www.cybersecurityobservatory.org

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

2020
Cybersecurity
Report

IDB
Improving lives

OAS
More rights
for more people

www.cybersecurityobservatory.org

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

2020 Cybersecurity Report

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

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB
Improving lives

OAS
More rights
for more people

Inter-American Development Bank (IDB)

President

Luis Alberto Moreno

Project Coordination

Miguel Porrúa

Technical Team

Ariel Nowersztern

Darío Kagelmacher

Santiago Paz

Pablo Libedinsky

Florencia Cabral

Benjamin Roseth

Organization of American States (OAS)

Secretary General

Luis Almagro

Project Coordination

Belisario Contreras

Technical Team

Kerry-Ann Barrett

Rolando Ramírez

Mariana Cardona Clavijo

Manuela Orozco Jaramillo

Nathalia Foditsch

Barbara Marchiori

Global Cyber Security Capacity Centre, University of Oxford

Professor Sadie Creese

Professor Michael Goldsmith

Carolin Weisser Harris

Jakob Bund

Andraz Kastelic

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB
Improving lives

OAS
More rights for more people

TABLE OF CONTENTS

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB
Improving lives

OAS
More rights
for more people

Institutional Messages

Message from Moisés J. Schwartz

Manager, Institutions for Development Sector of the IDB

The crisis caused in early 2020 by the COVID-19 pandemic has emphasized our dependency on vital infrastructure, which is often invisible or at best barely perceptible for most citizens. Our daily essentials, such as food supply chains, transport vehicles, payments and financial transactions, educational activities, government procedures, emergency services, and even water and energy, are among the many essentials that are ever more dependent on digital technologies, making them increasingly susceptible to cyberthreats.

Cybersecurity policies are fundamental to protect citizens' rights in the digital realm—including privacy and property ownership—as well as to strengthen their confidence in digital technology and comfort in its use. Online crime amounts to about half of global property crime. Looking at the bigger picture, the numbers are even greater. The economic damage caused by cyberattacks is estimated to be more than 1 percent of some nations' annual gross domestic product (GDP), while some attacks on critical infrastructure could cause damages reaching 6 percent of annual GDP.

This study shows that the Latin American and Caribbean (LAC) region is not sufficiently prepared to handle cyberattacks. Only 7 of the 32 countries studied have a critical infrastructure protection plan, while 20 have established cybersecurity incident response teams, often called CERTs or CSIRTs. This limits their ability to identify and respond to attacks.

Identifying danger in cyberspace is the first step. Acting against these dangers is, in fact, a significant challenge for LAC countries. For example, 22 of the countries studied are considered to have very low capacity to investigate cybercrime, while they also greatly struggle in the criminal trial process. Some of the difficulties are due to the legal framework: one-third of the countries do not have one for dealing with cybercrime, and only five have ratified the Budapest Convention, the leading framework for international cooperation in dealing with cybercrime. In the case of these borderless crimes, international cooperation is key to success.

Whereas LAC governments are aware of the need to protect the digital space on which so much of society's proper functioning depends, their cybersecurity policy implementation efforts have not advanced with the needed urgency. As of the beginning of 2020, only 12 countries had approved a national cybersecurity strategy (which can be deemed an accomplishment, considering that only five countries had a strategy in 2016). Moreover, only 10 countries had established a centralized government entity to take charge of national cybersecurity management.

Why is progress so modest in the LAC region? One factor is the lack of skilled human capital. The region's gap in cybersecurity professionals is estimated to be about 600,000 workers. This problem is even worse when analyzing gender disparities, as it is estimated that less than a quarter of cybersecurity professionals are women. Faced with this scarcity, only 20 of the countries studied have any professional training programs in cybersecurity.

The Inter-American Development Bank (IDB) is working closely with LAC governments as well as with multilateral organizations such as the Organization of American States (OAS) to tackle these challenges. Given the growth the cybersecurity sector is experiencing globally, policy development in LAC countries offers economic opportunities, especially under current conditions caused by COVID-19 and as the region begins to revitalize its economy in its wake. The application of cohesive cybersecurity policies will allow the region to enjoy the benefits of the fourth Industrial Revolution, with the goal of protecting citizens and boosting economic activity.

The IDB is grateful to the governments of Israel and Spain for their technical and financial support. Both countries have been extremely generous in sharing their knowledge and experience. Cybercrime knows no borders, and as such requires a global response. I invite all LAC countries to become models of international cooperation and coordination in an area that is so relevant to our daily lives. The IDB is committed to this goal, and will continue to support LAC governments in their efforts to protect citizens from digital threats.

Message from

Farah Diva Urrutia

Secretary for Multidimensional Security of the OAS

Since 2004, the OAS has continuously emphasized cybersecurity in the hemisphere. The Organization strives to ensure an open and secure cyberspace in all OAS member states.

With the publication of the 2020 edition of the report "Cybersecurity: Risks, Progress, and the Way Forward in Latin America and the Caribbean," the OAS seeks to provide a detailed description of the national capacities of the countries of Latin America and the Caribbean (LAC) to combat cyberterrorism and ensure safer access to the internet in the region. This year in particular, the COVID-19 global pandemic has highlighted the vital role of information and communication technologies (ICTs) in the delivery of essential services and their deep integration in our societies.

OAS More rights for more people

The COVID-19 pandemic provides us with an opportunity to reflect on the progress in the expansion of ICTs, internet connectivity, and cybersecurity in the hemisphere. Our increased reliance on cyberspace during the crisis underscores the need to draw lessons for what lies ahead in the continuous transformation of our societies and economies, and in ensuring cybersecurity globally.

In a more general sense, in the last decade, cyberattacks have increased in frequency and resourcefulness. The low cost and the minimal risk that these crimes entail have been key factors in their growth. With the simple use of a computer and access to the internet, cybercriminals can cause enormous damage while remaining relatively anonymous.

Both individuals and institutions are exposed to the uncertainty and unpredictable nature of cybercrime. Therefore, it is imperative to address these threats. The efforts to do so must be multidimensional in nature because a variety of factors are required to build a resilient cybersociety. Policies and legal frameworks must be adjusted and all stakeholders from civil society, as well as the public and private sectors, must work to create a culture of cyberawareness and train qualified professional. A cybersecurity strategy is therefore an ongoing and complex effort.

This report, prepared in collaboration with the Inter-American Development Bank (IDB) and the Global Cyber Security Capacity Centre of the University of Oxford, analyzes the cybersecurity capacity of OAS member states and encourages countries to implement the most up-to-date standards in cybersecurity, while protecting the fundamental rights of their people.

As in the previous edition, the study analyzes the cyber maturity of each country in the five dimensions identified in the Cybersecurity Capacity Maturity Model for Nations (CMM): (i) Cybersecurity Policy and Strategy; (ii) Cyberculture and Society; (iii) Cybersecurity Education, Training, and Skills; (iv) Legal and Regulatory Frameworks; and (v) Standards, Organizations, and Technologies.

The progress made in the region—much of it with the support of the OAS—is evident. The 2016 report, for example, indicated that four out of five countries lacked cybersecurity strategies or a critical infrastructure protection plan. By the beginning of 2020, 12 countries had approved national cybersecurity strategies, including Colombia (2011 and 2016), Panama (2013), Trinidad and Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), Mexico (2017), Guatemala (2018), Dominican Republic (2018), Argentina (2019), and Brazil (2020), with several others in progress.

With regard to data collection and validation carried out by our member states, the report represents an overview of the complex and changing universe of cyberspace. We hope that this study provides a perspective that allows us to appreciate where we are, that enables us to make decisions based on evidence, and that improves our collective understanding of the challenges and opportunities implied by cybersecurity in our region. The information and analysis in this report will help all stakeholders—governments, private sector, academia, and civil society—to work to build a safer, more resilient, and productive cyberspace in our hemisphere.

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB
Improving lives

OAS
More rights
for more people

What Has Changed Since the 2016 Report?

Miguel Porrúa
Digital Government Principal Specialist, Data and Digital Government Cluster Coordinator, **IDB**

Belisario Contreras
Manager, Cybersecurity Program, **OAS**

When the first edition of the report "Cybersecurity: Are We Ready in Latin America and the Caribbean?" was released in March 2016, the Inter-American Development Bank (IDB) and the Organization of American States (OAS) aimed to provide the countries of Latin America and the Caribbean (LAC) not only with a picture of the state of cybersecurity but also guidance about the next steps that should be pursued to strengthen national cybersecurity capacities. This was the first study of its kind, presenting the state of cybersecurity with a comprehensive vision and covering all LAC countries.

Until the publication of the study, the region did not seem to realize the magnitude of the problem. Meanwhile, cyberattacks in the region have been increasing, mainly targeting LAC financial institutions. The COVID-19 pandemic and the increase in digital activity that has generated in the region, has further exposed the vulnerabilities of the digital space in LAC. The ThreatMetrix Cybercrime Report identified Latin America as a focus for account creation fraud, with around 20 percent of the total volume against an industry average of 12.2 percent.[1] Every year, millions of new LAC users connect to the internet for the first time. This, in turn, creates a melting pot of new customers who are not as tech-savvy as more mature digital customers. This contributes to an environment of heightened risk. Therefore, not only is LAC a target to these types of attacks, but it is also a significant source of them.

