NATIONAL CYBERSECURITY STRATEGY

Mexico 2017

CONTENT

EXECUTIVE SUMMARY

The National Cybersecurity Strategy is the document that establishes the vision of the Mexican State in the matter, based on the acknowledgement of:

A. The importance of the information and communication technologies (ICTs) as a political, social and economic development factor in Mexico, in the understanding that more individuals are connected to the Internet and that both private and public organizations develop their activities in cyberspace.
B. The risks associated with the use of technologies and the growing number of cybercrimes.
C. The need for a general cybersecurity culture.

The increase of risks, threats and sophisticated computer attacks, the emergence of new ways and techniques to exploit vulnerabilities, and the increase of criminal conduct occurring through ICTs make cybersecurity a complex issue. Also, the global nature of cyberspace and the concurrence of different sovereignties and legal frameworks complicate matters more.

In economic terms, according to the Latin American and Caribbean Cybersecurity Trends report[1], cybercrime costs to the country between 3 and 5 billion dollars a year. In addition, it is noted that the risks and threats in cyberspace are global threats that have become more evident at different dialogue and cooperation spaces and mechanisms.

The risks and threats in cyberspace may become a possible attack on human dignity, on the integrity of people, on the credibility, reputation and assets of companies and public institutions, and have effects on public safety or even national security.

Several countries have developed cybersecurity strategies, in line with their own circumstances, their economic, social and political capacity. Some of the different global strategies are already at an advanced stage of maturity, implementing their second or third version, with years of experience, and with institutions and resources. Other countries have had their cybersecurity strategy published only for a few years or even months. The different progress levels of the countries and their cybersecurity strategies underscore the need and importance of positively impacting individuals, private organizations, academia and government institutions with concrete cybersecurity actions.

[1] See OAS Report: Latin American and Caribbean Cybersecurity Trends available on the website https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern% C3% A9tica% 20in% 20Am% C3% A9rica% 20Latina% 20y% 20el% 20Caribe.pdf consulted in October 2017.

The National Cybersecurity Strategy (ENCS, for short in Spanish acronym) defines objectives and cross-cutting themes, sets out the guiding principles, identifies the different stakeholders involved and gives clarity on the articulation of efforts between individuals, civil society, private, and public organizations in the field. It also presents the governance model for the strategy's implementation, monitoring and evaluation.

In Mexico, the Federal Government, in its role as facilitator, promoted spaces for dialogue, discussion, and learning through different fora and workshops in a collaborative process called "Towards a National Cybersecurity Strategy". The workshops took place between March and October 2017. During these meetings, the different stakeholders shared ideas, concerns and proposals on cybersecurity which showed great coincidences on the elements that the Strategy should address, such as the need:

- To articulate the development of cybersecurity actions that serve individuals, companies, and public agencies of the Mexican State.
- To collaborate and cooperate across the different sectors as a key element for the development, monitoring and evaluation of the strategy.
- To learn the dimension of risks and threats in cyberspace, the state of cybersecurity in the country, the development of a national assessment, as well as to obtain evidence to improve decision making processes on cybersecurity.
- To consider the global context as part of the challenge, and diplomacy as a way to establish dialogue and agreements to address cybercrimes, risks and threats.
- To develop specialized human capital in cybersecurity matters.
- To promote the responsible use of ICTs and reinforce a culture of cybersecurity that includes awareness, education, and training.

In the case of Mexico, although it is true that there was no strategy *per se*, during the current administration actions were taken by the Government here were exercises and valuable efforts in the matter by the civil society, private organizations, academia, technical community and public agencies across the different powers and levels of government.

The **general objective** of the National Cybersecurity Strategy is to identify and establish cybersecurity actions for the social, economic, and political spheres, so both private and public organizations use and take advantage of ICTs in a responsible manner and contribute to the sustainable development of Mexico.

To achieve the general objective, **5 strategic objectives** have been established for:

1. Society and Rights
2. Economy and Innovation
3. Public Institutions
4. Public Security
5. National Security

Three **guiding principles** have been considered for the development of the ENCS:

A. A Human Rights Perspective
B. A Risk-Management Approach
C. Multidisciplinary and Multi-Stakeholder Collaboration

To achieve the strategic objectives, **8 cross-cutting pillars** will be developed for:

1. Cybersecurity Culture
2. Capacity Building
3. Coordination and Collaboration
4. ICT Research, Development and Innovation
5. Standards and Technical Criteria
6. Critical Infrastructure
7. Legal Framework and Self-Regulation
8. Measurement and Monitoring

In an initial stage, the Interministerial Commission for the Development of the Electronic Government (CIDGE, for short in Spanish) through the Subcommittee on Cybersecurity will be in charge of coordinating the Federal Government entities and articulating the efforts of the different actors for the implementation and monitoring of the strategy.

The success of ENCS relies on the collaboration of the different stakeholders and in the shared responsibility for ICT adoption and use. This is a live document that aims to be constantly updated as required.

RATIONALE

The National Cybersecurity Strategy is based on the 2013-2018 National Development Plan. It is also cross-cutting, contributing significantly towards achieving the objectives of the "2013-2018 Program for an Approachable and Modern Government", the "2014-2018 National Public Security Program" and the "2014-2018 National Security Program".

Given the increasingly widespread use of ICTs in the daily activities of individuals, private, and public organizations; its importance as a factor of political, social and economic development; the economic value of the information; and the inherent risk of the use of technology, it is imperative to have a National Cybersecurity Strategy for Mexico, that articulates the actions directed to individuals, private organizations, and public institutions.

The trend of digitalization results in more people using technology, more services being connected to the Internet and depending on information systems for their operation, which means that vulnerabilities, risks, and threats increase.

The International Telecommunications Union has indicated in several reports that cyber-attacks increased by 30% between 2011 and 2012, affecting 550 million people worldwide and causing economic losses of 110 billion dollars.

