentiality Policy of the Ministry of Health and Social Protection for the treatment and protection of personal data, which adheres to the Habeas Data law<sup>56</sup>.

The purpose of collecting health-related data is to process government services online and manage the services offered by the institution. The Ministry cannot transfer personal data of any kind to countries that do not provide adequate levels of data protection, i.e., that comply with the standards set by the Superintendence of Industry and Commerce provided in law 1581 of 2012. The security and confidentiality of the information must be always guaranteed.

In Colombia, the use of CoronApp<sup>57</sup> was implemented, an official mobile application of the Government of the Republic that allows inhabitants to have access to updated, free and accurate information on the health emergency related to the pandemic, its evolution in the country and prevention alerts, as well as to report through mobile terminals a self-diagnosis of their health status allowing the identification of possible cases. Its use is voluntary, and the citizen is free to download, use or uninstall the mobile application, as well as to request the removal of personal data.

The National Institute of Health is responsible for the handling of this information. The holder's authorization is not required when a court order has been issued or in cases of medical or health emergency.

However, it has been raised that it faces constitutional problems<sup>58</sup>. Some of the issues raised include doubts about the respect for freedom and other guarantees in force that must be observed in the collection, processing and circulation of personal data, the need for the information collected when an emergency to have clear expiration protocols, and to be eliminated when the cause for which it was collected ends.











# 02

Cloud-based  
services



Technology, data, information, and innovation have brought new challenges, especially for governments. Those who must determine to what extent and at what speed they will adopt these trends to develop better operational efficiency, help generate digital trust and improve social welfare. This action requires ensuring optimal connectivity to support this management.

Cloud services refer to the on-demand use of information technologies to provide flexibility, availability, access, and security, serving as a basis for the benefit of other processes linked to artificial intelligence (AI), the internet of things (IoT), and big data. This driver translates into agility, efficiency, and innovation.

-  The possibility for governments to have quick access to the technologies facilitates their adaptation process and encourages innovation.
-  The inclusion of these services in education boosts the development of technological skills and promotes the training of ICT talent<sup>59</sup>.
-  By guaranteeing security, access to new technological resources is enabled more quickly.
-  It does not generate additional costs associated with specialized equipment and increases technological competitiveness.
-  Increases efficiency by facilitating the management of administrative tasks.
-  Allows the incorporation of new governance models to create the IT environment according to the need.

<sup>59</sup> Talent specialized in tasks related to Information Technology and Telecommunications.



Cloud services and implementation environments are generally classified according to the infrastructure and service model according to the user's needs. The most common ones are presented below:

TYPE OF SERVICE	TYPE OF IMPLEMENTATION	SELECTION CRITERIA
<b>IAAS</b> (Infrastructure as a service) IT infrastructure leasing service to operate client computer applications	<b>PUBLIC CLOUD:</b> IT services and resources are managed and owned by the provider and are not exclusive for customer use.	All applications and data that are not national security or highly sensitive or restricted to be in the public cloud by rule or internal policy of the organization.
<b>SAAS</b> (Software as a service) Leasing service of computer applications for customer use, including required infrastructure.	<b>PRIVATE CLOUD:</b> IT services and resources are maintained on a network for the exclusive use of the client, usually its own facilities, regardless of whether the provider is owner or not.	Applications or data of national security or highly sensitive, as indicated by the regulations that must be protected in a particular way.
<b>PAAS</b> (Platform as a service) Infrastructure and software rental service for the development and operation of customer applications.	<b>HYBRID CLOUD:</b> It is a combination of public and private cloud; data and applications use resources from both clouds.	When you need to combine applications and data that should be in the private cloud and applications and data that may be in the public cloud.
	<b>COMMUNITY CLOUD:</b> Private cloud used by a set of associated clients that can share applications and resources.	When there are opportunities to share infrastructure and application capacity between organizations.

Figure 3: Classification of cloud services. Source: (García Zaballós, Iglesias Rodríguez, Puig Gabarró, & Campero, 2020).



It is estimated that globally, cloud-based services will have a valuation of 623 trillion dollars by 2025<sup>60</sup>. Such is the importance of this technology that several countries have implemented policies for the adoption of these services over the last ten years. Cloud infrastructure will grow 26.7% in Latin America by 2021<sup>61</sup>.

Adoption of cloud-based services are one way in which countries in the region can foster the development of new businesses and improve their economy. Aiming to save costs and promote innovation, the shift from traditional IT hardware to cloud services can empower governments, freeing them from obsolete, inefficient, and slow technological processes that require significant capital investments.

<sup>60</sup> (CRC, 2020)

<sup>61</sup> (trendTIC, 2020)

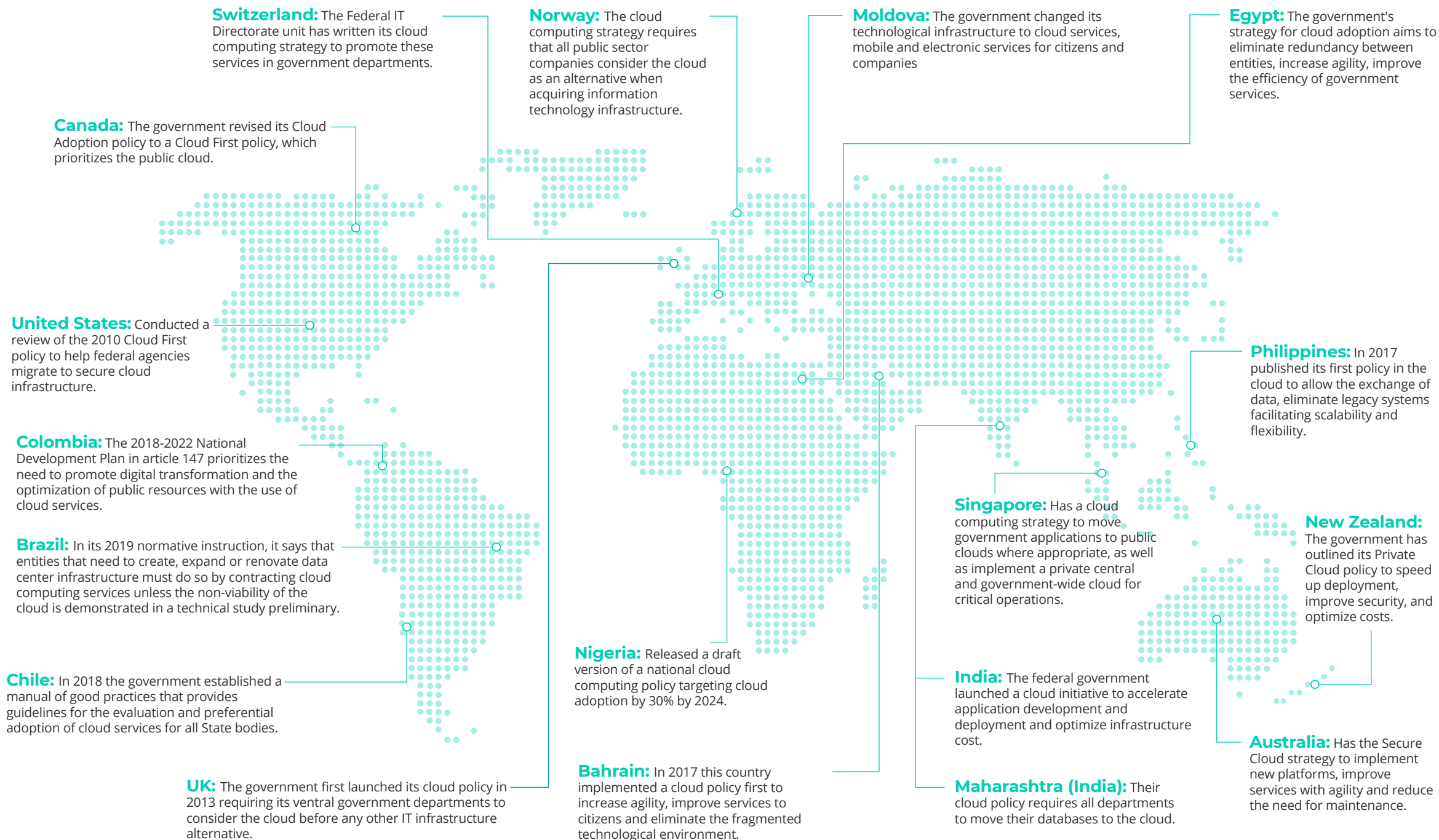


Figure 4: Strategies and policies for the adoption of cloud services. Source: (TicTac, 2020)







## 2.1. LEGAL AND REGULATORY FRAMEWORKS >>>>

### Peru >>>>

In Peru, through the document "Guidelines for the Use of Cloud Services"<sup>62</sup>, recommendations are established to prepare strategies for the use of the cloud in each government entity, but without defining a priority for its use. The document establishes recommendations to prepare strategies for the use of the cloud in each government entity, but without defining a priority for its use. Under Law No. 27658, known as the Framework Law for the Modernization of State Management, the different instances, agencies, entities, organizations, and procedures were declared to be in the process of renewal, with the purpose of improving public management through innovation in the country, in a decentralized manner and with greater citizen participation.

Under Legislative Decree No. 604, the National Informatics System was established with the purpose of developing activities related to the use of ICTs, in an integral manner, under specific regulations and with technical and management autonomy. In addition, it has as its scope of competence "the legal instrumentalization and technical mechanisms for the organization of computing resources and the state's informatics activity, as well as all associated

documentation; the operation and exploitation of data banks and magnetic information files at the service of public management. This development corresponds to the systematic planning of processes, methods and techniques supported by applied science and technology, which are established for the purpose of using, processing, and transporting information"<sup>63</sup>.

Currently, through Supreme Decree No. 022-2017-PCM, the Secretariat of Digital Government<sup>64</sup> - SeGDi, is appointed as the body with technical-normative authority at the national level, responsible for formulating and proposing national and sectoral policies, national plans, standards, guidelines, and strategies in the field of information technology and e-government. Under this decree, the SeGDi is the entity in charge of regulating cloud services.

The guidelines set forth by the SeGDi propose the adoption of Internet Protocol version 6<sup>65</sup> (IPv6)<sup>66</sup> to be included in the processes and contracts made with cloud service providers. Likewise, the minimum-security requirements to be taken into consideration are given:

- Having an information security policy, information security controls, risk management process, as indicated in R.M. N° 004-2016-PCM, in terms of organization, planning, support, operation and evaluation<sup>67</sup>.
- Observe the good practices guide indicated in the Security Directive<sup>68</sup> in the field of personal data protection.

<sup>62</sup> (Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros - SeGDi - PCM., 2018)

<sup>63</sup> Article 3 (Presidencia del Consejo de Ministros, 2018)

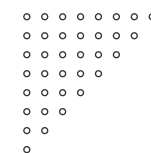
<sup>64</sup> (Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros - SeGDi - PCM., 2018)

<sup>65</sup> Internet protocols are a set of rules that determine how data is transmitted over the network. In response to the limited space that IPv4 has, IPv6 is an update of this protocol, designed to solve the problem of address exhaustion.

<sup>66</sup> (Presidencia del Consejo de Ministros, 2018)

<sup>67</sup> (Presidencia del Consejo de Ministros, 2016)

<sup>68</sup> (Autoridad Nacional de Protección de Datos Personales - Directiva de Seguridad de la Información, 2011)



- Have a Service Level Agreement - SLA<sup>69</sup> with the cloud service provider, in which the responsibilities of the public entity and the cloud service provider are clearly defined.
- At a minimum, require from the cloud service provider a widely recognized information security certificate based on international standards, which must be issued by an independent auditing organization, such as: Federal Risk and Authorization Management Program (FedRAMP)<sup>70</sup>, among others.

In addition, in terms of personal data protection for the use of cloud services, Law No. 29733, known as Personal Data Protection Law and discussed in the previous section, is taken as a reference. In this law, the safeguarding of data is guaranteed, according to the principle of purpose in which the cloud service provider must guarantee that it will not use the data for any other purpose that is not related to the contracted services.



- To have and apply personal data protection policies in line with the applicable principles and duties established by the Law and these regulations.
- Make visible the outsourcing involving the information on which the service is provided.

<sup>69</sup> In 2018, guidelines were published for the Subscription of a Service Level Agreement - SLA, in order to ensure the availability, capacity and scalability of the services used by all government entities. (Secretariat of Digital Government of the Presidency of the Council of Ministers - SeGDi, 2018).

<sup>70</sup> It provides a standardized approach for security assessment, authorization and continuous monitoring of cloud products and services. In the U.S., FedRAMP enables agencies to use modern cloud technologies, with an emphasis on security and protection of federal information, and helps accelerate the adoption of secure cloud solutions.

<sup>71</sup> Article 6, Constitución Política. (Presidencia de la República de los Estados Unidos Mexicanos, 2013)

<sup>72</sup> Article 52

<sup>73</sup> Article 63 & 64

<sup>74</sup> (Reglamento De La Ley Federal De Protección De Datos Personales En Posesión De Particulares, 2011)

### Mexico >>>>

In Mexico, the regulatory and legal framework for the use of cloud computing can be traced back to its own political constitution, in which the State "shall guarantee the population's integration into the information and knowledge society, through a universal digital inclusion policy with annual and six-year goals"<sup>71</sup>. This right consigned in the Mexican magna carta was decreed in 2013, after several modifications in telecommunications matters, which gave way to the creation of the Federal Telecommunications Institute (IFT), the regulatory entity of the sector.

As discussed in the previous chapter, the Federal Law for the Protection of Personal Data in Possession of Individuals<sup>72</sup>, guarantees privacy and self-determination of personal data; while the General Law for the Protection of Personal Data in Possession of Obligated Subjects<sup>73</sup>, regulates the processing of personal data. Particularly, it is important to highlight these considerations when using cloud services, in which it is contemplated<sup>74</sup>:

- Refrain from including conditions in the provision of the service that authorize or allow it to assume ownership or ownership of the information on which the service is provided.
- Keep confidentiality regarding the personal data on which the service is provided.
- To disclose changes in its privacy policies or conditions of the service it provides.
- Allow the responsible to limit the type of processing of personal data on which the service is provided.
- Establish and maintain adequate security measures for the protection of personal data on which the service is provided.
- Ensure the deletion of personal data once the service provided to the controller has been terminated and the controller has been able to retrieve it.
- Prevent access to personal data to persons who do not have access privileges, or in the event of a well-founded and reasoned request from a competent authority, inform the data controller of this fact.

Similarly, there are suggested minimum criteria for the contracting of cloud computing services involving the processing of personal data<sup>75</sup>, to guide those responsible for the processing of personal data in the selection and/or contracting of suppliers for

infrastructure services, platform, and software in the cloud, to comply with the obligations established in the regulations, avoiding any breach of the security of personal data.

## Chile

In Chile, during the last few years, the regulatory and legal framework of cloud-based services has been modified to strengthen personal data protection rights. In this way, the country has been advancing a series of adjustments since 2020 to Law 19.628, in force since 1999, on the protection of private life, to create a control body and regulate the consent and obligations of data controllers<sup>76</sup>. This law gives the right to demand from whoever is responsible for the data bank, information about the purpose of storage and to whom such information is transmitted, as well as to request its deletion, blocking or modification<sup>77</sup>. Law 19.223 is the basis for the classification of computer crimes, i.e., it establishes specific criminal offenses for unauthorized access, theft, and destruction of information systems<sup>78</sup>.

Under this context, the National Cybersecurity Policy 2017-2022 serves as the current normative and regulatory framework. Within this policy, it is important to highlight the efforts to update the current legislation, seeking homogenization with the international regulation based on the Budapest Convention, of which countries such as Peru and Colombia are also part of, with the purpose of providing a space for cybersecurity cooperation beyond their borders<sup>79</sup>.

<sup>75</sup> (Instituto Nacional de Transparencia y Protección de Datos Personales, 2018)

<sup>76</sup> (BID, 2020)

<sup>77</sup> (Ministerio Secretaría General de la Presidencia, 2020)

<sup>78</sup> (Ministerio de Justicia, 1993)

<sup>79</sup> (BID, 2020)

## Colombia

Law 19.799 regulates the electronic signature and signature certification services, establishing the different types of electronic signature, technological conditions, electronic documents, the way to manifest and give probative value, to consider the use of this type of signature by governmental entities<sup>80</sup>. Also, Law 19.880<sup>81</sup> provides guidelines for the contracting of services, in which cloud services are included by default.

Finally, Law 21.230, known as the Banking Modernization Law, grants the Financial Market Commission (CMF) the right to publicly disclose information subject to banking secrecy if the processing is anonymous. Given this transnational data processing, the CMF is the only entity that defines the specific regulation and prevents the localization of data outside the country. In addition, in 2017, Circular 3629 was enacted, which establishes minimum guidelines for the use of cloud services. It states that each banking entity must report annually on the risk tolerance it is willing to incur according to the cloud service it acquires (public, hybrid or private)<sup>82</sup>.