The rise in the number of cyberattacks has spurred an increase in the interest in *cybersecurity* in the region. Utilizing a simple example, the search frequency of the word *cybersecurity* on one of the more well-known internet search engines[2] increased from 20 to 100 from March 2016 to June 2019.[3] In other words, the word *cybersecurity* has become an increasingly popular search for users in LAC. Coincidentally, users searching for *cybersecurity* in LAC tended to search for courses and training opportunities in the field. That is to say, more people in LAC are aware of the importance of cybersecurity and are seeking for ways to improve their knowledge.

Given the increase in cyberattacks, the OAS and the IDB have found it necessary to re-implement the Cybersecurity Capacity Maturity Model for Nations (CMM) to measure the growth and development of the capacities of our member states to defend against the growing threats of cyberspace. Both institutions are pleased to see how cybersecurity has gained importance in the political agenda of the region in recent years and how governments, citizens, and businesses show an enormous interest in knowing more about the subject. Having more trained professionals has become essential to design and implement the cybersecurity policies and measures that are necessary to ensure a country's resilience in the face of increasingly sophisticated and complex cyberattacks. Both the IDB and the OAS are paying special attention to this need and offering various opportunities for LAC professionals to update their skills.

This new study has given us a refreshed vision on where we are and the opportunities upon which our region can capitalize. For instance, although LAC countries have enhanced their cybersecurity capacities since 2016, the average maturity level of the region is still between 1 and 2 according to the CMM, in which 1 stands for Start-up and 5 stands for Dynamic or advanced. In other words, most countries in LAC have started formulating some cybersecurity initiatives including capacity-building measures. More significantly, some of these are already in place; however, they are being implemented in an ad-hoc manner, lacking coordination among key stakeholders. The average maturity level of the 32 countries' cybersecurity should not overshadow the strides taken by the region over the past three years.

From the analysis, the cybersecurity maturity level of the Southern Cone subregion was the highest in all of the five CMM dimensions, with an average between 2 and 3. Although "Legal and Regulatory Frameworks" was the most developed dimension, "Standards, Organizations, and Technologies" had the most significant improvement since 2016. It is noteworthy that all dimensions present similar levels of cybersecurity maturity, which suggests that countries in this region are addressing cybersecurity from a comprehensive perspective. Uruguay was graded with the highest maturity level in the region in four out of the five dimensions.

The Andean Group had an average cybersecurity maturity level of 2. This reveals the importance of focusing cybersecurity efforts to strengthen the deployment of cybersecurity standards and technical controls in the region and to encourage responsible disclosure. Colombia has the most-developed cybersecurity in this group, particularly in the "Cybersecurity Policy and Strategy" and "Cyberculture and Society" dimensions.

In the case of Central America and Mexico, they presented an average maturity level of 2 in the "Cyberculture and Society" and "Cybersecurity Education, Training and Skills" dimensions, while the "Cybersecurity Policy and Strategy" and "Standards, Organizations, and Technologies" dimensions are below 2. Like in the Andean Group, Central America and Mexico should focus on enhancing the deployment of cybersecurity standards and technical controls, as well as encourage the development of a cybersecurity marketplace. Notably, the "Legal and Regulatory Frameworks" dimension has a maturity level between 2 and 3. Mexico has the best position in the region, with a maturity level between 2 and 3 in almost all dimensions. Finally, the Caribbean region has a maturity level between 1 and 2 in all dimensions. However, while "Legal and Regulatory Frameworks" was the most mature dimension, as it was in 2016, "Cybersecurity Policy and Strategy" was the least mature. The development of a national cybersecurity strategy, provides a country with a more strategic and comprehensive approach that addresses and allows a better understanding of cybersecurity challenges. Likewise, this strategic planning allows for prioritization of their objectives and investments in cybersecurity. It is noteworthy that two of the countries with the greatest development in cybersecurity in the region have a national cybersecurity strategy, that is, Trinidad and Tobago and Jamaica.

The great challenges of cybersecurity, like those of the internet itself, are of a global nature. Therefore, it is undeniable that the countries of LAC must continue to foster greater cooperation among themselves, while involving all relevant actors, as well as establishing a mechanism for monitoring, analysis, and impact assessment related to cybersecurity both nationally and regionally. More data in relation to cybersecurity would allow for the introduction of a culture of cyberrisk management that needs to be extended both in the public and private sectors. Countries must be prepared to adapt quickly to the dynamic environment around us and make decisions based on a constantly changing threat landscape. Our member states may manage these risks by understanding the impact on and the likelihood of cyberthreats to their citizens, organizations, and national critical infrastructure. Moving to the next level of maturity will require a comprehensive and sustainable cybersecurity policy, supported by the country's political agenda, with allocation of financial resources and qualified human capital to carry it out.

The COVID-19 pandemic will pass, but events that will require intensive use of digital technologies so that the world can carry on will continue happening. The challenge of protecting our digital space will, therefore, continue to grow. It is the hope of the IDB and the OAS that this edition of the report will help LAC countries to have a better understanding of their current state of cybersecurity capacity and be useful in the design of the policy initiatives that will lead them to increase their level of cyberresilience.

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB Improving lives

OAS More rights for more people

Expert Insight

Regional Trends in Cybersecurity Readiness, 2016–2020

Sadie Creese
Director,
Global Cyber Security Capacity Centre, University of Oxford

In 2015, the Organization of American States (OAS) was the first organization in the world to embark on a deep and broad study of cybersecurity capacities across a whole region, assessing the status of developments in Latin America and the Caribbean.

Against this backdrop, the second round of cybersecurity assessments presented in this report offers a longitudinal perspective on detailed cybersecurity capacity developments across the region, providing an opportunity for governments in the region to systematically take stock of their progress in light of developments in neighboring nations. These insights can also help governments to streamline their efforts in line with the milestones they have identified on the strategic level, in national cybersecurity strategies, related action plans, or other cybersecurity capacity-building programs. Furthermore, this data will provide additional insight to actors who provide resources for capacity building on the impact that their investment has had to date that will allow them, and also practitioners, researchers, international organizations, and governments, to identify successes and best practices in capacity building. Not least, this longitudinal data also facilitates a better understanding of the value of capacity assessments in guiding policy and investment priorities.

The Cybersecurity Capacity Maturity Model for Nations (CMM), which was the basis for the OAS and Inter-American Development Bank (IDB) regional studies in 2016 and 2020, follows a comprehensive approach that evaluates capacity in five dimensions: Cybersecurity Policy and Strategy; Cyberculture and Society; Cybersecurity Education, Training, and Skills; Legal and Regulatory Frameworks; and Standards, Organizations, and Technologies. To reliably measure cybersecurity capacity, every dimension is further broken down into factors, aspects, and indicators, with each level assessing capacity with progressive granularity.

The CMM was devised by the Global Cyber Security Capacity Centre (GCSCC) in 2013. To ensure that the CMM remains up to date and a powerful tool that captures important developments, the model undergoes regular review. As requirements for capacity evolve, it becomes necessary to reflect this progress in the model to adequately capture advances and offer insights into possible next steps for further improvement. In this vein, the model itself was updated in February 2017, in step with evolving security challenges and based on the experience of deploying the model in the field.

This revised version of the model, used in the 2020 study, adds a range of new aspects for analysis, such as the Mode of Operation of the Incident Response capacity, User Understanding of Personal Information Protection Online, Reporting Mechanisms, reporting of cyberincidents by Media and Social Media, Data Protection Legislation, Child Protection Online, Consumer Protection Legislation, Intellectual Property Legislation, Formal Cooperation and Informal Cooperation on cybercrime matters, Software Quality, Technical Security Controls, and Cryptographic Controls.

The present study not only contributes significant data to the international cybersecurity capacity community, it also shows the value of capacity assessments in guiding national strategy, policy, and resource allocation, and in resolving investment trade-offs across areas of capacity building. Throughout Latin America and the Caribbean, visible progress has been made across all aspects covered by the model from 2016 to 2020 (the period between the two studies), as reflected in rising capacity maturity scores. The longitudinal data across the two studies suggest several trends and indications of synergies between capacity-building efforts for different aspects.

Aspects within the Cybersecurity Policy and Strategy dimension have progressed more than those of any other dimension, indicating that a systematic strategic approach to cybersecurity capacity is recognized as being important. Further, countries with improvements in the content or development processes of their national cybersecurity strategy saw greater advances across the board, indicating that investing in a strategic approach has positive outcomes for cybersecurity. Since 2015, the number of countries in the region that have adopted a national cybersecurity strategy (NCS) has more than doubled. Colombia, which spearheaded endeavors in this area, developing the first NCS in the region in 2011, is currently implementing the second iteration of its NCS.