The Cybersecurity Capacity Maturity Model developed in the 2016 Cybersecurity Report: *Cybersecurity - Are We Ready in Latin America and the Caribbean?*[2] underlines that cybercrime costs the world up to US $ 575 billion per year, which represents 0.5% of the global gross domestic product. That is almost four times more than the annual amount for international development aid. In Latin America and the Caribbean, this type of crimes cost around 90 US billions per year. With these resources we could quadruple the number of scientific researchers in our region.

Regarding the *2014 Latin American and Caribbean Cybersecurity Trends*[3] report sponsored by the Organization of American States (OAS), it is estimated that the costs inherent to cybercrime around the world amounted to 113 billion US dollars and, 3 billion dollars only for Mexico.

---

[2] Inter-American Development Bank, IDB, 2016; Cybersecurity Are we ready in Latin America and the Caribbean? available at: https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

[3] See OAS Report on Latin American and Caribbean Cybersecurity Trends, available on the website https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern% C3% A9tica% 20in% 20Am% C3% A9rica% 20Latina% 20y% 20el% 20Caribe.pdf

In Mexico, Internet users have increased from 40 to 65.5 million in just 4 years (2012 to 2016). According to the recent study: Habits of Internet Use in Mexico of the Mexican Internet Association [4], up to 70 million Internet users have registered in Mexico in 2016.

The Federal Police, through its Scientific Division, promoted a Cybersecurity Strategy to strengthen, among other topics, social awareness on the responsible use of ICTs. With the strategy, the Scientific Division has managed to respond to more than 51,000 citizen complaints and more than 200,000 cyber incidents. Nearly 17,000 fraudulent websites have been deactivated and more than 2,000 cybersecurity alerts have been issued to public and private institutions.

The National Commission to Protect and Defend Financial Services Users (CONDUSEF, for short in Spanish) states that[5]: during the first quarter of 2011 cyber-fraud increased from 7% (38,539 complaints) of claims of possible fraud, to 42% (639,857 complaints) in the same period in 2017. The amount claimed in the first quarter 2017 amounts to 1.16 billion pesos, of which 53% of the total was paid, and 90% of the issues were resolved in favor of the user. Regarding the sector with the most cyber-fraud, 91% is for e-commerce. Likewise, the increase in online transactions for individuals and mobile banking (167% and 74% respectively) is noteworthy, when compared to the previous year. The average monthly e-commerce cyber-fraud in 2017 was 193,000 cases, when, in the previous year, it was only 131,000. As for mobile banking cyber-fraud, a historical figure occurred in March 2017, with 3,682 cases.

It is clear that only the sum of the efforts of all those involved in cybersecurity will allow designing and building the foundations around the use and exploitation of ICTs in a free, responsible and reliable environment that will enable the development of capacities, taking advantage of opportunities and the economic, political, and social growth of the population.

---

[4] See Mexican Internet Association, Habits of Internet Use in Mexico 217 https://www.asociaciondeinternet.mx/es/

[5] See CONDUSEF, https://www.gob.mx/cms/uploads/attachment/file/240895/RECLAMACIONES_IMPUTABLES_A_UN_POSIBLE_FRAUDE_2011-2017_ver5.pdf

INTRODUCTION

Considering that the activities performed in cyberspace also have an impact on the tangible world, it is urgent to develop a framework of reference in cybersecurity, in order to promote technological and economic innovation in the country, while contributing to the strengthening of institutions and with full compliance and respect for human rights. The ENCS is the strategic document of the Mexican State regarding cybersecurity.

The complexity and transnational nature of the dynamics of the digital era involve the need to address cybersecurity in a comprehensive, collaborative, holistic and cross-cutting manner. The goal is that any effort addressing this phenomenon should evolve over time, always focusing on the joint effort of all sectors.

The National Cybersecurity Strategy seeks to contribute to the sustainable development of Mexico, based on several guiding principles in connection to cybersecurity:

A. A Human Rights Perspective
B. A Risk-Management Approach
C. Multidisciplinary and Multi-Stakeholder Collaboration

In a first phase, the National Cybersecurity Strategy briefly addresses the international context of cybersecurity, describing the different international scenarios and mechanisms, both binding and non-binding, which are related to the subject and where the Mexican State participates. The purpose is to show the relevance of cybersecurity on the international agenda, where our country is an important actor.

Later, the national context is developed, indicating the digital development of the country, the telecommunications sector and Internet users, as well as some necessary references that have been developed in Mexico regarding cybersecurity.

The main part of this document describes the strategic objectives and cross-cutting pillars. On the one hand, the aforementioned strategic objectives constitute the five realms to be protected and from which general actions are derived to benefit civil society, the private sector, public institutions and the academic and technical communities, bearing in mind the particularities of each of these actors.

Together with the five strategic objectives, eight cross-cutting pillars are proposed, as the backbone of the National Cybersecurity Strategy. These will also serve as a basis for the development of the corresponding implementation plan.

The institutional framework is also considered, which will be part of the cybersecurity governance model. It shows how the Government will coordinate the issue of cybersecurity through the competent agencies, so that the cooperation and

participation channels of the multiple stakeholders interested in the subject will be established in the future.

INTERNATIONAL CONTEXT

The lack of a cybersecurity culture and responsibility in the use of ICTs can create constant risks and threats in cyberspace. The vulnerability of information systems can seriously affect people, their information, their assets, their reputation and even their dignity. Globalization and hyperconnectivity demand solutions focused on international collaboration in a precise, efficient, and effective manner.

Given the complexity of society in the digital age and the challenges posed by the use and exploitation of ICT in the information society, it is important to raise the issue of cybersecurity from an international context perspective. Within the **United Nations** (UN), the **World Summit on the Information Society** (WSIS) promotes a people-centered vision,[6] both in its first two phases, carried out in 2003 and 2005, as in the process of reviewing the implementation of its results, in 2015.[7]

The **Group of Governmental Experts** (GGE)[8] was created to analyze the threats, challenges and dimensions of cybersecurity, as well as to consolidate recommendations and guidelines on the peaceful use of ICTs, the application of international law in cyberspace, voluntary standards, measures for the promotion of trust and stability, and the strengthening of national capacities. Mexico is part of the GGE.