In the Colombian legislation for cloud services there are two regulatory mechanisms, the first, focused on the protection of personal data and the second, on the regulations related to the way to manage operational risks.

By means of Statutory Law 1581 of 2012 (discussed in the previous chapter), it is established that it is a fundamental right of individuals to request and obtain existing information about themselves and to request its deletion or correction if it is false or outdated. Likewise, it defines the categories of data, including sensitive data<sup>83</sup>, and prohibits its treatment, unless it is information of a public nature.

For its part, the Superintendence of Industry and Commerce in 2015, published a series of guidelines for the protection of personal data in cloud services. This guide proposes to organizations that want to acquire this type of services to analyze the risks<sup>84</sup> in each of the stages of the flow of information and that the provider complies with the regulations of data processing.

Law 1995 of 2019 establishes, in Article 147 of the National Development Plan (PND) 2018-2022, clearly the need to prioritize cloud services for the optimization of public resources and to advance in the

<sup>80</sup> (Ministerio de Economía, 2014)

<sup>81</sup> (Ministerio de la Secretaría General de la Presidencia, 2018)

<sup>82</sup> (Ministerio de Hacienda & Superintendencia de Bancos e Instituciones Financieras, 2017)

<sup>83</sup> Defined as those that may affect the privacy of the holder or whose improper use may generate discrimination (Congress of the Republic of Colombia, 2012).

<sup>84</sup> The associated risks identified by the SIC are the lack of control over the data and the lack of information on the processing and the conditions under which the service is provided.

digital transformation of the country, incorporating the emerging technologies of the Fourth Industrial Revolution<sup>85</sup>. It is important to note that the regulatory body for the ICT sector is the Communications Regulation Commission (CRC), in accordance with the Law for the Modernization of the ICT Sector<sup>86</sup>.

Similarly, progress has been made in sectoral issues such as in the financial system. In 2018 the Financial Superintendence of Colombia issued an external circular with the objective of facilitating cloud usage services in the sector. Three fundamental aspects for risk mitigation are derived from this circular and contractual responsibilities are established:

- 1 General obligations of the entities.
- 2 Service agreements or contracts.
- 3 Business continuity management.

This allows to give continuity to the outsourced processes in the cloud and to obtain access to the necessary information in case of audit or takeover by the supervisory bodies<sup>87</sup>.

<sup>85</sup> (García Zaballos, Iglesias Rodríguez, Puig Gabarró, & Campero, 2020)

<sup>86</sup> Ley N° 1975 de 2019 (Congreso de Colombia, 2019)

<sup>87</sup> (Asobancaria, 2018)

<sup>88, 89</sup> (Secretaría de Gobierno Digital Perú)

<sup>90</sup> (PQS, 2020)

<sup>91</sup> (DCD, 2020)

<sup>92</sup> (ITU, 2018)



## 2.2. CURRENT PUBLIC POLICIES: DIGITAL TRANSFORMATION STRATEGY >>>>

### Peru >>>>

The Digital Government Secretariat of the Presidency of the Council of Ministers leads the processes of technological innovation and digital transformation of the State. It is the governing body of the National Digital Transformation System and manages the digital platforms of the Peruvian State<sup>88</sup>. With this intention, there is the Digital Government Law, approved by Legislative Decree No. 1412, which establishes the framework for the proper management of digital identity, services, architecture, and security, as well as interoperability and data<sup>89</sup>. In Latin America, according to IDC (International Data Corporation), the cloud solutions market has a growth rate of 27% and by 2022, 70% of companies would integrate cloud management (through their public and private clouds) by implementing unified management of technologies, tools and processes<sup>90</sup>. Like several Latin American countries, the Peruvian government has decided to incorporate cloud services as part of its digital strategy. Peru seeks to invest 20% more in the use of cloud services than in previous years<sup>91</sup>.

The government seeks to facilitate procedures and accelerate the adoption of technology by citizens. For example, since 2012, the Law for the Promotion of Broadband and Construction of the Optical Fiber Backbone Network has been in force, whose purpose is to strengthen access and adoption of connectivity by the population<sup>92</sup>.

In 2020, the National Telehealth Plan was approved, with the objective of improving the population's access to health services in Peru using technologies, mainly in rural areas. In this way, it seeks to promote strengthening, improving the capacities of health personnel, equipment, and technological infrastructure. Likewise, financial mechanisms are established to contribute to their sustainability and initiatives that facilitate the implementation of the telehealth axes: telemedicine, tele management, tele training, tele information, education, and communication<sup>93</sup>.

As part of the country's transformation process (within the framework of the Law), the Peruvian Air Force (FAP) is the first Peruvian public sector institution to implement a Private Cloud model, with its main data center. This project works through the acquisition and implementation of an engineering system called Oracle Private Cloud Appliance (PCA)<sup>94</sup>.

From the Covid-19 juncture, the use of cloud services increased, with a rise of more than 25%<sup>95</sup> during the quarantine; considering that 68% of small and medium-sized companies had already acquired these services in 2019.

Several private initiatives emerged around the health and economic crisis:

- » Amazon Web Services has included pandemic response in its resiliency planning, and regularly scales to handle spikes in demand, such as black Friday. Pandemic response policies and procedures have been incorporated into disaster

<sup>93</sup> (Ministerio de Salud, 2020)

<sup>94</sup> (Oracle, 2020)

<sup>95</sup> El Comercio Perú, 2020)

<sup>96,97</sup> (CIO Perú)

<sup>98</sup> (Gobierno de México)

<sup>99</sup> (Gobierno de la República Mexicana, 2013)

recovery planning. Measures have been taken to ensure ample capacity and service continuity<sup>96</sup>.

- » Google Cloud formed an internal working group to plan for and mitigate business impacts resulting from Covid-19. The company expressed confidence that its systems can continue to support customers during this time<sup>97</sup>.

### Mexico >>>>

Mexico has the Undersecretariat of Communications and Technological Development, whose mission is to design and coordinate the strategy of public policies aimed at promoting technological and cognitive enablers in telecommunications and broadcasting. It favors inclusion, social development, and competitiveness of the country, especially in vulnerable populations and MSMEs<sup>98</sup>.

The digital transformation in this country is part of a digitalization strategy for economic, social, and political development, or National Digital Strategy. Understanding digitalization as the capacity of the country and its population to use digital technologies to generate, process and share information; likewise, it is related to the concept that describes the social, economic, and political transformations associated with the massive adoption of ICTs<sup>99</sup>. Therefore, the



Mexican government seeks to increase by 25%<sup>100</sup> its investment in cloud services in the coming years. In February 2020, Microsoft announced a \$1.1 billion investment plan to drive digital transformation in the country, including its first cloud data center region in Mexico<sup>101</sup>.

Mexico has content distribution centers and data centers connected to backbone networks and IXPs with broadband to ensure the necessary infrastructure to access cloud services<sup>102</sup>. In this country, data centers occupy an area of more than 250,000 square meters, distributed in 49 locations in six states<sup>103</sup>, making the country the second largest data center market in Latin America, after Brazil.

According to Veritas' Truth in Cloud study, of the 91% of organizations that use some cloud service, 50% use hybrid schemes: they have a part in the cloud and another in their own infrastructure<sup>104</sup>. In the case of Mexico, 52% of those surveyed in the country described their infrastructure as half in-house and half in the cloud. Of the companies, 31% have most of their information in the cloud and 8% are under an "all in cloud" scheme. In addition, 25% are interested in working under this model.

Both the Mexican government and the private sector seek to increase the use of cloud services by companies and users. This is how the National Electoral Institute

(INE) used cloud services for the elections of deputies, senators and governors that took place in 2018. The PREP (system that provides the preliminary results of the elections, based on the tally sheets), thanks to the solutions provided, managed to diversify the storage and processing of data in different "microservices", allowing to block the thousands of attacks days before the elections, supporting more than two million users on its website during voting<sup>105</sup>.

On the other hand, the Tax Administration Service (SAT)<sup>106</sup> created the SENHA project (managed hybrid cloud services) in 2017, to perform the migration to the hybrid cloud. For this it made use of IaaS and PaaS, which allowed to ensure efficiency, according to the needs of taxpayers, exercising better control, through migration, enablement, implementation, testing, stabilization and operation of SAT applications<sup>107</sup>.

With the Covid-19 situation, around 1.8 million Mexicans lost their jobs<sup>108</sup>. Companies that have taken advantage of cloud services have been less impacted by the disruption of operations in different sectors caused by the health and economic emergency<sup>109</sup>. About 28% of the total budget of technology companies is dedicated to cloud-based services, while 45% is allocated to SaaS, 30% to IaaS and 19% to PaaS.

<sup>100</sup> (Thompson Reuters, 2020)

<sup>101</sup> (Microsoft, 2020)

<sup>102</sup> (Gobierno de la República Mexicana, 2013)

<sup>103</sup> (IFT, 2020)

<sup>104</sup> (Cascada Insights, 2019)

<sup>105</sup> (TicTac, 2020)

<sup>106</sup> Mexican Tax Authority

<sup>107</sup> (TicTac, 2020)

<sup>108</sup> (Forbes, 2020)

<sup>109</sup> (El Economista, 2020)

## Chile

The main guide of the digital transformation strategy is the Digital Government Division Chile (DGD), which is part of the Ministry General Secretariat of the Presidency (SEGPRES). The DGD's mission is to coordinate and advise intersectoral to the organs of the State administration in the strategic use of digital technologies, supporting their use, data, and public information to improve management and the delivery of close and quality services to people. This, through technology, standards, and digital adoption<sup>110</sup>.

In 2018, the State administration issued a manual of good practices for the use of cloud services<sup>111</sup>, where some relevant concepts are clarified and characteristics and considerations to consider when using these services are shown. In line with this policy, in November 2019, Law No. 21180 on Digital Transformation of the State was published where<sup>112</sup>:

1 The completion of administrative procedures through electronic means is promoted.

2 Documents and signatures are handled electronically.

<sup>110</sup> (Gobierno Digital Chile)

<sup>111</sup> (División de Gobierno Digital Chile, 2018)

<sup>112</sup> (Gobierno Digital Chile, 2019)

<sup>113</sup> It is expected that by 2021 all the regulations will be ready, once published they will be in force after 180 days (Gobierno Digital Chile, 2019)

<sup>114</sup> (PwC, 2020)

<sup>115</sup> (DF SUPLEMENTOS, 2020)

<sup>116</sup> (Talento Digital Chile, 2020)

<sup>117</sup> Corporación de Fomento de la Producción Chile

<sup>118</sup> (Microsoft, 2020)

3 The old system of notification by registered letter is changed to a system of unique digital addresses, which will be composed by the e-mail addresses provided by the interested parties in a procedure and whose registry will be kept by the Civil Registry and Identification Service, according to a regulation to be issued in the future<sup>113</sup>.

Half of all government IT spending is going to the cloud, reaching 60% of all IT infrastructure and all software, services, and technology spending by 2020. As a result of the pandemic, 30% of companies have defined to have a cloud first strategy, that is, they think their technology strategy in cloud mode, in the first instance<sup>114</sup>. From now on, there is a need to accelerate digital initiatives; it is expected that in 2021 more than 70% of companies migrate their services to the cloud<sup>115</sup>.

In Chile has been implemented a commitment to the training of ICT talent to facilitate the adoption of tools such as the cloud. For this purpose, there is "*Talento Digital Chile*"<sup>116</sup> which integrates companies, training institutions and government to develop new skills in people, according to the demands of the digital economy. This project is developed with Fundación Chile and CORFO<sup>117</sup>, bringing together training institutions and government officials, to train from 2020 and within five years, about 10,000 people in ICT skills.

Similarly, to accelerate the digital transformation of companies, Microsoft is leading the "*Transforma Chile*"<sup>118</sup> initiative. Through this project, there will be a data center region and it is expected that by 2025 there will be more than 180,000 people trained in digital skills, thus joining the initiative of the Chilean government.



# Colombia

The entity in charge of the design and development of the digital transformation strategy in the country is the Ministry of Information and Communication Technologies (MinTIC). The Digital Transformation Directorate of MinTIC is responsible for<sup>119</sup>:

- 1 Defining the degree of digitalization of the different sectors and developing strategies for each one.
- 2 Promoting e-commerce.
- 3 Promote the use of ICTs in the productive processes of MSMEs and their associated value chain.
- 4 Support and manage research related to cognitive computing, internet of things, data analytics, artificial intelligence, robotics, among others.

There is Law 1978 of 2019<sup>120</sup> that highlights the use of ICTs to generate conditions to promote legal certainty and investment in the sector in Colombia. For example, the award of electromagnetic spectrum with 20-year licenses, allows telecommunications operators to have the confidence to improve the deployment of new networks in the country<sup>121</sup> and the promotion of the software and cloud computing industry.

It is worth clarifying that, to guarantee the efficiency of the public procurement system in Colombia, there is "Colombia Compra Eficiente", a decentralized entity attached to the National Planning Department (DNP). Its objective is to be an innovation platform for demand-supply interaction and to promote the development of innovative goods and services. It is a fundamental tool for strengthening innovative companies, through the demand for products and services focused on providing solutions to strategic government projects. This entity uses Price Framework Agreements (PFA) to coordinate and manage the processes.

Through the third generation of AMP public and private cloud, the general conditions for the contracting and provision of cloud services between 2019 and 2021<sup>122</sup> are established. For the case of private cloud, services must be provided by data centers accredited by Colombia Compra Eficiente (CCE) in three levels of availability. When it comes to public cloud services, purchasing entities will be able to acquire the totality of public cloud services from providers such as Amazon Web Services, Google Cloud, Microsoft Azure and Oracle Cloud.

The Colombian government is working to optimize the management of public resources in ICT projects using ICT demand aggregation instruments with the inclusion of new technologies and technology service delivery models in the public procurement system, and the prioritization of cloud services<sup>123</sup>. This is evidenced in the National Policy CONPES for Digital Transformation and Artificial Intelligence of November 2019.

<sup>119</sup> (MinTIC Colombia, 2020)

<sup>120</sup> (Ley 1978 de 2019)

<sup>121</sup> (TicTac, 2020)

<sup>122</sup> (CCE, 2019)

<sup>123</sup> (CONPES, 2019)

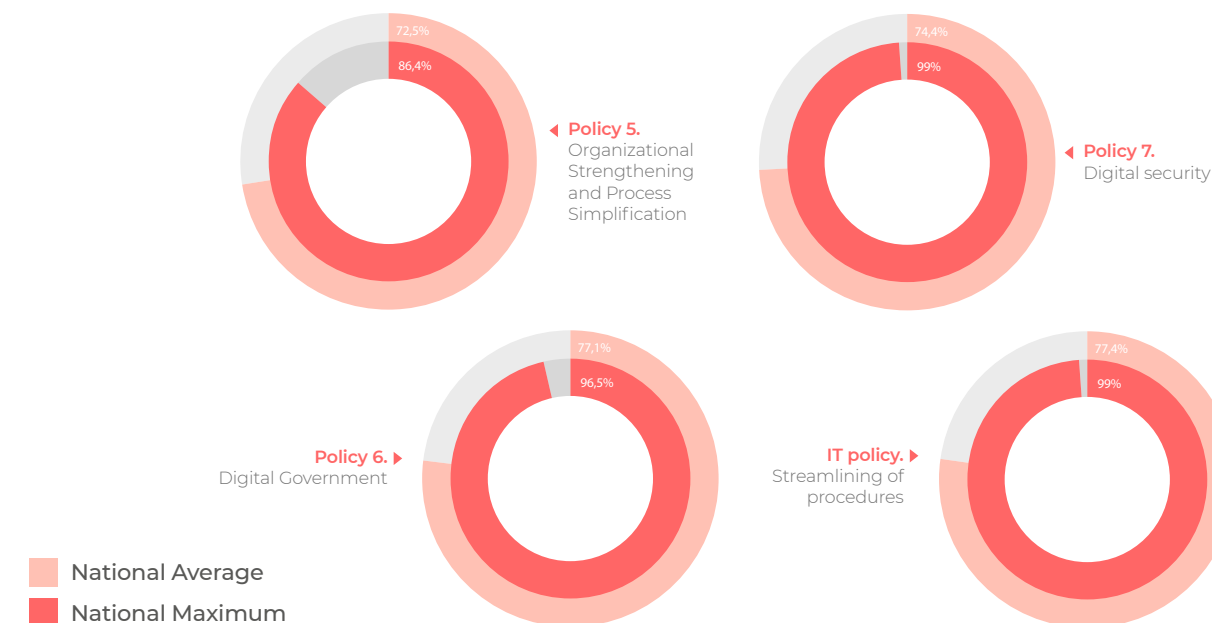


Figure 5: Performance in policies for digital transformation. Source: (TicTac, 2020)

Colombia is a reference country in the region when talking about companies that take advantage of data<sup>124</sup>, largely due to the flexibility of the cloud. This not only allows companies to have access to cutting-edge technology in real time but can also help them as they begin the process of digital change, with small prototypes during the process in which they must join new users for their modular growth<sup>125</sup>.