Significant improvements were also recorded in fostering a cybersecurity mind-set within governments and among internet users. Although not part of a dedicated awareness-raising campaign, multi-stakeholder consultations conducted in support of the development of national cybersecurity strategies raised awareness among the participating organizations about their respective activities, responsibilities, and capabilities. These awareness gains can then filter through to others and help develop and sustain capacity in this space. Progress in the organization and content of strategies is reflected in greater consideration of information and communication technology (ICT) security issues among government representatives. However, data suggests that both groups—government officials and general internet users—still lag behind the private sector, and that the sensitization of general internet users to security remains comparatively low overall. In this regard, it is worth recalling that cybersecurity capacity building of a nation remains a continuing and whole-of-nation endeavor, which, by definition, can only succeed if based on an inclusive approach that incorporates vulnerable groups across all of society.

Notably, users in countries with more advanced and specific legislation also reported higher levels of trust and confidence in their use of the internet. This could be a reflection of a perceived increase in safety that ICT security-specific laws, data and consumer protection legislation, and child protection online (introduced as new measurements in the revised CMM) bring to the online experience of users.

Maturity scores for Substantive Cybercrime Legislation largely plateaued in the 2016–2020 period, possibly because the aspect already holds the highest average score across the region. This progress on substantive legislation has been increasingly complemented by progress in Procedural Cybercrime Legislation, which is the legal aspect that has seen the most activity in the period since 2015. Substantive legislation will nonetheless experience further capacity increases in real terms, since enforcement critically depends on procedural provisions.

The sole exception to this marked progress in capacity was in the assessments of Cyberdefense Coordination. However, Cyberdefense Coordination is a sensitive issue outside of the Americas as well; more so than on other aspects, we believe assessments of Cyberdefense Coordination efforts are constrained by the sensitivity of the information involved and potential reluctance to share relevant details—factors that can also pose an impediment to Cyberdefense Coordination in itself.

Further comparative research on the longitudinal data could provide additional insights into whether advances in hitherto under-prioritized areas could catalyze advances in other areas and should therefore become a focus going forward. All aspects of Cybersecurity Education, Training, and Skills, for instance, rank in the bottom half in terms of progress. Shortages in the workforce of qualified cybersecurity professionals is a near-universal challenge. Yet, without adequate funding for professional training and education, this supply-demand mismatch carries the risk of limiting maturity gains going forward. A lack of a supporting cybersecurity skills base could also have cascading negative effects on capacity-building efforts in other areas. These considerations highlight the need to balance investments in short-term maturity gains to address immediate security threats with long-term plans to foster skills and education that make substantial and self-sustaining contributions to national cybersecurity.

Responsible Disclosure was the aspect with the lowest maturity score in the region. The breadth and integrated approach of the CMM make it possible to further contextualize the scores of individual aspects. In this vein, risks associated with the lack of an institutionalized mechanism for sharing information about discovered vulnerabilities and policies on ethical hacking could possibly be compounded by the similarly low scores for internal response capacities, including Organization of Critical Infrastructure Protection, Crisis Management, Risk Management and Response, and Cybercrime Insurance—which rank towards the bottom and have seen little improvement since 2015.

A key purpose of any CMM assessment is to discover measures that worked well but also to identify gaps. In this regard, the OAS and all participating countries in the region deserve recognition for producing this updated baseline and for charting a path that other regions could follow in gaining greater substantiated awareness of their capacity levels.

In addition to commitments to cybersecurity capacity building at the national level, Latin America and the Caribbean has been the host of vibrant regional initiatives. For instance, 2016 saw the launch of CSIRT Americas, a platform enabling regional cooperation and information exchange among the governmental and national incident response teams of OAS member states. In the wake of the WannaCry ransomware attack in 2017, CSIRT Americas has facilitated the identification and early isolation of infection hotspots across the Americas to curb the spread of WannaCry within the region. To mitigate future outbreaks, the platform has built up a central repository of tools for its regional constituents to preempt and combat ransomware infections. Since 2015, the incident response community itself has grown to 20 national cybersecurity incident response teams (CSIRTs) within the region.

Teams from the Americas have trained alongside their counterparts from Europe, Africa, and Asia in regular annual exercises, organized in partnership between the OAS and the Spanish National Cybersecurity Institute (INCIBE) and the Spanish National Center for Critical Infrastructure Protection since 2016. In 2018, the OAS, the IDB, and INCIBE hosted the first joint cybersecurity challenge specifically to support and encourage young talent in Spain and the Americas to pursue a career in cybersecurity-related fields.

In its commitment to promote compliance with the baselines for responsible behavior in cyberspace identified by the consensus reports of the UN Group of Governmental Experts on Information Security, the OAS in 2017 established a Working Group on

Cooperation and Confidence-Building Measures in Cyberspace. Exchanging best practices with the Organization for Security and Cooperation in Europe (OSCE), the working group has developed two sets of confidence-building measures, now adopted by OAS member states. As part of these measures, OAS member states have resolved to share information on national cybersecurity policies, establish a national point of contact to discuss cyberthreats at the regional level, identify a separate point of contact within their ministries of foreign affairs in furtherance of international cooperation and dialogue, and support these channels—where appropriate—with platforms and agreements to promote practices strengthening stability in cyberspace. Additional commitments include training diplomats and government officials generally on cybersecurity matters and strengthening capacity-building initiatives through awareness campaigns in both the public and the private sector.

The OAS and the GCSCC have a special relationship. The two organizations have been collaborating since the development of the CMM, conducting joint pilot deployments of the model in Jamaica and Colombia in 2015 and a later assessment in Brazil in 2018. This strategic partnership was formalized through a memorandum of understanding in 2015. As a trusted partner, the OAS was an active contributor in the revision process of the CMM. Collaboration between the two organizations also extends beyond the CMM, including joint initiatives at stakeholder events like the Internet Governance Forum (IGF). Going forward, the OAS and the GCSCC will be working closely together in testing a Cyber Harm Framework, to be deployed in conjunction with the CMM, as well as on establishing a regional hub in Latin America as part of a larger global constellation of regional cybersecurity capacity centers.

The EU’s Comprehensive Approach to Address Threats from Cyberspace

Pawel Herczynski
Managing Director for CSDP and Crisis Response, **European External Action Service**

Cybersecurity is critical to our prosperity and security. Malicious cyberactivities threaten not only our economies but also the very functioning of our democracies, freedoms, and values. Our future security depends on transforming our ability to protect us against cyberthreats: both civilian infrastructure and military capacity rely on secure digital systems.

This has been recognized in the Global Strategy on Foreign and Security Policy for the European Union (EU).[4] Building also on the approaches of the Digital Single Market; the Global Strategy; the Joint Communication to the European Parliament and the Council “Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU”;[5] the European Agenda on Security;[6] the Joint Framework on countering hybrid threats;[7] and the Communication on Launching the European Defence Fund,[8] the EU has decided to build greater resilience and strategic autonomy, boost capabilities in terms of technology and skills, and build a strong single market, as well as develop and implement a comprehensive EU approach for cyberdiplomacy at a global level.

Resilience

Strong cyberesilience needs a collective and wide-ranging approach. Effective structures to promote cybersecurity and to respond to cyberattacks in the EU member states but also in the EU’s own institutions, agencies, and bodies are needed. It also requires a more comprehensive, cross-policy approach to building cyberresilience and strategic autonomy, with a strong single market, major advances in the EU’s technological capability, and far greater numbers of skilled experts.

The NIS Directive concerning measures for a high common level of security of network and information systems[9] has a tremendous role in developing a new cybersecurity culture in the EU. Thanks to the NIS Directive, EU member states exchange information about cyberincidents, share best cybersecurity practices, cooperate, and are better coordinated. The NIS Cooperation Group, which was created by the directive, supports and facilitates the strategic cooperation and exchange of information among EU member states. Under the NIS Directive the operators of essential services (e.g., banks, telecom companies, energy providers, hospitals, etc.) are obliged to inform the national authorities when they are affected by serious cybersecurity incidents and have risk assessment plans prepared to identify risks. Responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services and digital service providers. However, a culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. We need more than ever before the cooperation and exchange of information as well as the pooling of different skills and experts as cyber threats and cybersecurity incidents are becoming more sophisticated in our digital economy and society.

One step towards improving the criminal law response to cyberattacks was already taken with the adoption in 2013 of the Directive on attacks against information systems.[10] This established minimum rules concerning the definition of criminal offenses and sanctions in the area of attacks against information systems and provided for operational measures to improve cooperation amongst authorities. The Directive has led to substantive progress in criminalizing cyberattacks at a comparable level across the member states, which facilitates the cross-border cooperation of law enforcement authorities investigating these types of offenses. Given the borderless nature of the internet, the framework for international cooperation provided by the Council of Europe's Budapest Convention on Cybercrime[11] offers the opportunity amongst a diverse group of countries to use an optimal legal standard for the different national legislations addressing cybercrime. A possible addition of a protocol to the convention is now being explored, which could also provide a useful opportunity to address the issue of cross-border access to electronic evidence in an international context.