The **Commission on Crime Prevention and Criminal Justice** (CCPCJ) prepared a study on cybercrimes, which seeks to strengthen the exchange of experiences and good practices and generate opportunities for cooperation and technical assistance for tactical and operational support to the States against criminal uses of ICT, including the Internet.[9]

---

[6] World Summit on the Information Society, Geneva Declaration of Principles, Document WSIS-03/Geneva/4-S (May 12, 2004), paragraph 1, available at: http://www.itu.int/net/wsis/docs/geneva/official/dop-en.html

[7] Resolution 70/125 of the General Assembly of the United Nations, paragraphs 48 to 54.

[8] By Resolution: Developments in the field of information and telecommunications in the context of international security, available at: https://www.un.org/disarmament/es/los-avances-en-la-informatizacion- and-telecommunications-in-the-international-security-context/

[9] United Nations Office on Drugs and Crime, Doha Declaration - Report of the 13th United Nations Congress on Crime Prevention and Criminal Justice (July 2015), see: http://www.unodc.org/documents/congress//Declaration/V1504154_English.pdf

The **Internet Governance Forum** (IGF) has included the Best Practice Forums[10] on cybersecurity issues since 2014. Mexico hosted the IGF meeting in 2016, where cybersecurity was considered a multifactorial phenomenon that is and will be a key element for sustainable development.

The **International Telecommunication Union** (ITU) develops the Global Cybersecurity Index, a survey[11] that measures the commitment of countries on the subject on three categories. Mexico, like other 76 countries, is in a "maturing" stage and only 21 countries are in the "leading" stage.

Within the framework of the **Organization for Economic Co-operation and Development** (OECD) in the 2016 Digital Economy Ministerial Meeting, the participating countries committed to collaborating to take advantage of the digital economy potential.[12] Regarding cybersecurity, Mexico, together with 40 other countries, endorsed the following 3 factors:

1. Reduce impediments to e-commerce within and across borders
2. Develop global technical standards that enable interoperability and a secure, stable, open, and accessible Internet
3. Develop, with decision-makers, privacy and data protection strategies, emphasizing transparency in the public sector.

The **Inter-American Development Bank** (IDB), with the **Organization of American States** (OAS) and the Global Cyber Security Capacity Centre (GCSCC) of the **University of Oxford**, published the document *Cybersecurity: Are We Ready in Latin America and the Caribbean?*[13], which places Mexico at a low implementation level in the components of Policy and Strategy, and Technologies.[14]

In the OAS, the cybersecurity program of the **Inter-American Committee Against Terrorism** (CICTE), leads the hemispheric platform for international cooperation and technical assistance in cybersecurity. Recently, the OAS agreed to the creation of a Working Group on Confidence-Building Measures in Cyberspace, which seeks to

---

[10] Best Practice Forums, available at: http://intgovforum.org/multilingual/content/best-practice-forums-4

[11] International Telecommunication Union, Global Cybersecurity Index 2017 (July 19, 2017), available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017 -R1-PDF-E.pdf

[12] Organization for Economic Co-operation and Development, Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (June 23, 2016), available at: http://www.oecd.org/centrodemexico/medios/declaracion-ministerial -sbore-the-digital-economy.htm

[13] Inter-American Development Bank and the Organization of American States, Cybersecurity: Are we Ready in Latin America and the Caribbean? (March 14, 2016), available at: https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

[14] Its content will be updated by the end of 2017, which would give space to evaluate progress after the definition of the ENCS.

create tools that take into consideration the international progress of the UN GGE, or of other fora, adjusting them to the needs and interests of the region.

In Latin America, the **Digital Agenda for Latin America and the Caribbean** (eLAC) has five implementation pillars.[15] The "Governance for the Information Society" pillar highlights "Objective 19: Promotion of security, privacy, data protection and trust in the use of the Internet" and "Objective 20: Preventing and addressing cybercrime through cybersecurity strategies and policies. Coordinate among response teams at the local and regional level during events."

Within the framework of the **Pacific Alliance**, the Digital Agenda was approved in December 2016 with the following precept: "Enhance cooperation in digital security and confidence-building in the use of ICTs".[16] This agenda has a road map featuring four tracks: 1. Digital Economy; 2. Digital Connectivity; 3. Digital Government, and; 4. Digital Ecosystem, which seek to improve the competitiveness of the countries that comprise it through ICTs and the promotion of the digital economy.

As for the **World Economic Forum** (WEF), it defines resilience and cybersecurity as key conditions for technological and economic development. In 2016, the Council of the Global Cybersecurity Agenda published its white paper detailing the obstacles in the public and private sectors, which hinder collaboration and the adoption of best practices in cybersecurity.[17] In addition, its Global Risks Report 2017 identified the massive data theft and cyber-attacks in the risk scenario for that year, also pointing out the challenge of emerging technologies in terms of governance.[18]

In the case of the **Internet Corporation for Assigned Names and Numbers** (ICANN), the organization has support entities and advisory committees with working groups on different topics, including cybersecurity. National authorities participate through the Governmental Advisory Committee; and work related to security issues in the management of single Internet identifiers is carried out through the Public Safety Working Group[19] of the aforementioned committee.

In terms of Internet governance, cybersecurity is also discussed. In addition to the work of the Internet Governance Forum (IGF), national and regional efforts are undertaken by the multi-stakeholder community. The IGF Latin American and Caribbean Regional

---

[15] Economic Commission for Latin America and the Caribbean, Digital Agenda for Latin America and the Caribbean (eLAC2018), (August 7, 2015), available at: http://repositorio.cepal.org/handle/11362/38886

[16] Pacific Alliance, Cali Declaration, (June 30, 2017), Annex I, paragraph 8, available at: https://alianzapacifico.net/?wpdmdl=9850

[17] World Economic Forum, Global Agenda Council on Cybersecurity, White Paper, April 2016, available at: http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

[18] World Economic Forum, The Global Risks Report 2017, January 2017, available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf

[19] Internet Corporation for Assigned Names and Numbers, GAC Public Safety Working Group, available at: https://gacweb.icann.org/display/gacweb/GAC+Public+Safety+Working+Group

Preparatory Meeting (LACIGF) is the arena for the different actors to touch on policy issues related to the Internet from a regional perspective. It has been held annually since 2008.[20] At the local level there are Dialogues on Internet Governance, which started in 2013.