In the wake of the pandemic, the telework drive has played a key role in economic revival. Several companies have been able to continue operating thanks to the possibility of their workers performing their tasks remotely. The Colombian government, through the MinTIC<sup>126</sup>, has carried out promotional campaigns, supporting telework and cloud computing.

Virtual forums have been held<sup>127</sup> and, together with the Ministry of Labor, a roadmap for the adoption of the Public Policy for the Promotion of Telework has been underway since 2018<sup>128</sup>.

In conclusion, for the countries of the Pacific Alliance, telework and e-commerce are key in the digital transformation process. In the short term, there is a strong demand for the continuity of managed services, collaboration tools for teleworking and information security. With the digital transformation, there is a demand more focused on technological infrastructure for e-commerce, telehealth and fintechgration<sup>129</sup>, looking for robust and secure solutions for remote work and the adoption of a digital economy.

<sup>124</sup>, <sup>125</sup> (La República, 2020)

<sup>126</sup>, <sup>127</sup> (MinTIC, 2020)

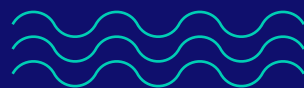
<sup>128</sup> (Ministerio del Trabajo, 2019)

<sup>129</sup> Term that refers to the use of technology in the financial system.



03

Broadband



Internet access has become an essential service. Many sectors have been able to continue their activities thanks to the connection facilities. On the other hand, the lack of this service has had a negative impact on the vulnerable population.

One of the most relevant aspects when considering the development of regulatory frameworks and the formulation of public policy regarding broadband in Latin America is the radioelectric spectrum. According to the Inter-American Development Bank (IDB) and the Organization for Economic Cooperation and Development (OECD), its importance lies in the low access to broadband in fixed networks, which have traditionally been much less developed in the region than in other parts of the world.



### 3.1. LEGAL AND REGULATORY FRAMEWORKS

In recent years, the Pacific Alliance countries have established a regulatory and legislative framework for broadband in each of their territories within their general telecommunications law. The government has sought to strengthen good practices that simplify rules and procedures and the technological neutrality with which they are applied to all devices. These actions are essential to enable the convergence of communications services and guarantee the independence between regulatory and policy-making bodies to encourage and ensure competition.

Governments have made efforts to adopt a comprehensive approach that includes regulatory improvement actions and policies to encourage infrastructure deployment, improve access and connectivity, as well as broadband adoption and use.

In this way, the legal and regulatory framework has focused on aligning all market participants' incentives to achieve significant progress in broadband. Establishing realistic short-, medium- and long-term objectives and goals, which have placed importance on mechanisms and agencies to be reviewed and updated periodically.

## Peru

Law No. 29904 or Broadband Promotion and Network Construction Law is the main normative and regulatory framework in the country<sup>130</sup>. It aims to stimulate the development, use and massification of broadband throughout the national territory, both in supply and demand, promoting the deployment of infrastructure, services, content, applications, and digital skills<sup>131</sup>. In addition, it establishes broadband as a public need and of national interest, giving free way for the construction of a National Backbone Fiber Optic Network<sup>132</sup>, which integrates all the provincial capitals of the country and the deployment of high-capacity networks in all districts. This, to enable broadband connectivity, both fixed and mobile, and its massification throughout the national territory, under competitive conditions. It also guarantees access and use of infrastructure associated with the provision of public utilities of electricity and hydrocarbons. As well as the use of the right of way of the National Road Network, with the purpose of facilitating the deployment of telecommunications networks necessary for the provision of fixed or mobile broadband<sup>133</sup>.

The law makes an important advance in the strengthening of science, technology, and innovation by grouping all public universities and research institutes to the National Research and Education Network, in order to integrate to regional and global networks in search of the acceleration of R+D+i processes.

Likewise, it grants the formulation of broadband public policies to the Ministry of Transportation and Communications through the Vice Ministry of Communications and the formulation of public policies regarding Electronic Government to the Office of Electronic Government and Informatics. Likewise, the Supervisory Body of Private Investment in Telecommunications (OSIPTEL) is appointed to determine and periodically update other technical characteristics of broadband Internet connections.

## Mexico

As mentioned in previous chapters, in 2013 there was a constitutional reform throughout Mexico that establishes the right to ICTs and to broadcasting and telecommunication services, including broadband and internet<sup>134</sup>. This constitutional reform gave basis to the Federal Law of Telecommunications and Broadcasting of 2014<sup>135</sup>. In 2020, it underwent some modifications with the objective of regulating the use, exploitation and exploitation of the radio electric spectrum, telecommunications networks, access to passive and active infrastructure and the provision of telecommunications-related services.

The amendment included the consideration of broadband internet access as a constitutional obligation and the legality of foreign investment. Likewise, it specifies the role of the national authorities in this

<sup>130</sup> (Ley 29904 de 2013)

<sup>131</sup> It includes provisions on digital literacy, the need to implement public access centers with broadband connections (Congress of the Republic of Peru, 2020).

<sup>132</sup> Design, deployment and operation of a fiber optic network.

<sup>133</sup> Article 9. Ley 29904. Ley de promoción de Banda Ancha y construcción de la Red Dorsal de Fibras Ópticas

<sup>134</sup> Article VI, XIV, XVI, XVII (Constitución Política de los Estados Unidos Mexicanos, 2013)

<sup>135</sup> (Ley Federal de Telecomunicaciones y Radiodifusión, 2020)

instance, defining the Federal Telecommunications Institute (IFT)<sup>136</sup> as the body in charge of the efficient development of broadcasting and telecommunications intervening in electromagnetic spectrum issues, networks, and the provision of related services, as well as guaranteeing equal access to infrastructure and other essential inputs for these services to citizens.

the contracted plan. It is important to mention that the regulation especially protects the user, since the operator will always be obliged to prove that the measurements made by the user are not correct.



## Chile

The general regulatory framework for telecommunications in the Chilean territory is Law 18168 of 1982<sup>137</sup>, which underwent several modifications in 2017, with Law 21046<sup>138</sup>. It defined the figure of Internet access providers, essential to set the service quality levels of internet access, understood under the denomination of broadband. By means of Decree 150 and Resolution 1498 of 2020<sup>139</sup>, the organization and operation is established, setting forth the regulations governing commercial offers and broadband service delivery. In other words, it establishes a system for measuring Internet quality speed, as well as the creation of the Independent Technical Body to guarantee quality and obtain statistical information.

In addition, the regulation provides a compensation system for users in case of non-compliance by Internet operators, by allowing discounts and adjustments to

## Colombia

Law 1978 of 2019<sup>140</sup>, better known as the Law of Modernization of the ICT Sector seeks to facilitate the deployment of high-cost infrastructure, so that investment in connectivity of the vulnerable population can be focused generating equity. Likewise, that same year the CRC provided a new definition regarding the minimum broadband levels (speeds of 25 Mbps downstream and 5 Mbps upstream)<sup>141</sup>. Operators may offer internet services with lower speeds; however, they are not called broadband.

This law establishes that all telecommunications network and service providers will have equal opportunities to access the use of the spectrum and will contribute to the Single Fund for Information and Communication Technologies<sup>142</sup>. The allocation of the spectrum seeks the maximization of social welfare, the certainty of the investment conditions and the resources to promote digital inclusion must be contemplated.

<sup>136</sup> (IFT, 2020)  
<sup>137</sup> (Ley 18168 de 1982)  
<sup>138</sup> (Ministerio de Transporte y Telecomunicaciones de Chile, 2017)  
<sup>139</sup> (Subtel, 2020)  
<sup>140</sup> (Ley 1978 de 2019)  
<sup>141</sup> (CRC, 2019)  
<sup>142</sup> Article 4



## 3.2. CURRENT PUBLIC POLICIES



Broadband is the maximum speed at which traffic can flow. Governments have committed to guaranteeing connectivity through policies that promote investment in infrastructure and electromagnetic spectrum. The Inter-American Development Bank (IDB) and the OECD propose policies to promote the expansion of broadband networks and services in the region from an intersectoral approach<sup>143</sup>.

- 1 The need for a stable regulatory framework to promote investment in broadband infrastructure through whole-of-government approaches.
- 2 Promotion of competition to discipline prices.
- 3 Giving accessibility to disadvantaged sectors, rural and remote areas, as well as avoiding fiscal disincentives for all of them.
- 4 Promote regional cooperation agreements and exchanges of regulatory experiences, deployment of regional infrastructures, data flows and reduction of prices for international connectivity and roaming.
- 5 Introduce broadband in institutions and companies, as well as greater transparency on the part of governments.
- 6 Promote the digitalization of governments.
- 7 Strengthen trust in digital services, with the articulation of existing policies and regulatory frameworks for consumer protection, digital security risk management and privacy protection.

<sup>143</sup> (IDB - OECD, 2016)



## Peru

It seeks to define the role of the State in the implementation of the National Dorsal Fiber Optic Network, its conformation, operation, management, and equipment. This based on the broadband service understood as permanent and high speed, which allows the flow of multimedia information, in addition to the appropriate use of digital services and applications<sup>144</sup>. It also specifies the efficient use of the infrastructure deployed and public resources, access, relevant procedures, obligations, and provision of Internet services.

Similarly, there is the Supervisory Agency for Private Investment in Telecommunications (OSIPTEL) which, as its name suggests, is responsible for overseeing telecommunications services in the country. OSIPTEL defines broadband as a permanent internet connection, at speeds that allow obtaining and providing multimedia information<sup>145</sup>; and through this entity, users can verify their broadband speed and demand clarity in the information provided.

With the purpose of massifying and developing broadband in Peru, the Ministry of Transport and Communications (MTC) issued ministerial resolution 810-2019-MTC/01.03 from September 2019. This resolution redefined the concept of regional networks to provide the service, and proposed the National Backbone Fiber Optic Network to provide

international connectivity services<sup>146</sup>, determined an update with a periodicity of no more than two years, the minimum speed for broadband Internet access. With all these measures, telecommunications investments in Peru grew 172% between 2000 and 2019, reaching 4.53 billion soles (US\$1.28 billion)<sup>147</sup> before the pandemic.

As of March 2020<sup>148</sup>, OSIPTEL asked internet providers to increase the minimum speed to facilitate teleworking and remote work activities. This gave rise to bill 5398 of 2020<sup>149</sup>, which seeks to guarantee optimal access to broadband internet access service users, as well as to reduce the asymmetry of information in the consumption decision of such users. In May of the same year, a modification of the Law for the Promotion of Broadband and Construction of the National Backbone Fiber Optic Network was made. This, with the purpose that the service providers of this type respect the threshold that can be called broadband according to the Peruvian Law.

Currently, broadband internet access providers guarantee 90% of the speeds offered in their advertising and in contracts with users, and this is clearly stated in the contracts. The Peruvian government expects telecommunications operators to resume their investments in 2021, according to the MTC<sup>150</sup>.

<sup>144</sup> (Ley 29904. Ley de promoción de Banda Ancha y construcción de la Red Dorsal de Fibra Óptica., 2020)

<sup>145</sup> (IFT, 2017)

<sup>146</sup> (Gobierno de Perú, 2019)

<sup>147</sup> (Bnamericas, 2020)

<sup>148</sup> (Gestión Económica Perú, 2020)

<sup>149</sup> (Gobierno de Perú, 2020)

<sup>150</sup> (Bnamericas, 2020)



## Mexico

On the other hand, the assignment of the radio spectrum is granted by applying the procedure established in the Sole Text of Administrative Procedures of the Ministry of Transport and Communications (TUPA). In May 2020, AMÉRICA MÓVIL PERÚ S.A.C. was authorized the temporary assignment of radio electric spectrum in the 2500-2690 MHz and 3400-3600 MHz frequency bands in several provinces of the country in the framework of the nationwide sanitary emergency declared due to the existence of COVID-19<sup>151</sup>.

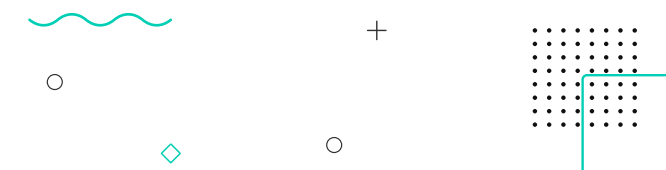
According to the Federal Telecommunications Institute (IFT), investment in telecommunications infrastructure grew 23% during 2019 in Mexico<sup>152</sup>. Operators invested 71.1 billion Mexican pesos (US\$3.28 billion) in infrastructure in 2019. Also, considering investment in non-tangible assets, total investment amounted to 113.4 million pesos (US\$6 million), or 46.7% more than what was invested in 2018<sup>153</sup>. In the last quarter of 2019, the GDP of the telecommunications and broadcasting sectors was Ps. 592 billion, with an annual growth rate of 7.5%; while the national GDP decreased 0.5%<sup>154</sup>.

Since 2015, an Annual Program for the Use and Exploitation of Frequency Bands is issued, through which the frequencies of determined spectrum subject to bidding, terms and conditions of use and provision of services are made known.

In 2018<sup>155</sup>, a broadband program was created to establish the sites to be connected each year, to develop a strategy to connect research, health, education and government institutions with points of presence of the Red Nacional de Impulso a la Banda Ancha (Red NIBA); this, in order to democratize access to these services. Thanks to these measures, Mexico was the fourth country with the highest growth in fixed broadband penetration from June 2013 to June 2019, with 49.0%; only below Portugal (60.2%), Turkey (57.4%) and Colombia (49.9%), according to the OECD<sup>156</sup>.

Between 2013 and 2019, fixed broadband subscriptions via fiber optic had a growth of 18.6%<sup>157</sup>. Currently, Mexico is the country with the highest growth in mobile broadband density, going from 23 to 74 lines per 100 inhabitants, representing a growth of 215.7%<sup>158</sup>.

As of December 2019, fixed internet service accesses via fiber optic were 4.7 million, representing an annual growth of 27.6% with respect to accesses registered in the previous year<sup>159</sup>. In the same period, mobile Internet access lines reached 97.4 million, representing an annual increase of 10.4%<sup>160</sup>. However, the growth in data consumption and in the number of connected devices will require future networks to have 20 times more capacity than they have today<sup>161</sup>.



<sup>151</sup> (Ministerio de Transporte y Telecomunicaciones del Perú, 2020)

<sup>152</sup>, <sup>153</sup>, <sup>154</sup> (IFT, 2020)

<sup>155</sup> (SCT - IFT)

<sup>156</sup>, <sup>157</sup>, <sup>158</sup> (Forbes México, 2020)

<sup>159</sup>, <sup>160</sup> (IFT, 2020)

<sup>161</sup>, <sup>162</sup> (GSMA, 2018)

The contribution of the mobile ecosystem to Mexican GDP increased from 3.5% in 2015 to 3.8% in 2020<sup>162</sup>. However, investment in telecommunications infrastructure was reduced because of the pandemic. Televisa, América Móvil and Axtel presented drops of up to 19% in investment, when a year earlier, at this same time, Capex grew more than 5.0% generalized in the industry compared to the 2018 figure<sup>163</sup>.

## Chile

In Chile, the entity responsible for the telecommunications sector is the Undersecretary of Telecommunications (SUBTEL). This entity considers broadband service as a permanent connection from a user to a service provider, to support a bidirectional transmission<sup>164</sup>. SUBTEL regulates the telecommunications market and obliges service providers to comply with their advertised speeds.

Currently, there is law 21.046 of 2015 to regulate minimum broadband speeds<sup>165</sup>. According to this law<sup>166</sup>, it is established that Internet access providers must comply with the service quality levels established by the provisions issued for this purpose by the Ministry of Transport and Telecommunications. Said regulation talks about the methodology and periodicity of measurements, minimum values and other technical characteristics that allow commercializing broadband Internet access services.

Since 2017, pilot projects have been promoted to implement Community Broadband. In this way, municipalities can bid and own physical infrastructure to provide data services<sup>167</sup>. There are ChileGob WiFi points, a project that helps to improve access in the most vulnerable places in Chile that have few connectivity alternatives<sup>168</sup>.

In terms of investment in telecommunications, Subtel earmarked around 86 billion Chilean pesos (approximately US\$ 112 million) in 2020 to reduce the digital divide, which will be distributed in the implementation of projects in six macro-areas throughout the country. In terms of electromagnetic spectrum, in November 2020 Chile held the first Latin American auction of specific frequencies for 5G<sup>169</sup>.

In July 2020, the General Comptroller of the Republic of Chile turned to the Minimum Guaranteed Internet Access Speed Law<sup>170</sup>, to implement a quality measurement system so that the speed contracted by users is close to the real speed they receive on their devices. In this way, one of the main problems of Internet users, who have complained about not receiving the speed contracted in the commercial promise, will be solved. This will be achieved through official and clear measurements of both fixed and mobile connections, which can later be used to complain to SUBTEL in case the promised speed is not being met.