Research and development

By cooperating, pooling the EU's cybersecurity expertise, and developing a common European cybersecurity research and innovation (R&I) road map and an industrial European cybersecurity strategy, Europe can help the cybersecurity industry and the ecosystem to grow, also resulting in stepping up the EU's cybersecurity capacity. This is why, in 2016, the European Commission signed a contractual public-private partnership (cPPP) with the European Cyber Security Organization (ECSO). The cPPP is instrumental in structuring and coordinating industrial resources of digital security in Europe. It includes a wide range of actors, from innovative SMEs to producers of components and equipment, operators of essential services, and research institutes, brought together under the umbrella of ECSO. The EU has committed to invest up to €450m in this partnership, under its research and innovation program Horizon 2020. In return, the industry has to invest three times as much in the same areas. As an ambitious next step, in September 2018 a new regulation was proposed to establish a network of national cybersecurity coordination centers and the new European Cybersecurity Industrial, Technology and Research Competence Centre. This proposal is currently being discussed by EU co-legislators. The Centre is seen as a way to tackle the fragmentation of Europe's cybersecurity ecosystem, to address the lack of cybersecurity skills and expertise, to pool our European resources, and to coordinate our efforts in strengthening the EU's cybersecurity capabilities and enable EU industries to develop worldwide competitive products and services. It will pave the way for a secure digital Europe, addressing all upcoming cybersecurity challenges arising from emerging technologies (e.g., IoT, artificial intelligence, quantum, HPCs, block chain) and used in critical sectors (e.g., transport, energy, health, finance, manufacturing, defense). It will also shape and implement the appropriate investments in cybersecurity for the next EU Multiannual Financial Framework Programme (MFF).

Capacity building

Global cyberstability relies on the local and national ability of all countries to prevent and react to cyberincidents and investigate and prosecute cybercrime cases. Supporting efforts to build national resilience in developing countries will increase the level of cybersecurity globally, with positive consequences for the EU.

Countering fast-evolving cyberthreats would suggest a need for training, policy, and legislation development efforts, as well as efficiently functioning computer emergency response teams (CERTs) and cybercrime units in all countries worldwide.

Since 2013, the EU has been leading on international cybersecurity capacity building and systematically linking these efforts with its development cooperation. The EU will continue to promote a rights-based capacity-building model in line with the Digital4Development approach.[12] The priorities for capacity building will be countries neighboring the EU and developing countries experiencing fast-growing connectivity and rapid development of threats. EU efforts will be complementary to the EU's development agenda in light of the 2030 Agenda for Sustainable Development and overall efforts for institutional capacity building.

The EU also defined its approach on cybersecurity capacity building in June 2018, when the Council in its conclusions on the EU External Cyber Capacity Building Guidelines recalled that cybersecurity capacity building is becoming one of the most important topics on the international cybersecurity policy agenda and stressed the role of cybersecurity capacity building in partner countries and regions as a strategic building block of the EU's cyberdiplomacy efforts.

Cyberdiplomacy

Guided by the EU core values and fundamental rights such as freedom of expression and the right to privacy and protection of personal data, and the promotion of open, free, and secure cyberspace, the EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyberstability as well as contributing to Europe's strategic autonomy in cyberspace. Given the global nature of the threat, building and maintaining robust alliances and partnerships with other countries is fundamental to the prevention and deterrence of cyberattacks, which are increasingly central to international stability and security. The EU will prioritize the establishment of a strategic framework for conflict prevention and stability in cyberspace in its bilateral, regional, multi-stakeholder, and multilateral engagements. The EU strongly promotes the position that international law, and in particular the UN Charter, applies in cyberspace. As a complement to binding international law, the EU endorses the voluntary non-binding norms, rules, and principles of responsible state behavior that have been articulated by the UN Group of Governmental Experts. It also encourages the development and implementation of regional confidence-building measures, both in the Organization for Security and Co-operation in Europe and in other regions. On a bilateral level, cyberdialogues[13] are further developed and complemented by efforts to facilitate cooperation with other countries to reinforce principles of due diligence and state responsibility in cyberspace. The EU also stresses that cybersecurity is not a pretext for market protection and the limitation of fundamental rights and freedoms, including the freedom of expression and access to information. A comprehensive approach to cybersecurity requires respect for human rights. In that regard the EU emphasizes the importance of all stakeholders' involvement in the governance of the internet.

Adopted in 2017, the framework for a joint EU diplomatic response to malicious cyberactivities (the "cyberdiplomacy toolbox"[14]) sets out the measures under the Common Foreign and Security Policy, including restrictive measures that can be used to strengthen the EU's response to activities that harm its political, security, and economic interests. The framework constitutes an important step in the development of signaling and reactive capacities at the EU and member state level.

Conclusion

EU cyberpreparedness is central to both the Digital Single Market and our Security and Defence Union. Enhancing European cybersecurity and addressing threats to both civilian and military targets is a must. In this challenging effort we count equally on the support of our global partners. Only together, being resilient and capable of protecting our people effectively by anticipating possible cyberthreats and cybersecurity incidents, building strong resilience in our structures and defense, recovering quickly from any cyberattacks, and deterring those responsible, can we provide open, secure, and safe cyberspace for all.

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB Improving lives

OAS More rights for more people

Emerging Threats in Cybersecurity:
Implications for Latin America and the Caribbean

Nayia Barmpaliou
Head of Public Policy and Initiatives,
Centre for Cybersecurity,
World Economic Forum

Cybersecurity in the Era of Hyper-Connectivity and Pandemics

The global pandemic of COVID-19 has marked a fundamental inflection point in our global course and accentuated as never before our reliance on digital infrastructure. While this crisis has exposed structural shortcomings that our society has carried along in multiple systems such as health, economy, employment, and education, it has also highlighted the catalyzing role of technology in the way we have collectively coped with the pandemic.

Within a span of three months, we experienced the acceleration of digital transformation that was previously anticipated in three years.[15] Our transition to the "digital of everything" era has profoundly reshaped our professional and personal lives. Even in the most disruptive environment of the pandemic, the internet and global digital infrastructure have made the provision of essential services possible, allowed businesses to continue operating, and sustained our individual social contacts. The result of this transition has been a dramatically augmented cyberattack surface in a digital ecosystem of already amplified vulnerabilities that includes more than 20 billion Internet of Things (IoT) devices connected worldwide.[16]

Even before the pandemic, cybersecurity breaches and data leaks were becoming the showstoppers for the digital economy. Cybercriminals are quick to exploit new attack vectors and capitalize on the gaps in law enforcement cooperation across jurisdictions given the inherently transnational nature of their malicious activities. In turn, the risk of cyberattacks on critical infrastructure and data fraud or theft has been consistently top of mind for business leaders globally. According to the World Economic Forum's Global Risks Report 2020,[17] the risk of cyberattacks on critical infrastructure and data fraud or theft ranked in the top ten of risks most likely to occur, while the recent COVID-19 Risks Outlook[18] identified cyberattacks as the third greatest concern due to our current and sustained shift to digital work patterns.

The available data backs these concerns; cybercrime damages are estimated to reach US$6 trillion by 2021, which amounts to the GDP of the world's third-largest economy.[19] Aside from the financial cost, cybercrime and cyberattacks undermine user confidence in the digital economy. Surveys indicate that of the global population with internet access, less than 50 percent trust that technology will improve their lives, showing a growing and profound lack of trust regarding data privacy.[20]

These trends are particularly pertinent for the Latin American and Caribbean (LAC) region that has witnessed an enormous expansion in the use of information and communication technology (ICT) in the past five years. As the region is moving more and more towards the digital economy, the need to ensure digital trust is heightened. Digital security risk management and privacy protection protocols constitute shared responsibilities by governments, the private sector, and individual users in an increasingly data-driven economy.[21] Further to the elevation of cybersecurity capacity building in the region's development agenda thanks to concerted and intensified efforts by the Inter-American Development Bank (IDB) and the Organization of American States (OAS) in recent years, the need for integrating cybersecurity and the fight against cybercrime in the region's digital strategies and policies has also been captured at the highest level as part of the Proposed Digital Agenda for Latin America and the Caribbean.[22]

A Cross-Cutting Issue in National Policy

The intrusion of the digital continuum into all areas of human activity and the unprecedented levels of technological innovation and interdependence have made it impossible to treat cybersecurity in isolation, as a technical issue or a distinct policy area. In recent years, cybersecurity has broken the glass ceiling of the technical silos and sits at the intersection of multiple disciplines and policy areas: digital access and connectivity, resilience, criminal justice, diplomacy, international security and defense, and digital economy and trade, as well as new technologies. With nations trying to reap the benefits of the Fourth Industrial Revolution, cybersecurity has been elevated to the zeitgeist of global policy. This has resulted in a significant increase in the adoption or revision of national cybersecurity strategies that take a whole-of-government or even at times a whole-of-society approach, as well as in the development or adaptation of national cybercrime legislation especially in developing countries that did not have relevant laws in place.

This report provides promising evidence that governments in the LAC region have taken important strides in the development and effectiveness of their national cybersecurity strategies that have also served as vehicles to improve the national cybersecurity culture and practices since they were last surveyed in 2016. Moreover, four LAC countries have since joined the Council of Europe's Convention on Cybercrime (i.e., the Budapest Convention), whose objective is to pursue a common criminal policy against cybercrime by offering a common framework for appropriate national legislation and for international cooperation.