The international trend in this matter indicates that cyber incidents and attacks are increasing in frequency, degree of affectation, and sophistication. Governments and businesses globally recognize the need for more robust information security and cybersecurity frameworks, measures and capacities, as well as cooperation and information exchange, to cope with the growing number of cyber-attacks, threats and risks in cyberspace, as well as the prevention and response to crimes that are committed through ICTs or against ICTs.

In this context, the International Telecommunications Union has indicated in several reports that cyber-attacks increased by 30% between 2011 and 2012, affecting 550 million people worldwide and causing economic losses of 110 billion US dollars.

[20] Preparatory Meeting for the Internet Governance Forum (LACIGF), available at: https://lacigf.org/

NATIONAL CONTEXT

As in most countries, the use of information and communication technologies in Mexico has increased in recent years thanks to the development of the telecommunications sector, the promotion of private investment, and economic and political stability in the international sphere; in addition to the public policies and the institutional and legal framework that favor Mexico's digitalization.

This widespread use and the different economic, political and sociocultural factors have led to the fact that in Mexico, according to data of the National Institute of Statistics and Geography (INEGI, for short in Spanish)[21]: during the second quarter of 2016, 59.5% of the population aged six or more declared being an Internet user. 68.5% of Mexican Internet users are younger than 35 years old. 47.0% of households in the country have Internet connection. Internet use is associated with higher levels of education: at higher education level, higher Internet use. Internet is used mainly as a means of communication, to obtain information in general and for the consumption of audiovisual content. Cellular phone users represent 73.6% of the population aged six years or older, and three of every four users have a smartphone.

Within the framework of the **2013-2018 National Development Plan**, in the **2013-2018 Program for an Approachable and Modern Government**, the **National Digital Strategy** was established with the purpose of promoting the digitalization of Mexico, through actions such as: digital government, open data, inclusion and digital skills, health and education services through ICTs, the use of ICTs in financial services, among others. It is important to strengthen cybersecurity so that all public services, mainly digital and people's rights to them, are carried out without barriers, in a reliable and resilient manner, with the aim of strengthening trust in ICT use and the relationship between public institutions, among the private sector and society

During 2017, the private sector report called Cybersecurity Assessment in Mexico: Gaps and Recommendations in a Hyper-Connected World produced some relevant findings such as:[22]

- The need to have a National Cybersecurity Agency to coordinate the strategy that is being defined, and to create the critical governance path on the

[21] Overview of Internet access and other ICTs in households. INEGI, 2017. Available at: http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf

[22] Last October, the Mexican Chamber of Electronics, Telecommunications and Information Technologies (CANIETI), together with the Mexican Information Technology Industry Association (AMITI) and the Mexican Internet Association, presented the results of the study called "Cybersecurity Assessment in Mexico: Gaps and Recommendations in a Hyper-Connected World", information available on CANIETI's Internet site: http://www.canieti.org/Comunicacion/prensa/boletinesdeprensa/Presentaindustria.aspx

Internet, and also to contribute to promoting certainty and trust in the new digital ecosystem.

- The importance of redefining the legal framework for cybersecurity, harmonizing federal and state-level legislation, guaranteeing the protection of personal data and stimulating information sharing. A framework to provide the police forces with adequate tools
- Guarantee the protection of critical infrastructure, especially cyber-resilience under a risk management approach to have clear mechanisms and protocols available for system recovery
- The development of skills and competences for the new digital ecosystem, clearly defining the new skills that will be needed, expanding, developing and recruiting the best possible talent

On the other hand, according to the same study of the private sector, the most important gaps of Mexican organizations are: "information classification, cybersecurity metrics, business continuity training and cyber resilience, as well as vulnerability testing by third parties" [23]:

> "In addition, large organizations have a greater perception of risk; they are oriented towards digital transformation; they are aware of threats and the need to act against them; but, above all, they have a high perception that they can be violated. This leads them to adopt the best practices in cybersecurity."
>
> "Among the main findings, only 65.3% of participating organizations consider themselves fairly prepared to face the threats and 59.7% said that digital transformation is necessary for the success of the business strategy. For 57.7% of participants, the areas of Operations, Finance and Brand Reputation are the most impacted in case of an attack. 47.54% considers that there is an alarming increase of new and more complex threats, which is why they are acting on the subject; and 46.7% indicated that there is an average probability that their digital assets will be stolen or damaged".

On the other hand, in order to contribute to the National Goal of "Mexico: a Country in Peace" in the 2013-2018 National Development Plan, the Federal Police, through its Scientific Division, has responded to more than 51,000 citizen complaints and more than 200,000 cyber incidents. Nearly 17,000 fraudulent websites have been disabled and more than 2,000 cybersecurity alerts have been issued to public and private institutions.

The National Cybersecurity Strategy is cross-cutting and articulated with other programs and strategies, following the provisions in the 2013-2018 National

---

[23] See the study "Cybersecurity Assessment in Mexico: Gaps and Recommendations in a Hyper-Connected World", information available on the CANIETI website: http://www.canieti.org/Comunicacion/prensa/present-boletines/Presentaindustria.aspx

Development Plan, in accordance with the values and principles established by the Political Constitution of the United Mexican States.

Political Constitution of the United Mexican States		
2013 – 2018 NATIONAL DEVELOPMENT PLAN		
2013-2018	2014-2018	2014-2018
Program for a Modern Government (PCMG)	**National Public Security Program** (NPSP)	**National Security Program**
ENCS		

NATIONAL CYBERSECURITY STRATEGY

Vision

By 2030 Mexico will be a resilient nation against the risks and threats of cyberspace, responsibly using the potential of ICTs for sustainable development in a reliable environment for all.

General Objective

To strengthen cybersecurity actions applicable to the social, economic and political spheres that allow the population, public and private organizations a responsible use and exploitation of ICTs for the sustainable development of Mexico.