<sup>163</sup> (El Economista, 2020)  
<sup>164</sup> (IFT, 2017)  
<sup>165</sup> (Ley Chile)  
<sup>166</sup> (IFT, 2017)  
<sup>167</sup> (Subtel Chile, 2017)  
<sup>168</sup> (WiFiChileGob)  
<sup>169</sup> (Bnamericas, 2020)  
<sup>170</sup> (SUBTEL, 2020)

## Colombia

The entity in charge of public policy formulation is the Ministry of Information and Communications Technologies (MinTIC) and the Communications Regulation Commission (CRC) is the regulatory body. Operators may offer broadband in the regions and municipalities where they can provide the service, in case of selling this type of plans in regions without coverage or with limited coverage, they will be incurring in misleading advertising and may be denounced before the SIC. The Superintendence of Industry and Commerce (SIC) is the entity in charge of verifying that operators comply with this new definition, the function of the CRC is to establish the rules that govern the relationship between the operator and the users, however, it is the SIC the one in charge of monitoring and controlling compliance with these<sup>171</sup>.

As of January 2019, Colombia has a new definition of broadband. With minimum speeds of 25 Mbps downstream (download) and 5Mbps upstream (upload)<sup>172</sup>. Complying with the guidelines of Law 1978 of 2019, the national government put into effect the investment agenda of the Single Fund for Information Technology and Communications (FUTIC) from 2021<sup>173</sup>.

With this broadband redefinition, the CRC encouraged an increase in fixed Internet speeds and the percentage of broadband connections in the country. The results of

Resolution CRC 5161 of 2017 were analyzed, where the speeds categorized as broadband (25 Mbps downstream and 5 Mbps upstream) were redefined and a definition was given for ultra-broadband speeds (50 Mbps downstream and 20 Mbps upstream) for fixed Internet connections, with which it was also possible to identify the impacts of Law 1753 of 2015 in this matter. The municipalities were classified according to the difficulty or ease of access. As a general conclusion, positive effects were obtained in the trends of average upload speed, download speed and percentage to broadband connections for the three groups.

On the other hand, to massify broadband internet access and reduce the digital divide, in 2020 the Colombian Government developed a subsidy scheme for internet in strata 1 and 2<sup>174</sup>. It seeks the adoption of mechanisms aimed at the massification of social internet plans for users of these socioeconomic strata.

Finally, in December 2020, the spectrum public policy was issued to be in force between 2020 and 2024, where strategies for internal adaptation of the functions and responsibilities of the MinTIC and the ANE have been proposed in terms of emphasis on radio and television services, modernization of spectrum management processes and regulation of unauthorized operations of the radio electric spectrum.

<sup>171</sup>, <sup>172</sup> (CRC, 2019)  
<sup>173</sup>, <sup>174</sup> (MinTIC, 2020)



# 04

Cybersecurity





Of the total population of South America<sup>175</sup>, 72% use the Internet<sup>176</sup>, while in North America, this indicator rises to 90%<sup>177</sup>. The expansion of technology and, more urgently, the COVID-19 pandemic have provided an opportunity to reflect the progress of ICT, connectivity, and cybersecurity in the region. By the close of Q1 2020, the global cybersecurity market grew by 9.7%; COVID-19 largely drove a figure. Total investment reached \$10.4 billion<sup>178</sup>. The concern and uncertainty derived from quarantine and isolation and companies' need to generate new work environments from virtuality were the perfect excuses for cybercriminals. Therefore, constant access to cyberspace makes it necessary to retake the lessons learned to address society's digital transformation with confidence, ensuring cybersecurity in everyday environments.



#### 4.1. LEGAL AND REGULATORY FRAMEWORKS >>>>

### Peru >>>>

In Peru, the regulatory framework is provided by the provisions analyzed in previous chapters, with each initiative providing a cross-cutting reference for the construction of its cybersecurity policy. For example, Laws 29733 (Protection of Personal Data), 29904

(Promotion of Broadband and Construction of the National Backbone Fiber Optic Network), and 27658 (Framework Law for the Modernization of State Management)<sup>179</sup>.

Likewise, there are Law 30618 of 2017 and Supreme Decree 106-2017-PCM that approve the Regulation for the Identification, Evaluation and Risk Management of National Critical Assets (ACN)<sup>180</sup>, this regulates digital security and gives functions to the National Intelligence Directorate (DINI), among which are the establishment of regulations to ensure digital security and the promotion of international cooperation for these objectives<sup>181</sup>.

<sup>175</sup> The total population in South America is approximately 427.7 million inhabitants. (Statista, 2021)

<sup>176</sup> (Hootsuite, We are Social, 2021)

<sup>177</sup> The total population of North America is approximately 579 million.

<sup>178</sup> (TicTac, 2020)

<sup>179</sup> Discussed in the chapters on privacy and broadband respectively.

<sup>180</sup> (Decreto Supremo - N° 106-2017-PCM)

<sup>181</sup> (Ley N° 30618)



Regarding the management of digital services, since 2018 through Legislative Decree 1412, the Digital Government Law is approved whose purpose is to establish the governance framework of digital government for the proper management of digital identity, digital services, digital architecture, interoperability, digital security, and data. As well as the legal regime applicable to the transversal use of digital technologies in the digitization of processes and provision of digital services by the entities of the Public Administration at the three levels of government<sup>182</sup>. In other words, the digital security framework is articulated with information security, the latter being the basis for the former<sup>183</sup>. Likewise, the following areas and entities in charge are established<sup>184</sup>:



**Defense:** The Ministry of Defense in the framework of its functions and competences directs, supervises, and evaluates the rules on cyber defense.



**Intelligence:** The DNI technical regulatory authority within the framework of its function's issues, supervises and evaluates the norms in the field of intelligence, counterintelligence, and digital security.



**Justice:** The Ministry of Justice and Human Rights, the Ministry of the Interior, the Peruvian National Police, the Public Prosecutor's Office, and the Judiciary, within the framework of their functions and competencies, direct, supervise and evaluate regulations on cybercrime.



**Institutional:** Public Administration entities must establish, maintain, and document an Information Security Management System (ISMS).

As evidenced by the cybersecurity 2020 report of the Organization of American States (OAS) and the Inter-American Development Bank (IDB)<sup>185</sup>, the Peruvian regulatory and legal framework has had certain developments and advances in recent years (Figure 5). For example, in terms of data protection and child protection, these are the areas where the country

has improved significantly in the last five years, showing a consolidated state. However, relevant aspects regarding consumer protection legislation, intellectual property, the criminal justice system and cooperation frameworks are still in a formative stage, which means that there is still a lack of organization and better definition of each of them.

<sup>182</sup> (Decreto Legislativo N° 1412)

<sup>183</sup> Article 30 (Decreto Legislativo N° 1412)

<sup>184</sup> Article 32 (Decreto Legislativo N° 1412)

<sup>185</sup> (BID, 2020)







Figure 6: Regulatory and legal frameworks for cybersecurity in Peru 2020 (IDB, 2020).

## Mexico

Mexico does not have a general cybersecurity law, however, since 2020 a discussion to promote it in the Senate has been advancing<sup>186</sup>. Even so, according to the Federal Telecommunications and Broadcasting Law of 2014, powers were granted to the Federal Telecommunications Institute (IFT), the entity in charge of regulating and supervising networks and the provision of telecommunications and broadcasting services in Mexico. In the same line, the IFT has pointed out the importance of developing a security regulatory framework for devices, infrastructure, and networks<sup>187</sup>.

Through the Federal Law for the Protection of Data in Possession of Individuals of 2010, it is established that those responsible for the processing of personal data must have administrative, technical, and physical security measures to protect the data against damage, loss, alteration, destruction or unauthorized use, access, or processing<sup>188</sup>. Likewise, the General Law for the Protection of Personal Data in Possession of Obligated Subjects of 2017, establishes taking high-level security measures, this includes administrative, physical and technical measures to ensure integrity, availability, confidentiality and protection<sup>189</sup>.

In addition, the country has managed to articulate and adopt international regulations, such as those provided in Article 14.3 of the Additional Protocol to the Framework Agreement of the Pacific Alliance, where it is established

that the State may take such measures as may be necessary to ensure the security and confidentiality of messages, or to protect the privacy of personal data of end users. Likewise, Article 19.5 of the trade agreement between Mexico, the United States and Canada, establishes a collaboration agreement to neutralize cybersecurity threats, developing risk management capabilities and information sharing.

It is worth noting that since 2014, Mexico has been an observer state in the Budapest Convention<sup>190</sup>, which is a framework for criminalization and helps in procedural matters by providing specific parameters for cooperation between nations. Although the country has been invited to become a full member, it has declined on several occasions. One of the main reasons is the series of legislative modifications since it implies in legislative and regulatory matters to guarantee the adequate protection of national legal systems. To implement in national legislation the criminal offenses provided for in the treaty in accordance with the principle of exact application of the criminal law, with unconditional transparency, from a perspective that involves human rights and recommendations of the entire civil society<sup>191</sup>.

According to the OAS and IDB cybersecurity report, the Mexican regulatory and legal framework has made significant progress in recent years. The country has improved significantly in areas such as data protection legislation, child online protection, consumer protection and intellectual property. However, it has yet to make progress in strengthening cooperation frameworks to combat cybercrime, as well as improving its court systems for the prosecution of cybersecurity crimes.

<sup>186</sup> (Mancera Espinosa, 2020)

<sup>187</sup> (Instituto Federal de Telecomunicaciones, 2018)

<sup>188</sup> Article 19

<sup>189</sup> Articles 80, 81 y 82 (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017)

<sup>190</sup> Sanctioned in 2001 by the European Union Commission, it is the first international treaty. The first international treaty on crimes committed over the Internet and other computer networks, dealing especially with copyright infringement, computer fraud, child pornography and breaches of network security. It also contains a number of powers and procedures, such as the search of computer networks and interception of computer networks.

<sup>191</sup> (Derecho Digitales; Red en Defensa de los Derechos Digitales, 2018)



Figure 7: Cybersecurity regulatory and legal frameworks Mexico 2020 (IDB, 2020)

## Chile

In Chile, the regulatory and legal framework is since 2019 in a state of transformation. This circumscribes a bill in process on personal data, a new law on Computer crimes, which contains the typification of new crimes, including the framework of the Budapest Convention and a procedural improvement of the proof of crime<sup>192</sup>. Similarly, the Cybersecurity Framework Law is being advanced, which aims to provide precise and timeless definitions and responsibilities on cybersecurity, as well as the creation of Response Centers for computer incidents/emergencies in the public and private sectors.

In addition, the bill for the registration of prepaid telephones that is contemplated as a prevention factor to mitigate cybersecurity crimes. Finally, through the bill on critical infrastructure for information systems, it is intended to provide a regulation and strategy to prevent and improve incidents of computer emergencies.

With all this panorama, in terms of computer crimes there is Law No. 19.223 of 1993, which punishes those who carry out illicit activities on information systems. As mentioned in the chapter on privacy, there is Law 19.628, which together with the reform of the Political Constitution of 2018, reaffirmed the right to honor and privacy, introducing the protection of personal data.

According to the OAS and IDB report, the Chilean regulatory and legal framework has made some

progress in recent years, especially in legislation related to data and consumer protection. However, it still has a long way to go, mainly in the areas of child protection and the criminal justice system.

<sup>192</sup> (Ministerio del Interior y Seguridad Pública, 2020)



Figure 8:: Cybersecurity regulatory and legal frameworks Chile 2020 (IDB, 2020)

## Colombia

The Colombian legal and regulatory framework is based on its Political Constitution. It establishes that all persons have the right to their personal and family privacy, as well as the right to know, update and rectify the information collected about them in data banks and in the files of public and private entities. In the collection, processing and circulation of data, freedom of information will be respected<sup>193</sup>.

Through Law 145317, a comprehensive criminal procedural legislation is used, which addresses cybercrimes and recognizes international treaties with INTERPOL and EUROPOL signed in 1960 and 2010, respectively. Since 2018, the country has been part of the Budapest Convention with the objective of preventing acts that jeopardize the confidentiality, integrity and availability of computer systems, networks, and data, as well as the abuse of these, considering such acts as crimes.

Law 1581 of 2012 establishes the basis for data protection, disclosure and reporting of security breaches. Through the Superintendence of Industry and Commerce, compliance with the regulations is guaranteed, as well as the disclosure of rights to its users. In related issues, such as electronic commerce<sup>194</sup>, pornography, and sexual exploitation of minors in cyberspace<sup>195</sup>, rationalization of formalities and

procedures, copyright and related rights<sup>196</sup>, various provisions are related. Similarly, the regulatory development of laws containing issues such as habeas data, electronic signature, authentication mechanisms, open certification entities and the national registry of databases, also obey specific guidelines depending on the case.

According to the cybersecurity report presented by the OAS and the IDB, Colombia is the country with the greatest advances in cybersecurity development in Latin America. The country has made progress in the last 5 years in critical issues such as data protection, child protection and consumer rights.

<sup>193</sup> Articles 11, 12, 13, 14, 17, 21, 22, 24, 29, 44

<sup>194</sup> Ley 527 de 1999. It defines and regulates the access and use of data messages, electronic commerce and digital signatures, and establishes the certification entities and other provisions.

<sup>195</sup> Ley 679 de 2001.

<sup>196</sup> Ley 962 de 2005. Establishes the incentive for the use of integrated technological means to reduce the time and cost of the procedures to be carried out by the administrators.



Figure 9: Regulatory and legal frameworks for cybersecurity Colombia 2020 (IDB, 2020)

## 4.2. CURRENT PUBLIC POLICIES

### Peru

Of the 33 million inhabitants, 60% are Internet users and connect mainly via computer or cell phone<sup>197</sup>. The number connected grew by approximately 13% compared to the beginning of 2020, however, Peru still does not have a cybersecurity policy. Instead, there is the National Cybersecurity Plan, which aims to protect the infrastructure, data and information of the State and the technology used for its processing, against internal or external threats, deliberate or accidental, to ensure confidentiality, integrity, availability, legality and reliability<sup>198</sup>. It is intended to be applied to the entities of the Public Administration, its resources, as well as its processes, proposing the creation of a National Cybersecurity Committee.

Through the National Cybersecurity Policy, the capacities of the state are strengthened to face the threats that threaten security, involving all sectors and entities, and promoting the participation of representatives of the private sector, society, and academia<sup>199</sup>. In this way, support for investigations related to computer attacks is considered, emphasizing the responsibilities of the state. This, with the intention of creating awareness among the population regarding the importance of information security, both in internal management and international cooperation.

Another of the points considered in the policy consists of specialized training in information security and cybersecurity management within the public administration, to face the threats that may arise, through awareness campaigns and programs with the support of the OAS and the Counter-Terrorism Support Committee (CICTE)<sup>200</sup>. Thus, in the first instance, training is given to officials and civil servants directly involved in cyber-attack issues, and then to the rest of the personnel. In the case of citizens, there is a dissemination strategy that includes conferences in educational institutions, forums that give rise to the exchange of opinions and experiences between public and private entities, civil society, and academia to share and disseminate good practices in cybersecurity<sup>201</sup>. The strategy has a territorial approach, which allows a better logistical organization, orienting these activities to specific needs according to the region.

To boost digital transformation and innovation, there is the National Digital Transformation System and the Digital Trust Framework. It organizes public administration activities and promotes its use in the work of companies, citizens, and educational institutions.

Peru has a national Computer Emergency Response Team (CSIRT), called PeCERT<sup>202</sup>, which reports to the Secretariat of Digital Government. Its mission is to coordinate the prevention, treatment, and response to cybersecurity incidents of public sector institutions, as well as to develop strategies, practices, and mechanisms necessary to meet the information security needs of the State<sup>203</sup>. This team coordinates and proposes standards for security in cyberspace, providing advice on technical protection tools.