Market Failure and Opportunity for Cybersecurity in the Digital Economy

While the rapid advancement in digital technologies brings great innovations to the fore, it also creates new vulnerabilities at a faster pace than they can be secured. To date, the imbalance between the time to market and the time to security remains a predominant issue, with market forces pressuring for new technology products without incentives to prioritize security features from the outset of product development.[23]

It is striking that despite shifting consumer behavior over growing concerns about privacy and security, the change in market objectives is not occurring fast enough and will inevitably lead to varying experiments in regulatory intervention and regimes. For now, we see that the prevalent lack of a security-by-design approach in technological development has generated a trend towards voluntary cybersecurity certification schemes for ICT products, for example in the EU and Singapore, with more countries focusing specifically on IoT. On the other end of the spectrum, this market failure has given rise to cybersecurity as one of the most diverse and rapidly expanding sectors worldwide. Before the COVID-19 crisis, global spending on cybersecurity products and services was expected to increase by 88 percent in the next eight years.[24] The economic downturn caused by the pandemic might lead to consolidation of this market. For the LAC region, as it is moving towards greater maturity on cybersecurity, it is important for national cybersecurity implementation strategies to consider measures that will limit the risk of the increased attack surface and get inspiration from existing standards or voluntary schemes.

The Strategic Business Cybersecurity Imperative

The notion that cybersecurity strategy forms an integral part of business strategy has gained more traction and actual implementation by businesses in the last five years, in part due to the publicity surrounding some large security breaches as well as increased legal and regulatory considerations, including the entry into force in May 2018 of the EU's General Data Protection Regulation (GDPR), which has a significant global footprint. Practically, this has been a key driver for business leaders and corporate boards to better understand the cyberrisks to their business operating model and strike the right balance between protecting the security of their assets, mitigating losses, and maintaining profitability in a competitive environment. This improved awareness at the corporate leadership level is a crucial first step in empowering informed corporate decision making for cybersecurity planning, response mechanisms, and investments. The launch of the Cyber-Risk Oversight Handbook for Corporate Boards by the Organization of American States and the Internet Security Alliance in 2019[25] marked a significant consultative effort to raise such awareness in the LAC region across stakeholders from corporate boards, senior management, governments, and academia and adapt the advice to regional specificities.

Meanwhile, as larger companies have been investing more in cybersecurity and security innovation, recent analyses note a significant increase in attacks targeting small- and medium -sized enterprises (SMEs). This creates a significant risk in the digital ecosystem, particularly considering that SMEs do not have the financial resources to invest heavily in cybersecurity or simply do not have security culture as a major driver of their agendas. In fact, the challenges that SMEs face in terms of lack of financial resources or security culture to secure their digital environment are quite different from those of bigger organizations. Reflecting this reality in the regional LAC context, one should note that according to the Organization for Economic Cooperation and Development, LAC's economic structure is composed of 99.5 percent micro, small, and medium enterprises.[26] Increasing cybersecurity awareness and promoting basic cybersecurity hygiene across the SMEs in the region should therefore be a critical priority in the coming years.

New Technologies Reshape the Cybersecurity and Policy Landscape

"Old" and "new" technologies are not only reshaping industry and the cybersecurity landscape but are more broadly challenging the traditional ways society has operated. The convergence of information technologies with operational technology and legacy systems already poses great challenges across the digital ecosystem. The emergence of new technologies and their applications such as artificial intelligence, big data, 5G networks, cloud computing, IoT, and quantum computing is drastically questioning our conventional thinking for the future of digital economy. On the one hand they offer immense opportunities for efficiencies and innovation, but they also amplify the attack surface and can create uncharted data privacy and security risks. For this reason, businesses and governments need to work together to develop a solid understanding of the related emerging cybersecurity risks from a policy, risk, and operational perspective. Part of the challenge will be to foster trust amongst different stakeholders of the ecosystem to reduce friction in the current regulatory and assurance models. Importantly for countries in the LAC region and other emerging economies, these emerging security issues will have to be addressed in a way that does not exacerbate barriers to accessing the benefits of emerging technologies.

Cybersecurity in a Fragmented and Polarized Global Architecture

In the era of a multi-polar and multi-conceptual global order, the geopolitical and social context both influences the development of technology and is impacted by technology. For one, the emergence of new technologies has the potential to significantly reshuffle geopolitical dynamics and alliances, while currently the convergence of new technologies with traditional applications plays a profound role in amplifying existing tensions over values for open and decentralized internet governance versus cybersovereignty or the use of cyberspace as a venue for strategic competition. Such polarization can undermine both security in cyberspace as well as trust for global cooperation against common cybersecurity challenges. The divergent approaches of major cyberpowers on how international law applies in cyberspace —which are under discussion at the relevant UN fora[27]— reflect quite a conflictual international environment, further exacerbated by calls for digital strategic autonomy even if it would be challenging to attain within the context of rapid technological change and global value chains.

Against this backdrop, regional organizations have been positioned as key stakeholders in promoting regional stability, security, and trust-building efforts in cyberspace in the form of confidence-building measures. The LAC region has also demonstrated significant progress to this end with the establishment in 2017 of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace by the OAS Inter-American Committee against Terrorism.[28]

Need for a Paradigm Shift in Public-Private Cooperation

The intrinsically complex and distributed nature of the digital ecosystem coupled with the multiple dimensions of public and corporate cyberpolicy have over time created a highly complicated stakeholder architecture. Digitalization has transformed our society into a system of systems whereby critical functions are distributed between public and private stakeholders in dispersed locations and with complex interdependencies. Therefore, recent years have taught us that public-private cooperation on cybersecurity requires thinking outside of traditional and rigid formats to overcome barriers and become truly effective. To address this heightened complexity and shared responsibility, we need a new generation of public-private partnerships that invalidate "silo thinking" and take a systemic approach in navigating the compound dynamics of policy, technological, economic, social, and geopolitical factors that shape the cybersecurity risk landscape and its interdependencies. As countries in the LAC region are accelerating their digital transformation, they have an opportunity to weave such systematic thinking into their public-private cooperation architecture so that it can be a differentiating factor for their cyberresilience.

Conclusion

The complexity of cybersecurity is a clear example of how our existing fragmented global architecture is not fit for purpose in the 21st century. The catalyzing effect of the COVID-19 pandemic on the economy has put immense pressure on our digital environment to remain secure, resilient, and effective. Cybersecurity is an integral component and key enabler for this unprecedented connectivity, and this new normal has reasserted the value of cyberse-curity as a global public good.

Beyond the operational protection of systems and networks, cybersecurity is, and shall remain, critical in assuring the integrity and resilience of the interconnected government, business, and socioeconomic processes that rest on top of our continuously complex tech-nology ecosystem. Addressing cyberrisk across the board requires continuous efforts and adaptation. The present report offers significant insights on the efforts made at the national level within the LAC region by capturing and quantifying national progress across different cybersecurity dimensions since the 2016 review and also demonstrates the region's cybersecurity posture improvement over time. This work can serve as an invaluable tool for decision makers in the public and private sectors to identify priority interventions as they move forward in further improving the state of cybersecurity in the LAC region through concerted and scalable national, regional, and international collaboration.

The Need for a Harmonized Response to Cyberthreats: A Roadmap

Sven Mikser
Minister of Foreign Affairs,
Republic of Estonia

Over the last decade, a number of threats have emerged in cyberspace that require the attention of governments worldwide. Three of the most pressing international cybersecurity issues involve the increasing instability caused by cybercrime, cyber-enabled intrusions into critical networks, and politically motivated cyberoperations. All these elements have been or are in the process of being implemented into states' political agendas around the globe. However, the extent to which the outlined issues have become a priority differs greatly between states. This has indicated a greater need for harmonization of states' efforts in increasing their cybersecurity. The question, therefore, is how to incentivize states to cooperate in a field that conventionally would be considered an internal issue.

One way to address the emerging challenges among states would be to implement an international approach that would focus on harmonization of cybersecurity capacities. Due to the high level of states' interconnectedness in cyberspace, the stability of one state affects the well-being of all those around it. Therefore, a regional approach would be able to incentivize many states to get involved in cybersecurity capacity building. There are many regional organizations that have taken up initiatives to solve the issue. For example, the Organization of American States (OAS) has been active in organizing cybersecurity capacity-building workshops over several years. These events are particularly important in order to lay the groundwork for building strong capacities at the state level by increasing awareness of the emerging cyberthreats and the development of possible coping mechanisms. Taking into account the first efforts that a variety of parties have contributed in cybersecurity awareness raising in Latin American and the Caribbean (LAC), further steps for achieving a more stable and prosperous cyberspace could be built upon a stronger regional cybersecurity cooperation.

The following elaborates on how regional cooperation and commonly shared values on cybersecurity would help states to overcome the three key threats highlighted above and offers some suggestions on how to move forward from the current state of development.

How Can Internationally Harmonized Cybersecurity Capacities Assure a Safer Cyberspace?