Principles

The strategy considers the following guiding principles:

A. **A Human Rights Perspective**
To consider, in the different cybersecurity actions the promotion, respect and fulfillment of human rights, among which the freedom of expression, access to information, respect for privacy, protection of personal data, health, education, and work are included

B. **A Risk-Management Approach**
To have the ability to handle uncertainty scenarios through preventive and corrective approaches, with the intention of minimizing the impact of the changing threats and risks of cyberspace.

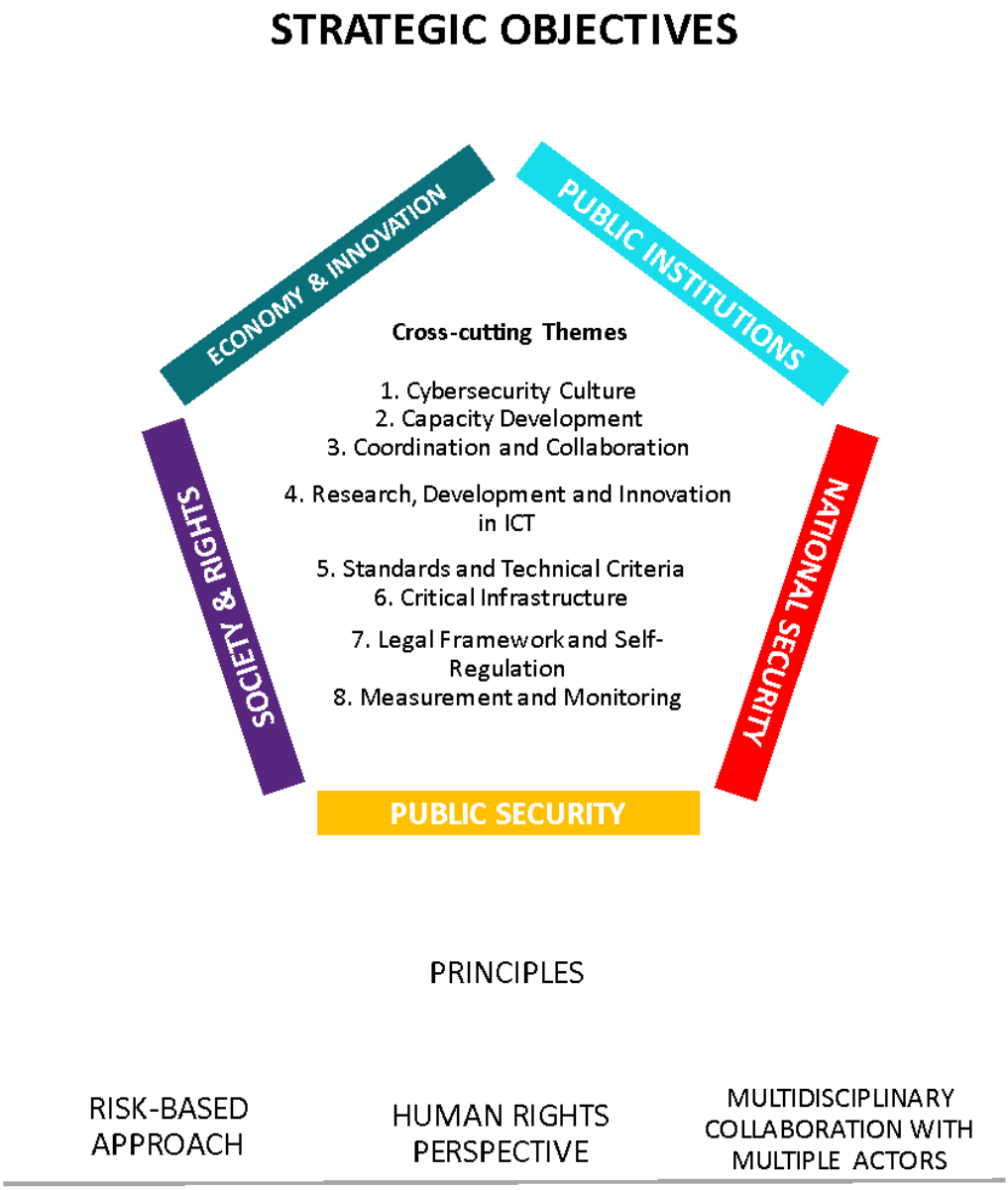
C. **Multidisciplinary and Multi-Stakeholder Collaboration**
To have a multidisciplinary collaboration approach of the different stakeholders (actors and sectors), with an Internet governance focus on cybersecurity, enabling the comprehensive, cross-cutting, and holistic development of the strategy while facilitating their open and transparent participation.

Structure of the National Cybersecurity Strategy

The National Cybersecurity Strategy is the document that reflects the general actions that must be developed by the Mexican State as a whole; civil society, academia, private sector, and public institutions, to achieve the maximum benefit of ICTs in a reliable and resilient environment that translates into benefits for all.

In order to fulfill the general objective, the strategy proposes **5 strategic objectives**, which require the development of **8 cross-cutting pillars** that are articulated, interdependent and contribute to achieving each of the strategic objectives. All the actions of each cross-cutting pillar will be developed following the **3 guiding principles**.

The graphic that follows presents the structure of the National Cybersecurity Strategy:



Strategic Objectives

I. Society and Rights

Create the conditions for the population to carry out activities responsibly, freely, and in a safe manner in cyberspace. Improve the quality of life through digital development, following human rights standards, respecting freedom of speech, privacy, and personal data protection, among others.

II. Economy and Innovation

Strengthen cybersecurity to protect the economy of different sectors of the country and promote technological development and innovation. Boost the national cybersecurity industry, in order to contribute to the economic development of individuals, private organizations, public institutions, and society.

III. Public Institutions

Protect information and computer systems of public institutions to ensure their optimal functioning and the continuity in the provision of services.

IV. Public Security

Improve capacities for the prevention and investigation of criminal behavior in cyberspace that affect people and their assets, with the aim of maintaining order and public peace.

V. National Security

Develop capacities to prevent risks and threats in cyberspace that may alter national sovereignty, integrity, independence, and impact development and national interests.