<sup>197</sup> (Hootsuite, We are Social, 2021)

<sup>198</sup>, <sup>199</sup>, <sup>200</sup>, <sup>201</sup> (Congreso de Perú)

<sup>202</sup> (PeCERT)

<sup>203</sup> (BID, 2020)

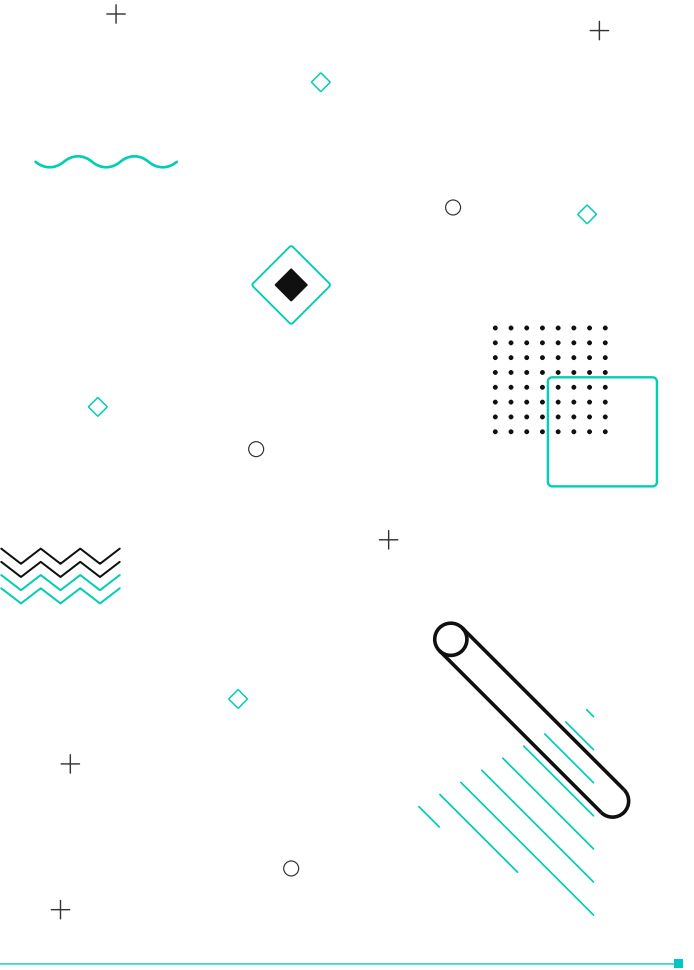


Currently, Peru does not have a risk management and response to the protection of critical infrastructure, since it lacks key contents in the cybersecurity policy and strategy, has low standards in technology acquisitions and a reduced national market for cybersecurity technologies, according to the IDB and OAS cybersecurity report<sup>204</sup>. Faced with this situation, the risk of cyber-attacks is increasing, and the response capacity is not fast enough.

The latest Microsoft Security Intelligence Report recorded, in 2018, an average monthly rate of malware incidents of 8% and 12%<sup>205</sup>. From 2018 to 2019, Peru concentrated 14% of the spyware<sup>206</sup> cases detected in Latin America, placing it as the third country with the most attacks of this type. In response to this situation, in 2021, it established the strategic axis called "State and Governance"<sup>207</sup>, which contemplates, among other things, the full operation of the national security and defense system, aimed at protecting the territory, to prevent and address any threat that endangers national security.

The government of Peru and the IDB, through the loan operation "project for the improvement and expansion of support services to provide services to citizens and companies at the national level", agreed to promote specific activities to strengthen national cybersecurity<sup>208</sup>. With this, it is expected to achieve savings of almost 35 million soles<sup>209</sup> per year by improving face-to-face services, tripling the number of daily data exchange transactions between government entities at the central level for the delivery of services, thus reducing unnecessary procedures for citizens.

The graph below shows the cybersecurity policy and strategy indicators in 2020, in relation to 2016. Since Peru does not have a clearly defined strategy as in the case of other countries, most of these criteria did not present significant changes. However, the mode of operation in incident response is considered better, as well as the organization in cyber defense.



<sup>204</sup>, <sup>205</sup> (ComexPerú, 2020)  
<sup>206</sup> Malicious spyware that steals personal data without user consent.  
<sup>207</sup> (Decreto Supremo - N° 106-2017-PCM)  
<sup>208</sup> (BID, 2020)  
<sup>209</sup> Equivalent to approximately USD 9 million.



Figure 10: Peru 2020 Cybersecurity Policy and Strategy (IDB, 2020)



Mexico

>>>>

Of the 129.6 million inhabitants, 71% are internet users<sup>210</sup>, being the cell phone the most used device to connect; with all this, the cases of cyber-attacks reached to grow up to 400%<sup>211</sup>. Since 2017, there is the National Cybersecurity Strategy raises five objectives: society and rights; economy and innovation; public institutions; public safety and national security. With this, it seeks to define the principles and identify the main actors involved, giving clarity on the articulation of efforts between individuals, civil society, private and public organizations in cybersecurity<sup>212</sup>. This is one of the most robust strategies in the region.

In the framework of the Pacific Alliance, in December 2016 the Digital Agenda was approved with the intention of: "enhancing cooperation in digital security and fostering trust in the use of ICTs". The main emphases are: digital economy, digital connectivity and digital ecosystem<sup>213</sup>. The Mexican government has maintained its focus on the idea that the digital ecosystem is created by the government.

From a human rights perspective, the strategy seeks to guarantee freedom of expression, access to information, respect for privacy, protection of personal data, health, education, and work. Likewise, it is expected to have the capacity to manage uncertainty scenarios through prevention and correction to reduce the impact of threats. The participation of actors in various disciplines is envisaged to ensure Internet governance that protects users. To achieve this, it is proposed to promote the culture of cybersecurity and

the development of capabilities related to the technological resources available to protect against threats, both in academia and in the public and private sectors. All supported by ICT research<sup>214</sup>, development, and innovation within a legal and regulatory framework.

Although Mexico does not have a specific law on cybercrime, Article No. 211 of the Penal Code contemplates computer crime<sup>215</sup>. However, these provisions are limited and leave several loopholes, making it difficult to fight cybercrime.

For years, Mexico has had a national CSIRT, CERT-MX, to prevent and mitigate cyber threats. CERT-MX is under the orbit of the Federal Police and is part of the CSIRT Americas network<sup>216</sup>. Various events are organized around it, courses and seminars are given, information is disseminated, and research is carried out.

Currently, according to MIT Analytics in Cambridge Massachusetts, with the pandemic, fraud and theft of classified information through cyber-attacks increased exponentially in Mexico<sup>217</sup>. With cybercrime a growing concern, Mexican organizations have included proactive cyber and privacy risk management, by design, in the project plan and budget from conception<sup>218</sup>. As seen in the chart below, they also factor cyber and privacy risk management into their project planning and budgeting as a key consideration.

<sup>210</sup> (Hootsuite, We are Social, 2021)  
<sup>211</sup> (El Economista, 2020)  
<sup>212, 213, 214</sup> (Gobierno de México)  
<sup>215, 216</sup> (BID, 2020)  
<sup>217</sup> (Foro Jurídico México, 2020)  
<sup>218</sup> (BID, 2020)



Figure 11: Cybersecurity policies and strategies Mexico. (IDB, 2020)

# Chile

Of the 19.6 million inhabitants, 82.3% are internet users<sup>219</sup>, with mobile devices being the ones with the highest traffic. There were 525 million cyber-attack attempts in the first half of 2020 alone<sup>220</sup>. Since 2017, the country has had the National Cybersecurity Policy 2017-2022, which states the intention of having a robust and resilient information infrastructure with the stipulation of technical measures to manage and overcome risks, identify critical infrastructures and have incident response, reporting and management teams. It also raises the protection of citizens in cyberspace with the prevention of incidents, implementation of punitive measures, respect, and promotion of fundamental rights. All of this is based on a culture of cybersecurity implemented through the promotion of good practices and responsibility in the use of technology by users.

Another important point is the establishment of national and international cooperation relations on cybersecurity, through forums and discussions. In principle, it is planned as a priority the renewal of computer emergency response equipment at national level, the optimization of control systems, the signing of agreements on critical infrastructure with academia and private entities and the regulation of computer crimes.

In 2018, the President of the Republic appointed a presidential advisor who reports directly to him on cybersecurity matters and a restructuring was carried

out in the Undersecretariat of the Interior to carry out the measures described in the aforementioned policy, through the Cybersecurity Coordination Unit (Exempt Resolution No. 5,006)<sup>221</sup>. In the same year, a National Cyber Defense Policy was approved and a specific unit for coordination of National Defense was created<sup>222</sup>. These units depend on the Ministry of Defense and the Ministry of Finance.

Since 2019, there is Law No. 21,180<sup>223</sup> on "digital transformation" which establishes the electronic format for administrative acts, in addition to promoting the use of interoperability platforms between the bodies of the State administration, the creation of a digital repository and the traceability of all communication between the different bodies of the State administration, ensuring security in the processes.

The Government CSIRT is a member of CSIRT Americas<sup>224</sup>, which gives it access to all the information offered by the platform, including the dynamic exchange of information through the Malware and Threat Information Sharing Platform (MISP) deployed in the hemispheric network. In 2020, the strengthening of the Government CSIRT, under the Ministry of the Interior and Public Security<sup>225</sup>, was proposed. It is mainly made up of the Ministries, the Intendancies, the Governors' Offices and the public bodies and services created for the fulfillment of the administrative function, including the Comptroller General of the

Republic, the Central Bank, the Armed Forces, the Armed Forces and Public Order and Security, the Regional Governments, the Municipalities, and the public companies; on the other hand, the private sector is incorporated by agreement, according to specific strategies.

There is the Chilean Cybersecurity Alliance, founded by nine institutions representing important sectors of the country, through recognized state, private and academic organizations, whose objective is to cooperate with the authorities in this area, generate new networks of contacts and international alliances<sup>226</sup>. Likewise, there is the Interministerial Cybersecurity Committee whose function is the analysis and implementation of the National Cybersecurity Policy and other associated measures.

Since 2018, Chile is ranked by the UN, as the second most developed country in terms of e-government in Latin America and the Caribbean. Likewise, various continuing education and postgraduate programs in cybersecurity have been promoted, both from a technical and legal point of view, to train skilled human resources in these areas<sup>227</sup>. The Chilean government is particularly interested in training the population in cybersecurity strategies.

The graph below shows the cybersecurity policy and strategy in 2020 compared to 2016. The protection of critical infrastructure did not have major changes, however, the development of a strategy allowed improving incident response capacity and cyber defense.



<sup>219</sup> (Hootsuite, We are Social, 2021)

<sup>220</sup> (Congreso Nacional Chile, 2017)

<sup>221</sup>, <sup>222</sup> (BID, 2020)

<sup>223</sup> (Ley 21180, 2019)

<sup>224</sup> (ITU, 2015)

<sup>225</sup> (BID, 2020)

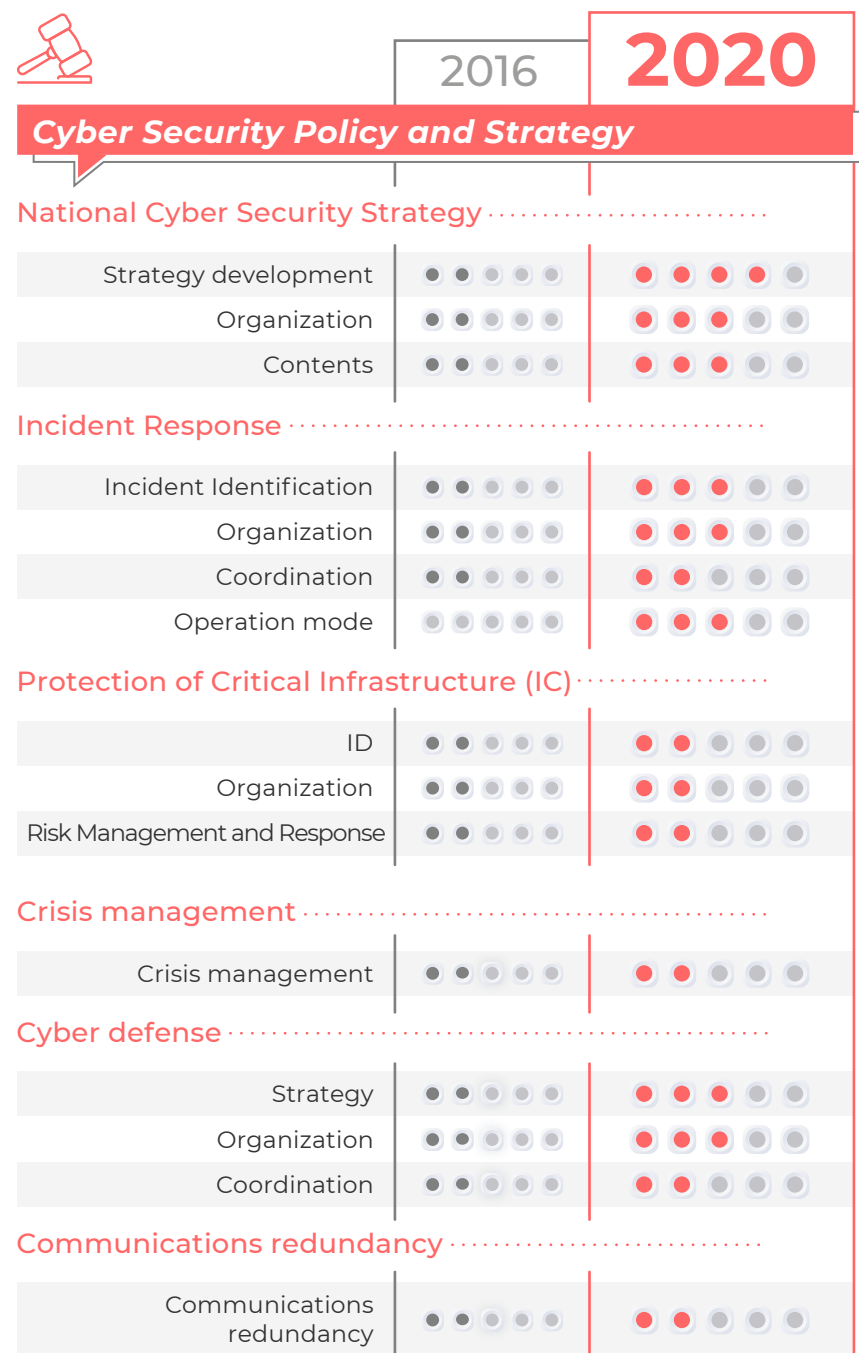


Figure 12: Cybersecurity Policy and Strategy in Chile. (IDB, 2020)

## Colombia

Of the 51.07 million inhabitants, 68% are internet users<sup>228</sup>, where the cell phone is the most used device for this purpose. Colombia adopted in 2016 a second national policy on cybersecurity whose objective is to strengthen the capacities of the State to respond to threats in this area<sup>229</sup>. The objective is to strengthen the State's capabilities to respond to threats in cyberspace. In the country, the dynamics of cybercrime during 2020 used as a vector of infection the concern and uncertainty derived from quarantine and isolation, as well as the need for companies to generate new work environments from virtuality<sup>230</sup>.

The Ministry of Information Technologies and Communications (MinTIC) has the direction of Digital Government, which has issued a model of Security and Privacy of Information (MSPI), where good security practices based on the rules of protection of personal data, transparency and access to public information are exposed<sup>231</sup>. This model seeks to contribute to the increase of transparency in Public Management, promoting the use of best practices in Information Security as the basis for the application of the Digital Security concept.

The Colombian Cyber Emergency Response Group (colCERT) is the national coordinating body for cybersecurity and cyberdefense. Its mission is to

protect the critical infrastructure of the Colombian State against cybersecurity emergencies that threaten or compromise national security and defense<sup>232</sup>. The entity has conducted simulation exercises of multiple cyber-attacks, adapted to the local context, to facilitate the exchange of knowledge and experiences in the prevention, detection and mitigation of the effects of a possible large-scale cyber-attack. In July 2021, the National Policy CONPES on Digital Trust and Security was issued<sup>233</sup>, which establishes measures to expand digital trust and improve digital security to strengthen inclusion and competitiveness. To achieve this objective, it is expected to strengthen the digital security capabilities of citizens, the public sector, and the private sector in the country; as well as update the governance framework for digital security in the country.

Colombia has a financial CSIRT, which seeks to establish a cyber intelligence sharing community<sup>234</sup>, structure incident management and mitigate the impact of risks. Similarly, in conjunction with the National Police, there is a Sandbox to respond to computer security incidents.

At the educational level, the MinTIC promotes the training of public officials in areas of cybersecurity and cyber defense through scholarships and digital security courses in specific areas. On the other hand, there is the

<sup>228</sup> (Hootsuite, We are Social, 2021)

<sup>229</sup> (BID, 2020)

<sup>230</sup> (TicTac, 2020)

<sup>231</sup> (MinTIC)

<sup>232</sup> (colCERT)

<sup>233</sup> (CONPES 3995, 2020)

<sup>234</sup> (Asobancaria)



**Cyber Security Policy and Strategy**

	2016	2020
<b>National Cyber Security Strategy</b>		
Strategy development	20%	80%
Organization	20%	80%
Contents	20%	80%
<b>Incident Response</b>		
Incident Identification	20%	80%
Organization	20%	80%
Coordination	20%	80%
Operation mode	20%	80%
<b>Protection of Critical Infrastructure (IC)</b>		
ID	20%	80%
Organization	20%	80%
Risk Management and Response	20%	80%
<b>Crisis management</b>		
Crisis management	20%	80%
<b>Cyber defense</b>		
Strategy	20%	80%
Organization	20%	80%
Coordination	20%	80%
<b>Communications redundancy</b>		
Communications redundancy	20%	80%





# Conclusions



# Privacy

## Mexico

There is the Federal Data Protection Law for public and private entities.

Knowledge of ARCO Rights (Access, Rectification, Cancellation and Opposition) is promoted.

The National Institute of Transparency, Access to Information and Protection of Personal Data - INAI is the authority responsible for promoting and monitoring compliance with the right to personal data protection in Mexican territory.

The collection of data from employees in their workplaces in the context of the pandemic does not require authorization.