Considering the borderless nature of crimes enabled by cyberspace, regional cooperation in capacity building is vital in order to react to organized cybercrime and stop cyberattacks before they become uncontrollable. The most recent cybersecurity incidents in 2018 and 2017 have demonstrated the risk for increasing financial damage and the number of people and states it influences. We have already witnessed larger-than-ever cybercrime operations that have halted the normal development of national economies, specifically targeting some of the core pillars of state economies such as the industrial and banking sectors.

Awareness raising among technical, political, and law-enforcement experts could help to make countries less vulnerable to cybercrime. The nature of the criminal acts taking place in cyberspace is changing rapidly, which is why countries need to invest more in educating their staff in law enforcement, judicial systems, and other relevant governmental institutions. Adapting to the new circumstances is also key in developing trustworthy public-private partnerships. Information sharing between the private sector, the public sector, and government institutions can already be seen in some countries, yet it is less noticeable in others. Regional harmonization of legal frameworks to address cybercrime, and law enforcement best practices, could contribute to regional safety and stability in cyberspace.

In addition to the increased numbers of cybercrime incidents, cyberenabled intellectual theft has become more widespread in many parts of the globe. The level of sophistication with which intellectual property has been stolen makes it impossible to avoid its attribution to a state actor.

Some of the malware that has been used shows signs of regional origin and is specifically built to target certain areas of the world. This is one of the reasons regional cooperation in tackling cyberenabled intellectual theft should be considered a part of an international and harmonized states-led approach.

In the background of the aforementioned activities, political influence operations conducted in cyberspace could now pose a serious concern for democratic countries. In 2018, presidential elections were held in the three largest democracies: Brazil, Colombia, and Mexico. Although the public news coverage reflects only a mild spread of disinformation during the election campaigns and voting periods, the issue of election interference will very likely continue to be on the agenda for most democratic countries in the coming years. Election meddling, disinformation campaigns, and security of the voting infrastructure are considered areas of concern when it comes to spreading political influence in foreign countries. Exploiting cyberenabled media outreach, some foreign countries may continue to try to undermine democratic institutions and policy making in the region. Shifting public opinion through online media has become a lingering part of contemporary politics that is particularly visible during the election season, and the structures to tackle it should already be in place before an election.

A Regional Approach to Harmonizing the Level of Cybersecurity Capacities

Advancing cybersecurity policies regionally should start from developing national building blocks. A national cybersecurity strategy could function as the primary awareness-raising and planning instrument in individual states. The existing cybersecurity strategies could offer a variety of examples and lessons.

Some of the countries that have released their cybersecurity strategies already in the 2000s have been first-hand witnesses to the developments that have occurred over time in offering a strategic vision on cybersecurity. In Estonia, cybersecurity has become a continuous part of the daily work of different ministries and state institutions. Its primary effect has been a deeply rooted intrastate policy coordination within the frameworks of the state's strategic policy making. Whereas the emphasis on Estonia's first cybersecurity strategy emerged from a case of hybrid campaign due to the 2007 events in Tallinn and became a part of the crisis response, the two later strategies have focused more broadly on strengthening cyberesilience and capabilities.

Developing a cybersecurity policy is an ongoing process. Among other strategic goals, Estonia's third cybersecurity strategy (2019–2021) has addressed cybereducation as one of the future areas where more investments should be made. The cyberdimension was also included in the country's national crisis response regulation. Some of the best practices that we have in continuing the work on the national level involve better national coordination and information exchange mechanisms, overcoming the gaps between the experts and the top national decision makers in the public and private sectors, and creating cybersecurity institutions and coordination structures. These practices are still part of our ongoing work today.

As cyberenabled malicious activities can easily spread from country to country, investigations cannot be effective without international cooperation. As we know, increasing numbers of our national information systems and critical infrastructure rely upon the safety of our networks. A whole-of-government cybersecurity strategy—including possible preventive measures, national legislation to address cybercrime, and operative international cooperation between states—should be one of the most eminent requirements in order to avoid activities that exploit critical infrastructure vulnerabilities.

Ways Forward for Regional Cooperation in Latin America and the Caribbean

Greater regional cooperation in developing a shared vision and learning from other states' best practices is key in harmonizing states' cybersecurity capacities. Several member states of the OAS have successfully adopted national criminal legislation, which entails provisions for IT-related crimes as well as cybersecurity strategies. In addition to the legal provisions, many states have already acceded to the Budapest Convention on Cybercrime. From both national and international perspectives, the Budapest Convention offers a comprehensive and trusted international legal framework for combating cybercrime, and during the almost two decades of its existence it has become a global instrument of reference. Thus, the Budapest Convention has developed into a preferred model for many countries in advancing their own national legislation, building up international cooperation, and exchanging electronic evidence.

Since cyberthreats are getting more sophisticated, it is the states' responsibility to assure that the activities of the perpetrators will not go unnoticed. Policy and legislative initiatives alongside capacity-building measures are key elements for combating threats arising from cyberspace, including the conduct of criminal perpetrators. Implementation of relevant legislation and adoption of strategic methods will support the effectiveness of the work done for criminal justice on a national level and international cooperation among OAS states under the auspice of international law provisions.

Raising awareness of cyberthreats at the political level is only the first step in developing more harmonized cybersecurity capacities in a region. Adopting and implementing national cybersecurity policies would lead to safer and more stable economic and political development in the region and would contribute to the local and global stability of cyberspace. Regional actors in LAC, such as the OAS, have already contributed to this process. Now is the time for more practical implementation.

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB
Improving lives

OAS
More rights
for more people

Building Cybersecurity Capacity:
Challenges for Post-Secondary Education in Latin America and the Caribbean

UNIVERSIDAD DE CHILE

Prof. Pablo Ruiz Tagle-Vial
Dean, Faculty of Law, **University of Chile**
Prof. Daniel Álvarez Valenzuela
Academic Coordinator, Center of Studies on Information Science Law, Faculty of Law, **University of Chile**

In recent years, several countries in Latin America and the Caribbean have witnessed and have been victims of the increasing number of cybersecurity threats which have come to affect not only public and private institutions, but also citizens of these countries. The increase in cybersecurity threats is reflected in the number of registered attacks as well as in their level of intensity and sophistication.

The diagnosis on the causes attributed to the rise of cyberthreats is known by all. In the previous version of this report published in 2016,[29] it was noted that the region's level of growth in digital technologies and the incipient processes of digital transformation which these countries are carrying out, as well as the dependence generated by technology, have been factors which have contributed to the increase in risks and threats to digital security that the countries of the region face.

In addition to the above, the previous version of this report also sheds light on how poorly prepared LAC countries are when facing new risk scenarios for the security of their inhabitants and, consequently, for the effective protection of their rights, an issue that manifested in all the dimensions analyzed in the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the Global Cyber Security Capacity Centre of the University of Oxford.[30]

In the present version of the report, countries' level of maturity in education, training, and capacity building remains extremely uneven. This does not surprise us, given the great economic, social, and cultural disparities which exist among the various LAC countries, as we will see below.

On the one hand, we have a group of countries—representing a third of the total number of those analyzed—that have considerably increased their ratings in areas such as education and training over the last years, reaching mid-level maturity. Such is the case of Uruguay, which achieved a level of strategic maturity in the area of professional training, as well as Guyana, which increased its ratings in almost all of the areas evaluated.

This group of countries also includes Argentina, Chile, Colombia, Costa Rica, the Dominican Republic, Mexico, Paraguay, and Trinidad and Tobago, which are, coincidentally, the countries that have a full or partial national cybersecurity policy or strategy, and that have developed an educational offer, both public and private, which takes into account specialized training on cybersecurity, both from a technical and legal standpoint.

On the other hand, the present report notes the marginal progress or lack thereof in the maturity level of two-thirds of LAC countries in terms of education, training, and development of skills in cybersecurity. In these countries, the offer of specialized training in digital security is nonexistent or incipient, and where it does exist usually only considers the technical dimension of cybersecurity.

These results invite us to rethink the strategies that each of these countries, as well as their public and private organizations, should adopt to improve their current maturity levels, while promoting mechanisms for international cooperation, both at the regional and sub-regional level. For example, countries which have been able to advance and improve their educational offer could support those who are in a less advantageous situation.

As has been said multiple times, the human factor is and will remain a fundamental element in any strategy that seeks to be successful, and post-secondary institutions play a fundamental role in this aspect. From our point of view, the challenges we face are multiple and require complex and differentiated solutions depending on the political, economic, and social reality of the various countries which make up the region.

For countries in this report that are at the initial stages of maturity, it seems unavoidable to pursue the development of specialized offerings of undergraduate and postgraduate studies in information technology and cybersecurity with an emphasis on the development of the necessary skills for a quality technical training. As has been the case in the past, international cooperation, as well as public-private partnerships, can play a fundamental role in identifying and prioritizing the most important needs of each country.

In addition to strengthening and expanding their undergraduate and postgraduate specializations, those countries that are currently in the Formative stage or have transitioned to the Established stage, should initiate curricular innovation processes for the mainstreaming of the minimal content that any professional should acquire in the field of information technology and digital security — and certainly including a gender perspective, to allow for other recently identified gaps to be closed. Among the minimal content that can be identified today we can mention risk management, regulation of technologies, protection of personal data, and computer crimes, among others.