Crosscutting Pillars

ET 1. Cybersecurity Culture

The set of values, principles and actions defined in terms of awareness, education and training carried out by all stakeholders, and impact the way society interacts in cyberspace moving towards a harmonious and reliable manner, and as a factor for sustainable development.

Cybersecurity culture will promote the fulfillment of the 5 strategic objectives, through the development of public policies, strategies, programs, projects, actions, and initiatives that will:

- Contribute to the promotion, fulfillment, and protection of the rights of individuals, public and private organizations, emphasizing the protection of children and adolescents in cyberspace and their rights
- Promote the responsible use of information and communication technologies, harmonious coexistence and harness the development of activities in cyberspace
- Encourage innovation and the economy for sustainable development
- Strengthen the prevention of risks and criminal behavior that affect individuals, private and public organizations
- Increase trust and continuity of public and private digital services and procedures
- Contribute to the prevention of risks that could affect critical infrastructures of information and operation

ET 2. **Capacity Development**

Set of actions aimed at the creation and strengthening of organizational capacities, human capital and technological resources in cybersecurity, which allow society, academia, private sector and public institutions to have the resources to manage risk and threats in cyberspace, as well as the increase of national resilience.

The development of capacities will aid in the fulfillment of the 5 strategic objectives through the development of public policies, strategies, programs, projects, actions and initiatives that:

- Encourage the development of human capital through the training of:
  i. Cybersecurity specialists and professionals
  ii. Professional leaders of cybersecurity as drivers of strategies and policies
  iii. Research and development professionals for the industry and marketing of cybersecurity
  iv. Professionals in investigation and prosecution of crimes committed through ICTs, as well as in the administration and delivery of justice.
- Establish the organization that should prevail in the public and private sectors in order to:
  i. Position cybersecurity at a strategic level in public and private organizations
  ii. Establish mechanisms for citizen participation in cybersecurity matters
- Generate the necessary technological infrastructure for:

i. The national technological development of cybersecurity and the gradual strengthening of cybersecurity in Mexico
ii. Increase the technical capacities for the identification and management of cyber incidents nationwide

ET 3. **Coordination and Collaboration:**

It is the set of actions aimed at coordinating and establishing the collaboration channels between the different public institutions, academia, civil society and private organizations in the field of cybersecurity, in the different cross-cutting themes, in order to consolidate the cybersecurity ecosystem and obtain the resilient capacity needed to establish preventive, proactive and reactive mechanisms that will provide trust and peace to the population in the use and exploitation of ICTs.

The development of coordination and collaboration actions will support meeting the 5 strategic objectives through the implementation of actions that:

- Strengthen international cooperation and collaboration
- Identify the coordination and cooperation mechanisms among the different actors involved at the national level
- Define and apply the cybersecurity governance model among civil society, private sector, academia and public institutions to share information and best practices in cybersecurity
- Establish protocols and communication channels that strengthen trust, reciprocity, and stimulate social responsibility of all actors

ET 4. **Research, Development and Innovation in ICT**

It is the set of actions aimed at establishing mechanisms to promote research, development and innovation in the use and exploitation of cybersecurity technologies in order to promote the development of human capital and technological innovation in the field and boost the national cybersecurity market that favors the development of capacities and the maturity of the national ecosystem.

The actions derived from research, development and innovation in ICT will allow the consolidation of the 5 strategic objectives through the creation of new models and technology aimed at minimizing the risks and vulnerabilities inherent to the technologies through the:

- Establishment of policies, programs, actions and initiatives that trigger and consolidate the cybersecurity ecosystem in Mexico, among

academia, civil society, the private sector and the public sector to trigger innovation in ICT related to cybersecurity
- Promotion of scientific and technological research that stimulates the development of cybersecurity skills
- Promotion of the national cybersecurity market that favors technological autonomy at the national level and triggers national economy in that sector.

ET 5. **Standards and Technical Criteria**

It is the set of actions focused on the development, adoption and strengthening of standards, technical and standardization criteria in cybersecurity, which admit the homologation and application of best practices and processes in the use and adoption of ICTs in a cybersecurity environment.

The development of standards and technical criteria will help fulfill the 5 strategic objectives through the:

- Establishment of criteria, standards and methodologies for the creation, use and adoption of hardware and software in order to strengthen the cybersecurity ecosystem and reduce risks and vulnerabilities inherent to technology
- Definition of reference frameworks to strengthen the cybersecurity of private and public organizations, academia and society in general
- Promotion of the participation of the academic, technical and scientific community in the development and strengthening of standards, methodologies and standardization in cybersecurity matters
- Identification and, where appropriate, promotion of the use of international standards and best practices in the field of cybersecurity

ET 6. **Critical Infrastructures**

A set of actions aimed at establishing the actions and mechanisms necessary to minimize the likelihood of risks and vulnerabilities inherent in the use of ICTs for the management of critical infrastructures, as well as to strengthen the resilience capacity to maintain the stability and continuity of services in case of a cybersecurity incident.

The set of measures and actions aimed at protecting critical infrastructures will help fulfill the 5 strategic objectives through the development of policies, a human capital development program and actions aimed at:

- The establishment of policies and actions that will be carried out within the framework of the National Cybersecurity Law and other related and applicable provisions in matters of national security and in collaboration with the national security authorities.

ET 7. **Legal Framework and Self-Regulation**

To promote and establish actions and mechanisms necessary for the alignment of the national legal framework connected to cybersecurity and self-regulation by the service providers, permit holders, distributors of ICT services, including the modification in order to provide legal certainty to the actions of Internet intermediaries, and society in general, which facilitates the use and exploitation of ICT and healthy coexistence in cyberspace.

The actions aimed at adapting the national legal framework and the development of self-regulatory mechanisms in the digital era are vital for the development of digitalization in the world and a key for the prevention of risks and threats and the investigation and sanction of criminals in the digital era. In addition, it is key to strengthening trust between society, the private sector and public institutions.