In the framework of the pandemic, there is the mobile application App Covid19, where the user, voluntarily and unilaterally, may delete the registration of the mobile device's location at any time.

## Peru

Citizen data is protected through the Political Constitution.

The National Authority for the Protection of Personal Data ANPD is the entity in charge of complying with and enforcing current regulations in this regard.

Peruvian law establishes the supremacy of fundamental rights and the authorization of the individual.

Penalty of up to 60 thousand USD for those who do not respect the privacy of users.

In the framework of the pandemic, there is the mobile App: Peru en tus manos, to find out information on issues related to symptoms to prevent, guide patients, maintain a statistical record and provide attention to citizen doubts, guaranteeing safety and security. corresponding confidentiality. Its use is voluntary.

# Privacy

## Colombia

The person responsible for the treatment must request the authorization of the owner at all times. This must be given orally, in writing or through unequivocal conduct (silence is not unequivocal conduct) and those responsible must keep the proof of said authorization.

The owner has the right to revoke his authorization through a claim.

The Superintendency of Industry and Commerce is in charge of protecting the fundamental right of Habeas Data (to know, update and rectify user data).

In the framework of the pandemic, the CoronApp mobile application is available. Its use is voluntary and the citizen is free to download, use or uninstall the mobile application, as well as to request the deletion of personal data.

## Chile

The right to privacy itself is not defined.

Chile is the first country in South America to adopt a regulatory framework on privacy.

There is no established supervisory authority.

In the framework of the pandemic, there is the CoronApp mobile application that has not been widely received, due to alleged gaps and inaccuracies in the rules of the mobile application and the rights of users. This could allow the data to be used for purposes that its holders do not fully dimension.

# Cloud

## Mexico

The State guarantees a universal digital inclusion policy with annual goals.

Suggested minimum criteria have been established for contracting cloud computing services, to comply with the obligations established in the regulations, avoiding any violation of the security of personal data.

Half of the companies that make use of cloud services have their own infrastructure and half in the cloud, and less than 10% are under an “all in cloud” structure.

Subsecretaría de Comunicaciones y Desarrollo Tecnológico (Undersecretariat of Communications and Technological Development), is the entity in charge of these matters.

The Mexican government seeks to increase its investment in cloud services by 25%.

## Peru

There is the Framework Law for the Modernization of State Management.

The entity in charge of these matters is the Digital Government Secretariat - SeGDi

The Peruvian Air Force (FAP) is the first institution in the Peruvian public sector to implement a Private Cloud model

From the Covid-19 situation, the use of cloud services increased, with an increase of more than 25% during the quarantine.

Peru seeks to invest in the use of cloud services 20% more than in previous years.

# Cloud

## Colombia

Cloud services have two regulatory mechanisms, the first, focused on the protection of personal data and the second, operational risks.

National Development Plan (PND) 2018-2022, clearly the need to prioritize cloud services.

The Financial Superintendency of Colombia issued an external circular with the aim of facilitating cloud use services in the sector, establishing the general obligations of the entities and the service agreements or contracts.

In the case of the private cloud, the services must be provided by data centers accredited by Colombia Compra Eficiente (CCE).

## Chile

There is Law 19,880, where the guidelines for contracting services are given.

In the case of banks, each bank must report annually on the risk tolerance it is willing to contract according to the cloud service it acquires (public, hybrid or private).



# Broadband

## Mexico

There is the Federal Law on Telecommunications and Broadcasting of 2014. In 2020, it underwent some modifications.

The amendment included the consideration of broadband internet access as a constitutional obligation and the legality of foreign investment.

The institution in charge of these matters is the Federal Telecommunications Institute (IFT) and the National Broadband Impulse Network (NIBA Network).

Mexico was the fourth country with the highest growth in fixed broadband penetration from June 2013 to June 2019.

Investment in telecommunications infrastructure fell due to the pandemic.

## Peru

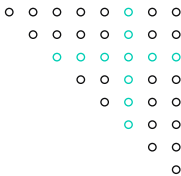
There is Law No. 29904 or Law for the Promotion of Broadband and Network Construction.

The construction of a National Fiber Optic Backbone Network - Red Dorsal Nacional de Fibra Óptica has been managed since 2012.

It seeks to strengthen science, technology and innovation by bringing together all public universities and research institutes to the National Research and Education Network.

There is the Supervisory Agency for Private Investment in Telecommunications (OSIPTEL), which determines and periodically updates other technical characteristics of Broadband Internet connections.

# Broadband



## Colombia



The Ministry of Information Technology and Communications (MinTIC) and the Communications Regulation Commission (CRC) are the entities in charge of these matters.

All providers of telecommunications networks and services will have equal opportunities to access the use of the spectrum and will contribute to the Single Fund for Information and Communication Technologies. Spectrum assignment seeks to maximize social welfare.

The Superintendency of Industry and Commerce (SIC) is the entity in charge of verifying that operators comply with this new definition.

As of January 2019, Colombia has a new definition of broadband. With minimum speeds of 25 Mbps download (download) and 5Mbps upload (upload).

In 2020, the Government of Colombia developed a scheme of subsidies for the internet in strata 1 and 2 that seeks the adoption of mechanisms aimed at the massification of social internet plans for users of these socioeconomic strata.

Strategies have been proposed for internal adaptation of the functions and responsibilities of the MINICT and the ANE in terms of emphasis on radio and television services, modernization of spectrum management processes, and regulation of unauthorized operations of the radioelectric spectrum.



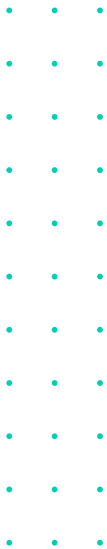
## Chile

A system for measuring internet quality speed was established, as well as the creation of the Independent Technical Body to guarantee quality and obtain statistical information.

Internet access providers must comply with the quality of service levels established by the provisions issued for this purpose by the Ministry of Transport.

Since 2017, pilot projects have been promoted to implement Community Broadband, such as the ChileGob WiFi points, a project that helps improve access in the most vulnerable places in Chile that have few connectivity alternatives.

The entity responsible for the telecommunications sector is the Undersecretariat of Telecommunications (SUBTEL), which in 2020 allocated about 86 billion Chilean pesos (approximately US \$ 112 million) to reduce the digital divide.



# Cybersecurity

## Mexico

+

## Peru

Mexico does not have a general cybersecurity law, however, since 2020 a discussion has been going on to promote it in the Senate.

The IFT has pointed out the importance of developing a security regulatory framework for devices, infrastructure and networks.

Since 2014, Mexico has been an observer state in the Budapest Convention, promoting international cooperation.

Of the 129.6 million inhabitants, 71% are Internet users.

It is proposed to promote the culture of cybersecurity and the development of capacities related to the technological resources available in order to protect against threats, both in academia and in the public and private sectors.

Mexico has a national CSIRT, the CERT-MX, to prevent and mitigate cyber threats. The CERT-MX is under the orbit of the Federal Police and is part of the CSIRT Americas network

With the pandemic, fraud and theft of classified information through cyberattacks increased exponentially in Mexico.

Laws 29733 (Protection of Personal Data), 29904 (Promotion of Broadband and Construction of the National Fiber Optic Backbone Network), and 27658 (Framework Law for the Modernization of State Management).

Regarding data protection and child protection, these are the areas where the country has improved significantly in the last five years, showing a consolidated state.

Relevant aspects regarding consumer protection legislation, intellectual property, the criminal justice system and cooperation frameworks are in a formative stage.

Of the 33 million inhabitants, 60% are Internet users and connect mainly through computers or mobile phones.

Peru does not yet have a cybersecurity policy. In its place, there is the National Cybersecurity Plan.

To promote digital transformation and innovation, there is the National Digital Transformation System and the Digital Trust Framework.

Peru has a national Computer Emergency Response Team (CSIRT), called PeCERT, which depends on the Digital Government Secretariat.

Peru does not have a risk management and response to the protection of critical infrastructure.

# Colombia



# Cybersecurity

# Chile

Through Law 145317, a comprehensive criminal procedural legislation is used, which addresses cyber crimes and recognizes the international treaties with INTERPOL and EUROPOL signed in 1960 and 2010, respectively. Since 2018, the country has been a part of the Budapest Convention.

Superintendency of Industry and Commerce, compliance with regulations is guaranteed.

Colombia is the country with the greatest advances in cybersecurity development in Latin America. The country has made progress in the last 5 years on critical issues such as data protection, child protection and consumer rights.

Of the 51.07 million inhabitants, 68% are Internet users.

The Colombian Cyber Emergency Response Group (colCERT) is the coordinating body at the national level in aspects of cybersecurity and cyber defense.

Colombia has a financial CSIRT, which seeks to establish a cyber intelligence exchange community, structure incident management, and mitigate the impact of risks. Similarly, in conjunction with the National Police, there is a Sandbox to respond to computer security incidents.

The MinTIC promotes the training of public officials in areas of cybersecurity and cyberdefense through scholarships and digital security courses in specific areas.

The response to incidents, the protection of critical infrastructure has improved, giving more tools in crisis management in 2020.

A bill (Law project) in process on personal data, a new law on computer crimes, which contains the definition of new crimes, including the framework of the Budapest Convention and a procedural improvement of the evidence of crime.

The Chilean regulatory and legal framework has made certain advances in recent years, especially in legislation related to data protection and the consumer. However, it still has a long way to go, mainly in the areas of child protection and the criminal justice system.

Of the 19.6 million inhabitants, 82.3% are internet users

There were 525 million attempted cyberattacks in the first half of 2020 alone.

Raises the protection of citizens in cyberspace with the prevention of incidents, implementation of sanctioning measures, respect and promotion of fundamental rights. All around a culture of cybersecurity implemented through the promotion of good practices and responsibility in the management of technology by users.

Undersecretariat of the Interior to carry out the measures described in the aforementioned policy, through the Cybersecurity Coordination Unit

National Cyber Defense Policy and a specific unit was created to coordinate National Defense.

There is the Chilean Cybersecurity Alliance, founded by nine institutions that represent important sectors of the country

The Government CSIRT is a member of CSIRT Americas

Chile is listed by the UN as the second most developed country in terms of electronic government in Latin America and the Caribbean.

The protection of critical infrastructure did not have major changes, however, the development of a strategy allowed to improve the capacity of response to incidents and cyber defense.



## General Conclusions – Already



Global awareness of the importance of privacy protection in a context where access to and correct treatment of available information is a valuable and forceful tool in large-scale decision making has left governments with great responsibility. The governments of the countries under study have shown a trend in their interest in promoting trust and coordination to preserve the fundamental rights of citizens in terms of privacy, with the management of government institutions in charge and information campaigns, as in Mexico's case, with the Transparency Institute.



Connectivity is a critical element in the process of digitization of services and democratization of information. However, quality Internet access in the countries studied still has a long way to go. Access to quality Internet, especially in rural areas, is limited, causing numerous drawbacks in education and economic growth, which have become more evident in the last year. Current policies in the countries studied show a general awareness in terms of infrastructure deployment and connectivity. However, it is worth strengthening the digital skills of the urban and rural population to maximize the benefits of connectivity.



Cloud services can guarantee transparency and equity in access to information if there is adequate regulation regarding information management and connectivity. The governments of the countries under study have digital transformation plans whose guidelines include implementing cloud services in the public context, as is the case of the National Development Plan in Colombia or the Good Practices Manual in Chile.



The increase in cyber-attacks in recent years is a common denominator in global terms. The countries studied by governments are aware of the imminent threat posed by mismanagement of citizen protection and security tools. In terms of regulations, countries such as Peru and Mexico consider cybersecurity in a cross-cutting approach as part of the digital transformation plan, while Chile and Colombia have implemented it under the legislation. The four countries share an interest in international collaboration to protect themselves from cyber threats, encouraging and supporting such management. On the other hand, the particular emphasis on training also positively impacts prevention and protection, according to the IDB.



## Proposals



Implementing cybercrime in legislative matters, as a crime itself allows defining more precise measures when judging these behaviors.



Continue with the digitization efforts of governments, promoting digital payments, cloud services and online procedures.



Strengthen the training programs in technological skills for the population according to the specific needs of each region. In this way, the available technological resources are used more efficiently.



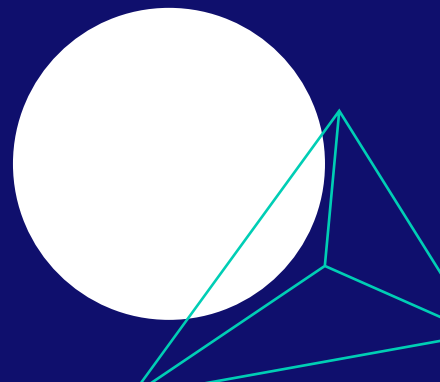
Provide government support to small and medium-sized companies to promote the use of broadband and cloud services such as subsidies for the implementation of these tools, such as training for their use.



Continue and strengthen regional support for cooperation in regulation regarding the deployment of infrastructure, prevention and reaction to cyber attacks, through the Pacific Alliance.



Developing a regulatory framework that focuses on promoting investment in technological infrastructure reinforces the efforts of governments to reduce social gaps, thanks to the democratization of the Internet service and its correct use.





# References



## Privacy

- Acosta, D. (27 de Abril de 2020). Big Data, COVID – 19 y desafíos en materia de privacidad. Obtenido de Universidad Externado de Colombia:  
<https://propintel.uexternado.edu.co/big-data-covid-19-y-desafios-en-materia-de-privacidad/>
- AVISO DE PRIVACIDAD INTEGRAL. (2020). Obtenido de SISTEMA DE DATOS PERSONALES DEL SISTEMA DE REGISTRO DE INFORMACIÓN DE LOCATEL (SIRILO) DE LA AGENCIA DIGITAL DE INNOVACIÓN PÚBLICA DE LA CIUDAD DE MÉXICO: <https://covid19.cdmx.gob.mx/resources/docs/aviso.extendido.pdf>
- BBC News Mundo. (26 de Octubre de 2020). Chile aprueba por abrumadora mayoría cambiar la Constitución de Pinochet: ¿qué pasa ahora y por qué es un hito mundial? BBC News. Obtenido de <https://www.bbc.com/mundo/noticias-america-latina-54686919>
- Buitrago, F., & George, S. (2017). The No Collar Economy. Obtenido de [www.nocollareconomy.com](http://www.nocollareconomy.com)
- CIPER CHILE. (22 de Abril de 2020). Obtenido de <https://www.ciperchile.cl/2020/04/22/problemas-de-proteccion-de-los-datos-personales-de-la-aplicacion-coronapp/>
- Congreso de la República del Perú. (2013). Decreto Supremo No. 003 de 2013. Obtenido de [http://www2.congreso.gob.pe/sicr/cendocbib/con5\\_uibd.nsf/C6AF75A37B50276D0525831A0061FA0B/\\$FILE/DS-3-2013-JUS.REGLAMENTO.LPDP\\_.pdf](http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C6AF75A37B50276D0525831A0061FA0B/$FILE/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf)
- Congreso General de los Estados Unidos Mexicanos. (2011). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Obtenido de [http://www.diputados.gob.mx/LeyesBiblio/regley/Reg\\_LFPDPPP.pdf](http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf)

- Congreso General de los Estados Unidos Mexicanos. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Obtenido de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>
- Congreso Nacional de Chile, Información Pública, Ley no. 20.285. (s.f.). Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=276363>
- Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg. Obtenido de <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37>
- Council of Europe. (2017). Protocol amending the Additional Protocol to the Convention on the Transfer of Sentenced Persons. Strasbourg. Obtenido de <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680730cff>
- Donoso, N., & Vega, M. (24 de Abril de 2020). ¿La Constitución protege nuestros datos personales? Los derechos digitales en tiempos de pandemia. La Tercera. Obtenido de <https://www.latercera.com/la-tercera-pm/noticia/la-constitucion-protege-nuestros-datos-personales-los-der-echos-digitales-en-tiempos-de-pandemia/IESMWS5TRJC4RLZROPWPHPQWSU/>
- Equipo Legal Amazon México. (2019). Manual de Protección de Datos Personales Para Organizaciones de la Sociedad Civil. USAID.
- Gobierno de Perú. (Mayo de 2020). Obtenido de <https://www.gob.pe/institucion/pcm/noticias/150943-gobierno-lanza-nueva-version-de-app-peru-en-tus-manos-para-advertir-a-los-ciudadanos-sobre-las-zonas-con-mayor-probabilidad-de-contagio>
- INFOCDMX. (2020). Obtenido de <https://www.infocdmx.org.mx/covid19/proteccion/>
- Instituto Nacional de Salud Colombia. (2020). Política de tratamiento de información relacionada con la CoronApp Colombia. Obtenido de <https://www.ins.gov.co/Normatividad/PolíticasInstitucionales/politica-de-tratamiento-de-informacion-coronapp-colombia.pdf>
- Lara, C., Picheira, C., & Vera, F. (s.f.). La privacidad en el sistema legal chileno. Obtenido de <https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf>
- Ley 1581 de 2012. (s.f.). Obtenido de [https://www.mintic.gov.co/portal/604/articles-4274\\_documento.pdf](https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf)
- Ley de protección de datos personales en Perú. (2011). Obtenido de [http://www.pcm.gob.pe/transparencia/Resol\\_ministeriales/2011/ley-29733.pdf](http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf)