Likewise, it is necessary to advance the development of multidisciplinary programs which allow the integral training of professionals who are able to understand the task of their respective disciplines from a broader perspective. This is essential in the transition to a digital society which several of our countries are currently experiencing, requiring not only professional and technical specialists in the area of information technology and cybersecurity, but also social science professionals, including those in the fields of law, political science, economics, and social communication, among others. In this area we cannot exclude mentioning the postgraduate programs that the University of Chile has offered for decades in its School of Engineering[31] and more recently in our Faculty of Law,[32] initiatives that since their inception have considered a multidisciplinary approach as an essential aspect of specialized postgraduate training.

Those countries that are in the Established stage of maturity require a greater commitment from their universities and higher-education institutions with research and development—through public and private efforts—on various aspects related to cybersecurity, such as cryptography and its diverse applications, the study of models and techniques of incident analysis, the use of artificial intelligence and neural networks in the resolution of complex problems, and security applications, among others. Research could be based on information collected by national cybersecurity authorities, the Cybersecurity Incident Response Team (CSIRT) Americas platform managed by the OAS, and the specialized companies operating in each country.

The virtuous circle stemming from this continuous exchange of information —with the due technical, legal, confidentiality, and security measures— will allow some of these countries to move towards the Strategic and Dynamic maturity stages. Hence, the educational offer, training, and research will be geared towards the real needs and strategic objectives of each country, as per the definitions adopted in their respective national cybersecurity policies or strategies, while maintaining a system for identifying and managing risks according to the kinds of threats and vulnerabilities that they face.

Finally, the challenge we face as institutions of higher education should be viewed, at least by public or state institutions, as a countrywide challenge that, in overcoming it, will allow us to have a free, open, safe, and resilient cyberspace, directly benefiting the people and the full exercise of their fundamental rights in cyberspace.

The Cybersecurity Capacity Maturity Model

The Global Cyber Security Capacity Centre (GSCC) at the University of Oxford, in consultation with over 200 international experts drawn from governments, civil society, and academia, developed the Cybersecurity Capacity Maturity Model for Nations (CMM).[33] The CMM is a model which seeks to provide an assessment of the maturity level of a country's cybersecurity capabilities, assigning a specific stage which corresponds to their degree of cybersecurity attainment. The five stages of maturity, which are assigned through an evaluation, range from the most basic (Start-up) to the most advanced (Dynamic).

The five stages are defined[34] as follows (see Figure 1):

- ***Start-up:*** At this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.

- ***Formative:*** Some aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined—or simply new. However, evidence of this aspect can be clearly demonstrated.

- ***Established:*** The elements of the aspect are in place, and functioning. However, there is no well-thought-out consideration of the relative allocation of resources. Little trade-off decision making has been carried out concerning the relative investment in this aspect. But the aspect is functional and defined.

- ***Strategic:*** At this stage, choices have been made about which indicators of the aspect are important, and which are less important for the particular organization or state. The Strategic stage reflects the fact that these choices have been made, conditional upon the state's or organization's particular circumstances.

- ***Dynamic:*** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict, or a significant change in one area of concern (e.g., cybercrime or privacy). Dynamic organizations have developed methods for changing strategies in stride. Rapid decision making, reallocation of resources, and constant attention to the changing environment are features of this stage.

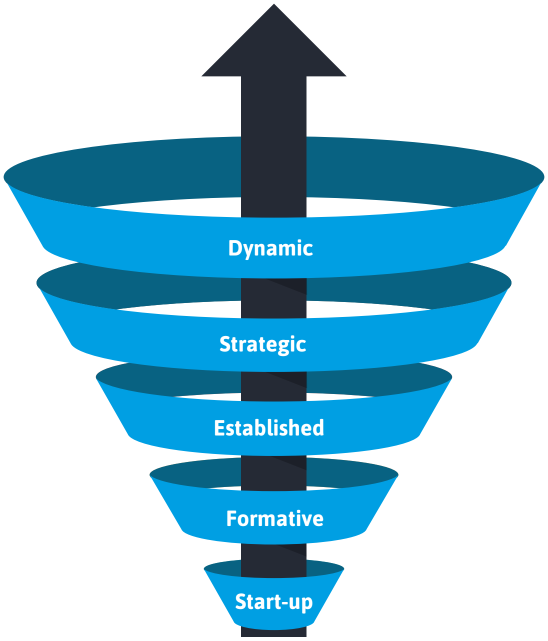


Figure 1: The Five Stages of Maturity

The assessment of the maturity levels is divided into five dimensions (see Figure 2) that correspond to essential and specific aspects of cybersecurity: (i) Cybersecurity Policy and Strategy; (ii) Cyberculture and Society; (iii) Education, Training, and Skills; (iv) Legal and Regulatory Frameworks; and (v) Standards, Organizations, and Technologies. These are further subdivided into a set of factors that describe and define what it means to possess cybersecurity capacity in each dimension, and indicate how to enhance maturity.

The following table details the factors that compose the dimensions:

Dimension 1 Cybersecurity Policy and Strategy (devising cybersecurity strategy and resilience)	**D1.1** National Cybersecurity Strategy **D1.2** Incident Response **D1.3** Critical Infrastructure (CI) Protection **D1.4** Crisis Management **D1.5** Cyberdefense **D1.6** Communications Redundancy
Dimension 2 Cyberculture and Society (encouraging a responsible cybersecurity culture within society)	**D2.1** Cybersecurity Mind-set **D2.2** Trust and Confidence on the Internet **D2.3** User Understanding of Personal Information Protection Online **D2.4** Reporting Mechanisms **D2.5** Media and Social Media
Dimension 3 Cybersecurity Education, Training, and Skills (developing cybersecurity knowledge)	**D3.1** Awareness Raising **D3.2** Framework for Education **D3.3** Framework for Professional Training

Dimension 4 Legal and Regulatory Frameworks (creating effective legal and regulatory frameworks)	**D4.1** Legal Frameworks **D4.2** Criminal Justice System **D4.3** Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 Standards, Organizations, and Technologies (controlling risks through standards, organizations, and technologies)	**D5.1** Adherence to Standards **D5.2** Internet Infrastructure Resilience **D5.3** Software Quality **D5.4** Technical Security Controls **D5.5** Cryptographic Controls **D5.6** Cybersecurity Marketplace **D5.7** Responsible Disclosure

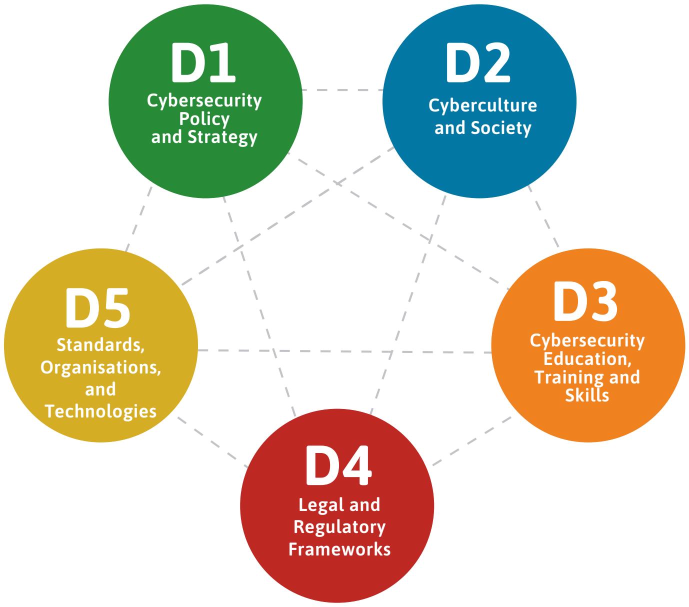

D1
Cybersecurity Policy and Strategy
D2
Cyberculture and Society
D3
Cybersecurity Education, Training and Skills
D4
Legal and Regulatory Frameworks
D5
Standards, Organisations, and Technologies

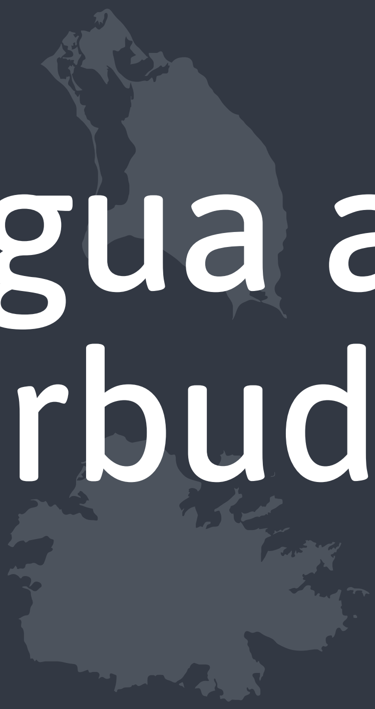
Figure 2: The Five Dimensions of the CMM

The primary data used in this report was collected using an online instrument that was distributed to all Organization of American States (OAS) member states. Following the collection of data from the online instrument, this was cross-referenced with desktop research and consultation with member states for validation of stated findings. Using the CMM as a baseline, this report presents results of the cybersecurity capacity review of Latin America and the Caribbean based on data validated by December 2019. Each country profile concludes with a summary table that lists the five dimensions and their respective level of maturity according to the 2016 and 2020 reports.