The above will help fulfill the 5 strategic objectives through:

- The development of capacities of legal operators and decision makers in public and private institutions, as well as civil society; on the digital ecosystem, cybersecurity and Internet governance to analyze and propose modifications or legislative harmonization according to the needs of the information society that enables facing risks and threats in cybersecurity
- Legal certainty so that public and private institutions can carry out their tasks in a cooperative environment, where law enforcement agencies increase their effectiveness in the investigation, prevention, prosecution and sanction of cybercriminals
- The analysis and establishment of mechanisms and self-regulation procedures that favor the construction of trust among individuals, the public sector and private organizations adhering to legal provisions
- The standardization and harmonization of criminal codes and complementary laws in relation to cybercrimes, as well as the legal tools available to law enforcement agencies to prosecute them

ET 8. **Measurement and Monitoring**

It is the set of policies and actions aimed at the promotion and development of approved measurement mechanisms that monitor the results obtained from

the implementation of the National Cybersecurity Strategy and its impact on the social and economic development of the country, with the aim of identify areas of opportunity for continuous improvement.

The development of measurement and monitoring mechanisms will help the fulfillment of the 5 strategic objectives through the creation of statistics and indicators for:

- The joint collaboration of actors for the development of methodology for the construction of a national diagnosis of risks and threats in cyberspace
- The establishment of centralized statistics related to the implementation and impact of cybersecurity and the Strategy in the economic, political and social sectors
- Obtaining data for the continuous improvement and updating of the National Cybersecurity Strategy

Scope and Future

The National Cybersecurity Strategy is a document designed to evolve according to the needs of society around cybersecurity, in order to have the capacity to adapt and continuously improve regarding the challenges, risks, threats and vulnerabilities inherent in future technologies and the new social dynamic in the short, medium and long term.

It is also a document that reaffirms the vision that cybersecurity is an enabler for the development of the potential of the country's digitalization and a key piece for the sustainable development of Mexico and the world.

There are risks and threats in cyberspace, and the techniques for malware and criminal behavior also evolve –even faster than public policy or regulation can react– so we must be prepared to know and temper the possible risks that technologies will bring.

The National Cybersecurity Strategy is a live document that will set the path for the development of cybersecurity in Mexico, with a comprehensive, cross-cutting and holistic approach and with the collaboration of the different stakeholders, namely: civil society, public institutions, private sector and technical and academic communities.

INSTITUTIONAL FRAMEWORK

At the national level, different cybersecurity efforts are underway in public and private institutions, as well as in technical and academic communities and civil society.

The Government of the Republic, in the framework of the Interministerial Commission for the Development of Electronic Government (CIDGE, in Spanish)[24], unanimously adopted the creation of the Subcommittee of Cybersecurity in October 2017, which is chaired by the Secretariat of the Interior (SEGOB, in Spanish) through the National Commission for Security (CNS, in Spanish), (Federal Police/Scientific Division).

Among the members of this subcommittee are various agencies and entities of the Federal Public Administration. The purpose is for the National Cybersecurity Strategy to have a comprehensive, holistic and cross-cutting development from the Federal Executive and to enable connection with different interested stakeholders, that is to say: civil society, private sector, technical and academic communities and public institutions of the different powers and of the different government areas, including any autonomous public institution.

Among other tasks, the Cybersecurity Subcommittee will be responsible for:

- Approving and publicizing the Strategy
- Following up and coordinating the implementation of the ENCS in collaboration with the different Federal Public Administration (APF, in Spanish) agencies and entities

[24] In accordance with Article Three, Section III and Nineteenth of the Agreement, which aims to create the Interministerial Commission for the Development of Electronic Government on a permanent basis, published in the Official Gazette of the Federation on December 9, 2005, and the Third Agreement of the Minutes of the 18th Ordinary Session of the Interministerial Commission for the Development of Electronic Government, of October 11, 2017, the Subcommittee on Cybersecurity was created, comprising the following authorities: 1. The Scientific Division of the Federal Police, presiding. 2. The Head of the Technological Innovation and Strategy Unit of the Office of the President of the Republic. 3. The Digital Government Unit of the Ministry of Public Administration, and 4. The holders of the Information and Communications Technology Units of the Ministries of the Interior, Economy, Education, and Finance and Public Credit, as well as the head of the Information Technology and Communications Unit of the Attorney General's Office of the Republic.
The Cybersecurity Subcommittee has the following objectives: (i) To articulate the efforts of the Federal Executive and create the general criteria for all the divisions and entities of the Federal Public Administration to contribute to the generation of the ENCS and follow up on it through general and specific actions to develop throughout the administration; (ii) To promote the participation and collaboration of civil society, private sector, academia, technical community and international organizations in the field of cybersecurity; establish the ENCS Implementation Plan, and (iii) To propose the institutional strengthening of the entity responsible for following up on the ENCS.
The Cybersecurity Subcommittee has the following permanent guests: SEDENA, SEMAR, SAT, CNBV, PROFECO, CONDUSEF, IPN, CONACYT, CENACE, SRE, SSA, STCNS-OPR, and SE-SIPINNA.

- Promoting inter-institutional collaboration and cooperation schemes in the area of cybersecurity
- Promoting collaboration and cooperation with the different stakeholders: civil society, private sector, technical and academic communities

ENCS Implementation

The Cybersecurity Subcommittee will establish the working groups for the development of each of the cross-cutting pillars, which will directly impact on the different strategic objectives.

The working groups will integrate the efforts, actions and proposals of the different actors, according to their own capacities and attributions.

Role of the Cybersecurity Subcommittee on National Security

The Sub commission will be the formal link with the National Security Council, through the Specialized Committee on Information Security.

The actions needed to comply with the national security strategic objective must be approved within the National Security Council, and its implementation will be the responsibility of the Special Committee on Information Security, in coordination with the Cybersecurity Subcommittee, in its jurisdiction.

GLOSSARY

Critical Information Infrastructure (s) (CII). The essential information infrastructures considered strategic that are related to the provision of goods and essential public services and whose disturbance could compromise National Security in terms of the applicable law. .

Cyber Attack. Action carried out through the telecommunications networks with the aim of damaging the Critical Information Infrastructures, the Essential Information Infrastructures and the safety of people.