Ministerio de Justicia y Derechos humanos Perú. (12 de Marzo de 2020). Obtenido de <https://www.gob.pe/institucion/minjus/noticias/108768-divulgar-datos-personales-de-pacientes-con-corona-virus-puede-ser-multado-hasta-con-215-mil-soles>

MinSalud Colombia. (s.f.). POLITICA DE PRIVACIDAD Y CONFIDENCIALIDAD DEL MINISTERIO DE SALUD Y. Obtenido de <https://www.minsalud.gov.co/Documents/Politica-de-privacidad-y-confidencialidad-del-MSPS.pdf>

Mogollón Gonzalez, C. (30 de Marzo de 2020). COVID-19: Implicaciones de privacidad y protección de datos personales en México. Obtenido de <https://www.gtlaw.com/en/insights/2020/3/covid19-implicaciones-de-privacidad-y-proteccion-de-datos-personales-en-mexico>

Régimen Legal nacional de protección de datos personales. (s.f.). Obtenido de [https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20443/5/REG\\_NACIONAL\\_PROTECC\\_D\\_ATOS\\_PERSONALES%20\(LV\)\\_v5.pdf](https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20443/5/REG_NACIONAL_PROTECC_D_ATOS_PERSONALES%20(LV)_v5.pdf)

REGLAMENTO DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES. (2011). Obtenido de [http://www.diputados.gob.mx/LeyesBiblio/regley/Reg\\_LFPDPPP.pdf](http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf)

Rodríguez, K., & Alimonti, V. (2020). The State of Communication Privacy Law in Mexico. Electronic Frontier Foundation. Obtenido de <https://necessaryandproportionate.org/uploads/2020-mexico-en-faq.pdf#question1>

Rodriguez, K., Alimonti, V., & Castañeda, J. D. (2020). The State of Communication Privacy Law in Colombia. Electronic Frontier Foundation,. Obtenido de <https://necessaryandproportionate.org/uploads/2020-colombia-en-faq.pdf#question3>

Stanford. (2014). Stanford Encyclopedia of Philosophy. Obtenido de <https://plato.stanford.edu/entries/it-privacy/#ConVsInfPri>

Superintendencia de Salud Chile. (s.f.). Obtenido de <https://www.supersalud.gob.cl/portal/w3-article-3670.html>

Universidad Externado de Colombia. (2020). Obtenido de <https://www.uxternado.edu.co/derecho/la-aplicacion-coronapp-enfrenta-problemas-constitucionales/>

VARONIS. (s.f.). Obtenido de <https://www.varonis.com/blog/data-privacy/#comparison>

Viollier, P. (2017). Estado de la protección de datos en Chile. Derechos Digitales. Obtenido de <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

## Cloud-based services

Asobancaria. (26 de Noviembre de 2018). Semana Económica(1164). Obtenido de <https://www.asobancaria.com/wp-content/uploads/1164.pdf>

Autoridad Nacional de Protección de Datos Personales - Directiva de Seguridad de la Información. (2011). Ley N° 29733 - Ley de Protección de Datos Personales. Obtenido de <https://www.minjus.gob.pe/wp-content/uploads/2013/11/Directiva-de-Seguridad-DGPDP.pdf>

BID. (2020). Computacion en la nube Contribucion al desarrollo de ecosistemas digitales en paises del Cono Sur. Obtenido de <https://publications.iadb.org/publications/spanish/document/Computacion-en-la-nube-Contribucion-al-desarrollo-de-ecosistemas-digitales-en-paises-del-Cono-Sur.pdf>

Cascada Insights. (2019). Truth in Cloud. Obtenido de [https://www.veritas.com/content/dam/Veritas/docs/reports/Truth\\_in\\_Cloud\\_2019-CDM\\_Research.pdf//https://itmastersmag.com/noticias-analisis/en-mexico-el-cloud-es-hibrido-ahorro-en-costos-y-tiempo-de-procesamiento-son-clave-en-la-adopcion/](https://www.veritas.com/content/dam/Veritas/docs/reports/Truth_in_Cloud_2019-CDM_Research.pdf//https://itmastersmag.com/noticias-analisis/en-mexico-el-cloud-es-hibrido-ahorro-en-costos-y-tiempo-de-procesamiento-son-clave-en-la-adopcion/)

CCE. (2019). Colombia Compra Eficiente. Obtenido de Nube Privada III, Nube Pública III: <https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/nube-privada-iii>

ChannelNewsPerú. (23 de junio de 2020). Obtenido de <https://channelnewsperu.com/index.php/2020/06/23/tendencias-tecnologicas-se-aceleran-en-tiempos-del-covid-19/>

CIO México. (abril de 2020). Obtenido de <https://cio.com.mx/que-importancia-tiene-la-infraestructura-de-ti-en-contextos-de-alta-demanda/>

CIO Perú. (s.f.). Obtenido de <https://cioperu.pe/articulo/29947/covid19-prueba-el-estres-de-los-servicios-de-la-nube/>

Congreso de Colombia. (2019). Ley N°1978 de 2019.

Congreso de la República de Colombia. (2012). Ley Estatutaria 1581 de 2012. Obtenido de [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_1581\\_2012.html#:~:text=Por%20la%20cual%20se%20dictan,la%20protecci%C3%B3n%20de%20datos%20personales.&text=Los%20principios%20y%20disposiciones%20contenidas,de%20naturaleza%20p%C3%ABlica%20o%20privada.](http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html#:~:text=Por%20la%20cual%20se%20dictan,la%20protecci%C3%B3n%20de%20datos%20personales.&text=Los%20principios%20y%20disposiciones%20contenidas,de%20naturaleza%20p%C3%ABlica%20o%20privada.)

CONPES. (2019). Obtenido de [https://www.mintic.gov.co/portal/604/articles-107147\\_recurso\\_1.pdf](https://www.mintic.gov.co/portal/604/articles-107147_recurso_1.pdf)



CRC. (1 de Septiembre de 2020). Comisión Nacional de Regulaciones Colombia. Obtenido de <https://www.crc.com.gov.co/es/noticia/crc-publica-el-monitoreo-sobre-tendencias-tecnologicas-globales-y-su-evolucion-reciente>

DCD. (2020). Obtenido de <https://www.datacenterdynamics.com/es/noticias/la-inversi%C3%B3n-en-cloud-computing-podr%C3%ADa-crecer-hasta-un-20-en-per%C3%BA-en-los-pr%C3%B3ximos-a%C3%B1os/>

DF SUPLEMENTOS. (09 de 07 de 2020). Obtenido de <https://www.df.cl/noticias/site/artic/20200708/asocfile/20200708162003/20200709suple.pdf>

División de Gobierno Digital Chile. (19 de Febrero de 2018). Obtenido de <https://cdn.digital.gob.cl/Guia+Cloud+v2.pdf>

El Comercio Perú. (2020). Obtenido de <https://elcomercio.pe/economia/dia-1/cloud-computing-se-dispara-demanda-por-cloud-durante-la-cuarentena-del-covid-19-coronavirus-noticia/>

El Economista. (31 de marzo de 2020). Obtenido de <https://www.eleconomista.com.mx/tecnologia/El-Covid-19-convirtio-a-la-nube-en-una-infraestructura-critica-expertos-20200331-0092.html>

Forbes. (2020). Obtenido de <https://www.forbes.com.mx/tecnologia-negocios-pandemia-cambio-digital-cultural-google/>

García Zaballos, A., Iglesias Rodríguez, E., Puig Gabarró, P., & Campero, T. (2020). Contratación pública de servicios de computación en la nube: Mejores prácticas para su implementación en América Latina y el Caribe. BID.

Gobierno de la República Mexicana. (Noviembre de 2013). Estrategia Digital Nacional. Obtenido de [https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia\\_Digital\\_Nacional.pdf](https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf)

Gobierno de México. (s.f.). Obtenido de <https://www.gob.mx/sct/acciones-y-programas/subsecretaria-de-comunicaciones>

Gobierno Digital Chile. (s.f.). Obtenido de <https://digital.gob.cl/>

Gobierno Digital Chile. (Noviembre de 2019). Obtenido de <https://www.carey.cl/ley-sobre-transformacion-digital-del-estado/#:~:text=Con%20fecha%2011%20de%20noviembre,de%20la%20administraci%C3%B3n%20del%20Estado.>

IFT. (Julio de 2020). Instituto Feferal de Comunicaciones México. Obtenido de [http://www.ift.org.mx/sites/default/files/dgci\\_estudio-cloud\\_computing.pdf](http://www.ift.org.mx/sites/default/files/dgci_estudio-cloud_computing.pdf)



Instituto Nacional de Transparencia y Protección de Datos Personales. (2018). Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales. Obtenido de <http://inicio.inai.org.mx/nuevo/ComputoEnLaNube.pdf>

ITU. (2018). Estudio sobre TIC y salud pública en América Latina: la perspectiva de e-salud y y m-salud. Obtenido de [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-E\\_HEALTH.13-2018-PDF-S.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.13-2018-PDF-S.pdf)

La República. (Agosto de 2020). Obtenido de <https://www.larepublica.co/empresas/colombia-es-referente-en-la-region-al-hablar-de-empresas-que-aprovechan-la-data-3050979>

Ley 1978 de 2019. (s.f.). Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=98210>

Microsoft. (Febrero de 2020). Obtenido de <https://news.microsoft.com/es-xl/microsoft-anuncia-un-plan-de-inversion-de-1100-millones-de-dolares-para-impulsar-la-transformacion-digital-en-el-pais-incluyendo-su-primera-region-de-centro-de-datos-de-la-nube-en-mexico/>

Microsoft. (9 de Diciembre de 2020). Obtenido de <https://news.microsoft.com/es-xl/microsoft-anuncia-transforma-chile-para-acelerar-el-crecimiento-y-la-transformacion-de-los-negocios-incluyendo-una-nueva-region-de-datacenter-el-compromiso-de-capacitar-a-mas-de-180-000-personas/>

Ministerio de Economía. (2014). Ley N° 19.799. Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=196640>

Ministerio de Hacienda & Superintendencia de Bancos e Instituciones Financieras. (2017). Circular Bancos N° 3.629. Obtenido de <https://www.bcn.cl/leychile/navegar?i=1113077>

Ministerio de Justicia. (1993). Ley N° 19.223. Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=30590>

Ministerio de la Secretaría General de la Presidencia. (2018). Ley N° 19.880. Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=210676>

Ministerio de Salud. (2020). Plan Nacional de Telesalud del Perú 2020-2023. Obtenido de <https://www.teleiberoamerica.com/legislaciones/Peru-ResolucionMinisterial-1010-2020-MINSA.pdf>

Ministerio del Trabajo. (2019). Política Pública Teletrabajo. Obtenido de <https://www.mintrabajo.gov.co/relaciones-laborales/derechos-fundamentales-del-trabajo/teletrabajo/politica-publica-teletrabajo>

Ministerio Secretaría General de la Presidencia. (2020). Ley 19.628 - Sobre la protección de la vida privada.





Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=141599>

MinTIC & Ministerio del Trabajo. (2018). Libro Blanco: ABC del teletrabajo en Colombia. Obtenido de [https://www.teletrabajo.gov.co/622/articles-8228\\_archivo\\_pdf\\_libro\\_blanco.pdf](https://www.teletrabajo.gov.co/622/articles-8228_archivo_pdf_libro_blanco.pdf)

MinTIC. (junio de 2020). Estrategia Integral para mejorar las condiciones de prestación de servicios. Obtenido de [https://mintic.gov.co/portal/604/articles-1894\\_estrategia\\_final\\_u20200613.pdf](https://mintic.gov.co/portal/604/articles-1894_estrategia_final_u20200613.pdf)

MinTIC. (Marzo de 2020). MinTIC recomienda las siguientes herramientas virtuales para trabajar en casa. Obtenido de <https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126340:MinTIC-recomienda-las-siguientes-herramientas-virtuales-para-trabajar-en-casa>

MinTIC. (2020). Teletrabajo. Obtenido de <https://mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-571.html>

MinTIC Colombia. (Enero de 2020). Obtenido de [https://www.mintic.gov.co/portal/604/w3-propertyvalue-34313.html?\\_noredirect=1](https://www.mintic.gov.co/portal/604/w3-propertyvalue-34313.html?_noredirect=1)

MinTIC Colombia. (2020). Obtenido de [https://www.mintic.gov.co/portal/604/articles-149186\\_recurso\\_1.pdf](https://www.mintic.gov.co/portal/604/articles-149186_recurso_1.pdf)

Oracle. (2020). Obtenido de <https://www.oracle.com/cl/corporate/pressrelease/fap-cloud-computing-model-public-sector-2020-05-22.html>

PQS. (29 de Agosto de 2020). La nube privada y su aporte a la transformación digital de las empresas. Obtenido de <https://www.pqs.pe/tecnologia/la-nube-privada-su-aporte-la-transformacion-digital-de-las-empresas>

Presidencia de la República de los Estados Unidos Mexicanos. (2013). DECRETO por el que se reforman y adicionan diversas disposiciones de los artículos 6o., 7o., 27, 28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos, en materia de telecomunicaciones. Obtenido de [http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM\\_ref\\_208\\_11jun13.pdf](http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_208_11jun13.pdf)

Presidencia del Consejo de Ministros. (2001). Decreto Legislativo N° 604. Obtenido de <https://leyes.congreso.gob.pe/Documentos/DecretosLegislativos/00604.pdf>

Presidencia del Consejo de Ministros. (2016). Resolución Ministerial N° 004-2016-PCM. Obtenido de [https://cdn.www.gob.pe/uploads/document/file/357224/Resoluci%C3%B3n\\_Ministerial\\_N\\_004-2016-PCM\\_20190902-25578-19siyuu.pdf](https://cdn.www.gob.pe/uploads/document/file/357224/Resoluci%C3%B3n_Ministerial_N_004-2016-PCM_20190902-25578-19siyuu.pdf)

Presidencia del Consejo de Ministros. (2017). Decreto Supremo N° 081-2017-PCM. Obtenido de <https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-la-formulacion-de-un-plan-de-tra-decreto-supremo-n-081-2017-pcm-1552513-1/>

Presidencia del Consejo de Ministros. (4 de Enero de 2018). Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano. Obtenido de [https://www.peru.gob.pe/normas/docs/Lineamientos\\_Nube.PDF](https://www.peru.gob.pe/normas/docs/Lineamientos_Nube.PDF)

PwC. (2020). EL CLOUD SE CONSOLIDA CON LA LLEGADA DE LA PANDEMIA. Obtenido de <https://www.pwc.com/cl/es/prensa/prensa/2020/EL-CLOUD-SE-CONSOLIDA-CON-LA-LLEGADA-DE-LA-PANDEMIA.html>

Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros - SeGDi – PCM. (2018). Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano. Lima.

Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros - SeGDi. (2018). Lineamientos para la Suscripción de un Acuerdo de Nivel de Servicio – ANS.