Cyber Defense. Set of actions, resources and mechanisms of the State in matters of national security to prevent, identify and neutralize any cyber threat or cyber-attack that affects the national critical infrastructure.

Cyber Threat. Potential risk related to the vulnerabilities of computer systems and physical and passive infrastructure of public telecommunications networks that might allow damaging processes and/or the continuity of Critical Information Infrastructures, Essential Information Infrastructures, as well as the safety of people.

Cybercrimes. Criminal actions that use Information and Communication Technologies as a means or as an end and that are classified by a criminal code or other national code.

Cybersecurity. Set of policies, controls, procedures, risk management methods and standards associated with the protection of society, government, economy and national security in cyberspace and public telecommunication networks.

Cyberspace. It is a global digital environment comprising computer and telecommunications networks, where people communicate and interact; it allows the exercise of their rights and freedoms as would happen in the tangible l world.

Essential Information Infrastructure (s) (IIE, in Spanish). The networks, services, equipment and facilities associated with or connected to Information Assets, Information Communications and Technologies (ICT) and Operational Technologies (OT), the disturbance, interruption or destruction of which would have a major impact on the operation of the institutions.

ICT. Information and Communications Technologies that include computer equipment, computer programs, services and printing devices that are used to store, process, convert, protect, transfer and retrieve information, data, voice, images and video.

ICT Assets. Computer programs, computer goods, technological solutions, systems or applications, their components, databases or electronic files and the information contained therein.

Information. Set of organized and processed data included in documents and in ICT assets.

Information Asset (s). All information and the means that contain it, which, due to the importance and value it represents for any division or entity of the Federal Public Administration (APF, in Spanish), the Legislative and Judicial Powers, the autonomous constitutional organs, the productive enterprises of the State, the State, Municipal and Delegational governments, as well as individuals, must be protected to maintain confidentiality, availability and integrity, according to the value granted to it.

Information Security. Capacity to preserve the confidentiality, integrity and availability of information, as well as its authenticity, auditability, protection against duplication, non-repudiation and legality.

> **Auditability.** It defines that all the events on a system must be able to be recorded for subsequent control.
>
> **Authenticity.** It seeks to ensure the validity of the information in time, form and distribution. It also guarantees the origin of the information, validating the issuer to avoid phishing.
>
> **Legality.** It refers to compliance with the legal framework to which the institution in question is subject.
>
> **Non-Repudiation.** It refers to preventing an entity, body or person, who has sent or received information, from contending to third parties that the information was not sent or received by it/him/her.
>
> **Protection Against Duplication.** It consists in ensuring that a transaction is only made once, unless otherwise specified, as well as preventing a transaction from being recorded for later reproduction, in order to simulate multiple requests from the original sender.

Internet. Set of telecommunication networks that offer services and digital communications through the public telecommunications network.

National Catalog of Critical Information Infrastructures. List of the Critical Information Infrastructures of the different sectors of the country.

OT (Operational Technology). Hardware or software that detects or creates a change through the control and/or monitoring of physical devices, processes and events in institutions.

Personal Data. Any information concerning an identified or identifiable individual.

Reliability of Information. The information generated should be adequate to support decision-making and implementation of missions and functions.

Risk. The possibility of a threat taking advantage of a vulnerability and causing a loss or damage to ICT assets, critical infrastructures or information assets.

Threat (s). Any possible act that may cause any type of damage to the information assets of the units or entities of the APF, the Legislative and Judicial Powers, the autonomous constitutional bodies, the State productive enterprises, the State, Municipal and Delegational Governments, as well as individuals.

Vulnerabilities. The weaknesses identified in cybersecurity within the divisions or entities of the APF, the Legislative and Judicial Powers, the autonomous constitutional bodies, the State productive enterprises, the State, Municipal and Delegational Governments, and the individuals that potentially allow a threat to affect ICT assets, Essential Information Infrastructure, as well as Information Assets.

ANNEX

COLLABORATIVE PROCESS

TOWARDS A NATIONAL CYBERSECURITY STRATEGY

The process of developing the National Cybersecurity Strategy (ENCS, in Spanish) was realized with the support and participation of different stakeholders in Mexico: civil society, private sector, technical and academic community, and public institutions of the three branches and the different tiers of government. The dates the discussions on the subject were conducted were:

- **March 17, 2017** | Launch of the 2017 Mexico Cybersecurity Campaign: C5, Ecatepec, State of Mexico
- **April 19 and 20, 2017** | Multi-stakeholder workshop in collaboration with the OAS: Ministry of Foreign Affairs
- **May 16 and 17, 2017** | Follow-up meetings with interested parties: Office of the Presidency of the Republic
- **June 1 and 2, 2017** | Multi-stakeholder workshop: Tec de Monterrey Campus Mexico City
- **July 11, 2017** | Discussion forum: Senate of the Republic, Mexico City
- **July 12 and 13, 2017** | Multistakeholder workshop in collaboration with the OAS: Hotel Fiesta Americana Reforma, Mexico City
- **August 15, 2017** | Discussion forum: Memory and Tolerance Museum, Mexico City
- **September 6, 2017** | Presentation of the Study *Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado*: CANIETI, Mexico City
- **September 11, 2017** | Workshop to share good practices on Cybersecurity: Federal Institute of Telecommunications, Mexico City
- **October 11, 2017** | Creation of the CIDGE Cybersecurity Subcommittee: Mexico City
- **October 16, 2017** | First session of the CIDGE Cybersecurity Subcommittee: Mexico City
- **October 20, 2017** | Cybersecurity and Protection of Personal Data Discussion Group. INAI, Mexico City
- **October 23, 2017** | CNBV Forum on Cybersecurity *Fortaleciendo la ciberseguridad para la estabilidad del sistema financiero mexicano*: Mexico City.
- **October 26, 2017** | Second session of the CIDGE Cybersecurity Subcommittee: Mexico City

- **November 8 and 9, 2017** | 5th Latin American Meeting of Cybersecurity, Cybercrimes and Cyber Forensics: UNAM-INFOTEC-AMDETIC. Mexico City.