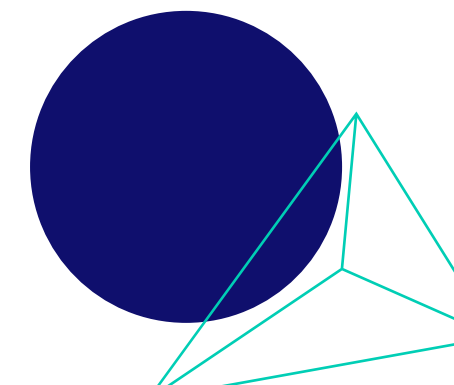
Secretaría de Gobierno Digital Perú. (s.f.). Obtenido de <https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital/>

Talento Digital Chile. (2020). Obtenido de <https://talentodigitalparachile.cl/>

Thompson Reuters. (2020). Obtenido de <https://www.thomsonreutersmexico.com/es-mx/soluciones-de-comercio-exterior/blog-comercio-exterior/cloud-impulsando-la-transformacion-digital>

TicTac. (2020). Recomendaciones para el avance de la política pública de Nube Primero en Colombia. Obtenido de <https://www.ccit.org.co/wp-content/uploads/tictac-2020-politica-publica-de-nube.pdf>

trendTIC. (2020). Obtenido de <https://www.trendtic.cl/2020/11/%EF%BB%BFinfraestructura-en-nube-crecera-26-7-en-america-latina-para-2021-idc/>



## Banda ancha

- BID - OECD. (2016). Broadband Policies for Latin Aamerica and the Caribbean - a Digital Economy Toolkit. Obtenido de [https://read.oecd-ilibrary.org/science-and-technology/broadband-policies-for-latin-america-and-the-caribbean\\_9789264251823-en#page1](https://read.oecd-ilibrary.org/science-and-technology/broadband-policies-for-latin-america-and-the-caribbean_9789264251823-en#page1)
- Bnamericas. (2020). Ericsson prevé despliegues de 5G en Chile y Brasil para 2021. Obtenido de <https://www.bnamericas.com/es/noticias/ericsson-preve-para-2021-despliegues-de-5g-en-chile-y-brasil#:~:text=Chile%20lleva%20a%20cabo%20la,de%20frecuencias%20espec%C3%ADficas%20para%205G.&text=%22En%20el%20caso%20de%20Brasil,principios%20de%202022%22%2C%20>
- Bnamericas. (2020). Perú espera repunte de inversión en telecomunicaciones para 2021. Obtenido de <https://www.bnamericas.com/es/noticias/peru-espera-repunte-de-inversion-en-telecomunicaciones-para-2021>
- Congreso de la República del Perú. (2020). Ley 29904. Ley de promoción de Banda Ancha y construcción de la Red Dorsal de Fibra Óptica. Obtenido de <https://leyes.congreso.gob.pe/Documentos/Leyes/29904.pdf>
- (2013). Constitución Política de los Estados Unidos Mexicanos. Obtenido de [http://www.dof.gob.mx/nota\\_detalle.php?codigo=5301941&fecha=11/06/2013](http://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013)
- CRC. (2019). Comisión de Regulación de Comunicaciones. Obtenido de <https://www.crcm.gov.co/es/noticia/10-cosas-que-debes-saber-sobre-la-nueva-definici-n-de-banda-ancha-en-colombia#:~:text=A%20partir%20de%20enero%20de,nueva%20definici%C3%B3n%20de%20Banda%20Ancha.&text=Con%20la%20medida%2C%20la%20Comisi%C3%B3n,y%20de%2020>
- CRC. (1 de Septiembre de 2020). Comisión Nacional de Regulaciones Colombia. Obtenido de <https://www.crcm.gov.co/es/noticia/crc-publica-el-monitoreo-sobre-tendencias-tecnologicas-globales-y-su-evolucion-reciente>
- El Economista. (2020). Coronavirus erosiona la inversión a infraestructura de telecomunicaciones en México. Obtenido de <https://www.eleconomista.com.mx/empresas/Coronavirus-erosiona-la-inversion-a-infraestructura-de-telecomunicaciones-en-Mexico-20200719-0003.html>
- Forbes México. (5 de Marzo de 2020). Obtenido de [https://www.forbes.com.mx/mexico-entre-los-paises-con-mayor-crecimiento-de-banda-ancha-ocde/#:~:text=M%C3%A9xico%20es%20el%20pa%C3%ADs%20con,el%20Desarrollo%20Econ%C3%B3mico%20\(OCD E\).](https://www.forbes.com.mx/mexico-entre-los-paises-con-mayor-crecimiento-de-banda-ancha-ocde/#:~:text=M%C3%A9xico%20es%20el%20pa%C3%ADs%20con,el%20Desarrollo%20Econ%C3%B3mico%20(OCD E).)

- Gestión Económica Perú. (2020). Osiptel pide a compañías aumentar ancho de banda de internet para facilitar el trabajo remoto. Obtenido de <https://gestion.pe/economia/coronavirus-en-peru-osiptel-pide-a-companias-aumentar-ancho-de-banda-de-internet-para-facilitar-el-trabajo-remoto-video-nndc-noticia/>
- Gobierno de Perú. (23 de Septiembre de 2019). Obtenido de <https://www.gob.pe/institucion/mtc/noticias/51280-mtc-publica-propuesta-para-masificar-el-desarrollo-de-la-banda-ancha>
- GSMA. (2018). Obtenido de <https://www.gsma.com/latinamerica/wp-content/uploads/2018/05/GSMA-MEXICO-AgendaDigital.pdf>
- Ministerio de Transporte y Telecomunicaciones de Chile. (2017). Ley 21046. Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=1111298>
- Ministerio de Transporte y Telecomunicaciones del Perú. (2020). Resolución dictorial N° 126-2020-MTC/27. Obtenido de <https://busquedas.elperuano.pe/normaslegales/asignan-espectro-radioelectrico-en-forma-temporal-a-america-resolucion-directoral-n-126-2020-mtc27-1869813-1/>
- BID - OECD. (2016). Broadband Policies for Latin Aamerica and the Caribbean - a Digital Economy Toolkit. Obtenido de [https://read.oecd-ilibrary.org/science-and-technology/broadband-policies-for-latin-america-and-the-caribbean\\_9789264251823-en#page1](https://read.oecd-ilibrary.org/science-and-technology/broadband-policies-for-latin-america-and-the-caribbean_9789264251823-en#page1)
- Bnamericas. (2020). Ericsson prevé despliegues de 5G en Chile y Brasil para 2021. Obtenido de <https://www.bnamericas.com/es/noticias/ericsson-preve-para-2021-despliegues-de-5g-en-chile-y-brasil#:~:text=Chile%20lleva%20a%20cabo%20la,de%20frecuencias%20espec%C3%ADficas%20para%205G.&text=%22En%20el%20caso%20de%20Brasil,principios%20de%202022%22%2C%20>
- Bnamericas. (2020). Perú espera repunte de inversión en telecomunicaciones para 2021. Obtenido de <https://www.bnamericas.com/es/noticias/peru-espera-repunte-de-inversion-en-telecomunicaciones-para-2021>
- Congreso Perú. (s.f.). Ley 29904. Obtenido de [http://www2.congreso.gob.pe/sicr/cendocbib/con5\\_uibd.nsf/94CE0C5D2DE573AF0525826C0075DCE5/\\$FILE/6\\_Reglamento\\_de\\_la\\_Ley\\_N\\_29904.pdf](http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/94CE0C5D2DE573AF0525826C0075DCE5/$FILE/6_Reglamento_de_la_Ley_N_29904.pdf)
- CRC. (2019). Comisión de Regulación de Comunicaciones. Obtenido de <https://www.crcm.gov.co/es/noticia/10-cosas-que-debes-saber-sobre-la-nueva-definici-n-de-banda-ancha-en-colombia#:~:text=A%20partir%20de%20enero%20de,nueva%20definici%C3%B3n%20de%20Banda%20Ancha.&text=Con%20la%20medida%2C%20la%20Comisi%C3%B3n,y%20de%2020>



El Economista. (2020). Coronavirus erosiona la inversión a infraestructura de telecomunicaciones en México. Obtenido de <https://www.eleconomista.com.mx/empresas/Coronavirus-erosiona-la-inversion-a-infraestructura-de-telecomunicaciones-en-Mexico-20200719-0003.html>

Forbes México. (5 de Marzo de 2020). Obtenido de [https://www.forbes.com.mx/mexico-entre-los-paises-con-mayor-crecimiento-de-banda-ancha-ocde/#:~:text=M%C3%A9xico%20es%20el%20pa%C3%ADs%20con,el%20Desarrollo%20Econ%C3%B3micos%20\(OCD E\)](https://www.forbes.com.mx/mexico-entre-los-paises-con-mayor-crecimiento-de-banda-ancha-ocde/#:~:text=M%C3%A9xico%20es%20el%20pa%C3%ADs%20con,el%20Desarrollo%20Econ%C3%B3micos%20(OCD E)).

Gestión Económica Perú. (2020). Osiptel pide a compañías aumentar ancho de banda de internet para facilitar el trabajo remoto. Obtenido de <https://gestion.pe/economia/coronavirus-en-peru-osiptel-pide-a-companias-aumentar-ancho-de-banda-de-internet-para-facilitar-el-trabajo-remoto-video-nndc-noticia/>

Gobierno de Perú. (23 de Septiembre de 2019). Obtenido de <https://www.gob.pe/institucion/mtc/noticias/51280-mtc-publica-propuesta-para-masificar-el-desarrollo-de-la-banda-ancha>

GSMA. (2018). Obtenido de <https://www.gsma.com/latinamerica/wp-content/uploads/2018/05/GSMA-MEXICO-AgendaDigital.pdf>

IFT. (2017). Instituto Ffederal de Telecomunicaciones. Obtenido de <http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/11337/documentos/marcoreferenciaban daancha23nov17.pdf>

IFT. (2020). Obtenido de <http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/crece-23-la-inversion-en-infraestructura-de-telecomunicaciones-durante-2019-comunicado-472020-1-de>

Ley 1978 de 2019. (s.f.). Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=98210#:~:text=La%20presente%20Ley%20tiene%20por,cierre%20efectivo%20de%20la%20brecha>

Ley 29904. Ley de promoción de Banda Ancha y construcción de la Red Dorsal de Fibra Óptica. (Mayo de 2020). Obtenido de [https://leyes.congreso.gob.pe/Documentos/2016\\_2021/Proyectos\\_de\\_Ley\\_y\\_de\\_Resoluciones\\_Legislativas/PL05398-20200601.pdf](https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL05398-20200601.pdf)

Ley Chile. (s.f.). Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=1111298>

Ley de Banda Ancha Perú. (2015). Obtenido de [http://transparencia.mtc.gob.pe/idm\\_docs/normas\\_legales/1\\_0\\_3532.pdf](http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_3532.pdf)



Ley Federal de Telecomunicaciones y Radiodifusión. (2020). Obtenido de [http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR\\_240120.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_240120.pdf)

MinTIC. (2020). Esquema de subsidios para internet en estratos 1 y 2. Obtenido de <https://www.mintic.gov.co/portal/inicio/Iniciativas/Servicios/Esquema-de-subsidios-para-internet-en-estratos-1-y-2/>

MinTIC. (11 de diciembre de 2020). MinTIC publica la Agenda de Inversión para la vigencia 2021. Obtenido de <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/160805:MinTIC-publica-la-Agenda-de-Inversion-para-la-vigencia-2021>

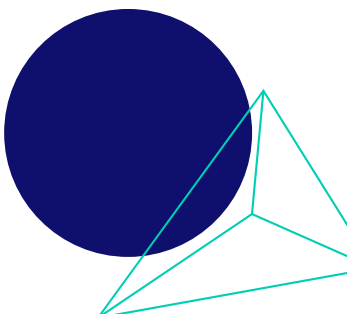
Resolución Ministerial N° 810-2019 MTC/01.03 Perú. (s.f.). Obtenido de <https://www.actualidadgubernamental.pe/norma/resolucion-ministerial-810-2019-mtc-0103/604057b0-863c-4aa4-a74e-c2433372e976>

SCT - IFT. (s.f.). Convenio Marco de Colaboración Internacional. Obtenido de <http://www.ift.org.mx/sites/default/files/industria/politica-regulatoria/convenio-marco-de-colaboracion-sct-ift-1.pdf>

SUBTEL. (22 de Julio de 2020). Secretaría de Telecomunicaciones. Obtenido de <https://www.subtel.gob.cl/subtel-define-nuevos-estandares-de-calidad-para-el-servicio-de-acceso-a-internet/>

Subtel Chile. (2017). Obtenido de <https://www.subtel.gob.cl/subtel-y-municipalidad-de-renca-impulsaran-proyectos-piloto-para-implementar-banda-ancha-comunitaria/>

WiFiChileGob. (s.f.). Obtenido de <http://www.wifigob.cl/>



Alianza Chilena de Ciberseguridad. (s.f.). Obtenido de <https://alianzaciberseguridad.cl/>

Asobancaria. (s.f.). Obtenido de <https://www.asobancaria.com/csirt/>

BID. (2020). Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe. Obtenido de <https://publications.iadb.org/en/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>

colCERT. (s.f.). Obtenido de <http://www.colcert.gov.co/>

ComexPerú. (Agosto de 2020). Obtenido de <https://www.comexperu.org.pe/articulo/la-ciberseguridad-en-el-peru-reto-para-la-transformacion-digital>

Congreso de Perú. (s.f.). Política Nacional de Ciberseguridad. Obtenido de [http://www2.congreso.gob.pe/sicr/cendocbib/con5\\_uibd.nsf/A36311FB344A1DC7052583160057706D/\\$FILE/Pol%C3%ADtica\\_Nacional\\_de\\_Ciberseguridad\\_peru.pdf](http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf)

Congreso Nacional Chile. (2017). Obtenido de [https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA\\_NACIONAL\\_DE\\_CIBER.pdf](https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf)

CONPES 3995. (Julio de 2020). Obtenido de <https://www.csirtasobancaria.com/publicaciones/conpes-3995-politica-nacional-de-confianza-y-seguridad-digital>

Convenio Budapest. (2001).

Decreto Legislativo N° 1412. (s.f.). Obtenido de <https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1/>

Decreto Supremo - N° 106-2017-PCM. (s.f.). Obtenido de <https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-para-la-identificacion-decreto-supremo-n-106-2017-pcm-1585361-1/>

Derecho Digitales; Red en Defensa de los Derechos Digitales. (2018). México y el Convenio de Budapest: Posibles incompatibilidades. Red en Defensa de los Derechos Digitales. Obtenido de [https://www.derechosdigitales.org/wp-content/uploads/minuta\\_r3d.pdf](https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf)

El Economista. (2020). Obtenido de <https://www.eleconomista.com.mx/tecnologia/La-Estrategia-Nacional-de-Ciberseguridad-de-Mexico-debe-trascender-del-papel-OEA-y-BID-20200831-0054.html>

El Economista. (2020). Obtenido de <https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html>

En TIC confío. (s.f.). Obtenido de <https://www.enticconfio.gov.co/>

Foro Jurídico México. (22 de Septiembre de 2020). Obtenido de <https://forojuridico.mx/ley-de-ciberseguridad-en-mexico-un-aspecto-clave-para-regular-la-vida-digital/>

Gobierno de México. (s.f.). Obtenido de [https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia\\_Nacional\\_Ciberseguridad.pdf](https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf)

Hootsuite, We are Social. (2021). Digital Report Chile. Obtenido de <https://datareportal.com/reports/digital-2021-chile>

Hootsuite, We are Social. (2021). Digital Report Colombia. Obtenido de <https://datareportal.com/reports/digital-2021-colombia>

Hootsuite, We are Social. (2021). Digital Report Mexico. Obtenido de <https://datareportal.com/reports/digital-2021-mexico>

Hootsuite, We are Social. (2021). Digital Report Perú. Obtenido de <https://datareportal.com/reports/digital-2021-peru>

[http://documentostics.com/documentos/convenio\\_cibercriminalidad.pdf](http://documentostics.com/documentos/convenio_cibercriminalidad.pdf). (s.f.). Obtenido de <https://www.redipd.org/es/tribuna/colombia-y-el-convenio-de-budapest-contr-el-ciberdelito>

Instituto Federal de Telecomunicaciones. (2018). Plan de acción en materia de ciberseguridad.

ITU. (2015). Obtenido de <https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/11B.pdf>

Ley 1928 de 2018. (s.f.). Obtenido de <http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf>



Ley 21180. (2019). Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=1138479>

Ley Federal de Protección de Datos en Posesión de Particulares. (2010). Ley Federal de Protección de Datos en Posesión de Particulares. Obtenido de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (2017). Obtenido de [https://www.dof.gob.mx/nota\\_detalle.php?codigo=5469949&fecha=26/01/2017#:~:text=%2D%20Se%20ex%20pide%20la%20Ley%20General,en%20Posesi%C3%B3n%20de%20Sujetos%20Obligados.&text=Tiene%20por%20objeto%20establecer%20las,en%20posesi%C3%B3n%20de%20sujetos%20obligado](https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017#:~:text=%2D%20Se%20ex%20pide%20la%20Ley%20General,en%20Posesi%C3%B3n%20de%20Sujetos%20Obligados.&text=Tiene%20por%20objeto%20establecer%20las,en%20posesi%C3%B3n%20de%20sujetos%20obligado)

Ley N° 30618. (s.f.). Obtenido de <https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legislativo-n-30618-1548998-4/>

Mancera Espinosa, M. Á. (2020). Proyecto de Decreto Ley Nacional de Ciberseguridad. Obtenido de [http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun\\_4064516\\_20200902\\_1599062884.pdf](http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf)

Ministerio del Interior y Seguridad Pública. (2020). Estrategia Nacional de Ciberseguridad. Obtenido de <https://www.camara.cl/verDoc.aspx?prmID=176320&prmTIPO=DOCUMENTOCOMISION>

MinTIC. (s.f.). Obtenido de <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

PeCERT. (s.f.). Obtenido de <https://www.pecert.gob.pe/>

Statista. (2021). Obtenido de <https://es.statista.com/estadisticas/1067800/poblacion-total-de-america-latina-y-el-caribe-por-subregion/>

TicTac. (2020). Ciberseguridad en Entornos Cotidianos. Obtenido de <https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-entornos-cotidianos-vfene-1.pdf>

TicTac. (2020). Informe Tendencias Ciberdelincuencia. Obtenido de <https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-entornos-cotidianos-vfene-1.pdf>

XMS. (2020). Obtenido de <https://www.xms.cl/ciberseguridad-en-chile-2020/#:~:text=Ciberseguridad%20en%20Chile%3A%20525%20millones%20de%20ciberataques%20en%20el%20primer%20semestre%202020,-2%20noviembre%2C%202020>