The 2016 values used were updated to reflect the Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition. All assessments conducted in the 2016 publication remain the same except for the inclusion of new indicators.

Country Profiles

Antigua and Barbuda



Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
95,426	184,000	72,524	76%

Despite Antigua and Barbuda not having formally adopted a national cybersecurity strategy or established a national CSIRT, there have been significant steps taken in addressing cybersecurity at the national level. In 2017, the government created the position of Director of Cybersecurity under the Ministry of Information, Broadcasting, Telecommunications, and Information Technology and appointed an official in November of that same year.

In terms of cybersecurity activities, in March 2016, Antigua and Barbuda participated in the Caribbean Stakeholder's Meeting II on Cybersecurity and Cybercrime organized by the Caribbean Telecommunications Union (CTU) in conjunction with the Commonwealth Secretariat, where a regional cybersecurity action plan was presented.[35] The action plan includes areas such as training, legislation, technical capacity, and law enforcement.[36] Moreover, in May 2017, Antigua and Barbuda hosted the ICT Week & Symposium and among the topics discussed was cybersecurity and cybercrime.[37] Antigua and Barbuda also actively collaborates with international and regional organizations such as INTERPOL and CARICOM IMPACS for the investigation of digital crimes. Furthermore, the Ministry of Information, Broadcasting, Telecommunications, and Information Technology had in its budget for the 2017 fiscal year a reference to retaining specialists to address cybersecurity matters, and to create a CSIRT.[38]

Antigua and Barbuda has some, albeit limited, cybersecurity service provision by the private sector. However, there seems to be limited engagement from the private sector and civil society in cybersecurity issues, although some companies have begun to make cybersecurity a priority by identifying high-risk practices and getting training in cybersecurity.[39]

Antigua and Barbuda is part of the international STOP.THINK.CONNECT campaign that promotes safe practices on the internet.[40] In terms of availability of formal training for cybersecurity, although there are no dedicated degrees, the Antigua & Barbuda International Institute of Technology does provide degrees in IT and computer science.[41] In June 2013, the government launched a national ICT in Education Policy for the country.

Antigua and Barbuda has had legislation on electronic crimes and data protection since 2013. More specifically, the Electronic Crimes Act provides for the "prevention and punishment of electronic crimes and for related matters." In addition, the Data Protection Act was also enacted in 2013 and provides for the protection of private information stored in both public and private databases. This law covers both the protection of personal data and the transparency in the processing of personal data. [42]

There has also been significant progress made in offering citizens a limited number of government services online, such as renewing driver's licenses.[43] Additionally, Antigua and Barbuda hosted the 21st Century Government Summit and Symposium in January 2018 on the most effective ways to use ICT to provide and deliver services to its citizens.[44] This event shows a willingness to keep moving forward in the development of their e-government capabilities.

Indicators: Antigua and Barbuda

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■■□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■■□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■□□□
Organization	■□□□□	■■□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■□□□□	■■□□□
User Trust in E-government Services	■□□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■□□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■□□□□	■□□□□
Uptake	■□□□□	■□□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■□□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■□□□□	■■■□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■□□□□	■□□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■□□□□	■■□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■□□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■■□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■■□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Argentina

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
44,044,811	61,897,379	32,723,051	74%

In recent years, Argentina has taken multiple measures to implement policies, as well as administrative and regulatory changes for the telecommunications, internet, and technology sectors in the country. In 2017, the enactment of Decree 577/2017 led to the creation of the Cybersecurity Committee under the Secretary of the Government of Modernization of the Chief of the Cabinet of Ministers, which included representatives of the Ministry of Defense and the Ministry of Security, with the purpose of continuing work in the development of a national cybersecurity strategy.[46] An Administrative Act bill is in process, which will expand the configuration of the Cybersecurity Committee. The National Cybersecurity Strategy was approved through a resolution published in the Official Gazette (829/2019) which created "the Executing Unit"[47] within the framework of the Cybersecurity Committee and within the authority of the Secretariat of Modernization of the Nation and invited the Provinces and the Autonomous City of Buenos Aires to adhere to the Strategy.[48]

The IDB, through a policy-based loan (PBL) approved in 2019, supports the Argentine government in the implementation of policies related to critical infrastructure, the security of personal data, and good practices in the use of ICT, with specific actions towards strengthening national cybersecurity capabilities.[49] In addition to strengthening international ties and its cybersecurity policies, Argentina has partnered with the United States to establish a working group that will improve cooperation on cybersecurity.[50] Agreements with countries such as Spain and Chile have been signed and memoranda of understanding with Korea, Russia, and China are being analyzed.[51]

Argentina has also established a National Program of Critical Infrastructures for Information and Cybersecurity (ICIC), created under JGM Resolution No. 580/2011 to create and adopt a regulatory framework to define and protect the strategic and critical infrastructure of the public and private sectors, as well as interjurisdictional organizations.[52] ICIC is, among other things, the home of the national CSIRT. Although the ICIC-CERT is not a member of CSIRT Americas, BA-CSIRT (the CSIRT of the City of Buenos Aires) is a member and can benefit from the network.

Although ICIC collaborates with the private sector, a PwC report found that 53 percent of companies surveyed in Argentina do not have a general cybersecurity strategy, 61 percent do not have a contingency plan on how to respond to an incident, and only 46 percent have a safety program for employees.[53]

There are several opportunities for Argentines to continue their education in cybersecurity, in public and private universities as well as offerings by civil society. In addition, BA-CSIRT offers training and awareness-raising talks to teach stakeholders about cybersecurity and the use of ICTs. As for legislation, Argentina enacted Law No. 26.388 in 2008, amending the criminal code to include cybercrime.[54] In addition, Law No. 26.904 incorporated grooming into the criminal code. Harming critical infrastructure and other crimes are typified in a bill soon to be sent to National Congress.[55] In addition, Argentina's accession to the Council of Europe's Budapest Convention on Cybercrime was ratified in June 2018.[56]

Argentina's Law 25.326, passed in 2000, covers personal data protection.[57] In fact, Argentina was one of the first countries in the Americas to have a regulatory framework for the protection of personal data, and it has strengthened and updated it since then. It is one of the few countries in the Americas that participates in the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe.[58] In 2018, a bill amending Law 25.326 was submitted to update the current regulatory framework.

Argentina has two decrees on e-government: Decree No. 378/2005, describing the e-government strategy to increase ICTs to improve the delivery and provision of government services;[59] and the more recent Decree No. 87/2017, for creating a digital platform to facilitate interaction between people and the State.[60] Decree No. 996/2018 created the Argentina Digital Agenda, which involves "developing cybersecurity skills to build confidence in digital environments."[61]

Indicators: Argentina

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■■□□□	■■□□□
Organization	■■□□□	■■■□□
Content	■■□□□	■■□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■■■■□	■■■■□
Organization	■■■□□	■■■□□
Coordination	■■□□□	■■■□□
Mode of Operation	□□□□□	■■□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Risk Management and Response	■■□□□	■■□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■■□□□	■■□□□

1-5 Cyberdefense

	2016	2020
Strategy	■■□□□	■■□□□
Organization	■■■□□	■■■□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■■□□□	■■□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■■□□□	■■□□□
Private Sector	■■□□□	■■■□□
Users	■■□□□	■■□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■■□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■■□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■□□□
Executive Awareness Raising	■■■□□	■■■□□
3-2 Framework for Education		
Provision	■■■□□	■■■□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■■□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■□□	■■■■□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■■□□
Consumer Protection Legislation	□□□□□	■■■□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■■□□	■■■□□
4-2 Criminal Justice System		
Law Enforcement	■■■□□	■■■□□
Prosecution	■■■□□	■■■□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■■□□□	■■□□□
Standards in Software Development	■■□□□	■■□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■■□□□	■■□□□
Cybercrime Insurance	■■□□□	■■□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■■□□□

Bahamas
(Commonwealth of The)

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
381,761	353,540	324,497	85%

The Government of the Commonwealth of The Bahamas began efforts in 2014 for the development of a national cybersecurity strategy which contemplated the establishment of the national CSIRT.[62] The development of the cybersecurity strategy and establishment of a national CSIRT is critical given that cybercrime has been on the rise over the last couple of years, even though the country has seen an overall decrease in serious crime.[63] While the strategy has not yet been adopted, in 2017 the Bahamas Police Force combined the Tracing and Forfeiture Section of the Drug Enforcement Unit and the Commercial Crime Section at the Central Detective Unit to create the new Cybersecurity Unit.[64] This unit now provides the country with a centralized actor tasked with protecting the country's cyberspace.

After the country was ranked 129th in the Global Cybersecurity Index (GCI), the leaders of the private sector expressed the need for improvements in cyber readiness in the country.[65] Although there are some private-sector providers of cybersecurity services and trainings, there is still a general need for more involvement from the private sector to actively protect themselves from cyberattacks.

The Bahamas passed legislation for both cybercrime and data protection in 2003, namely the Computer Misuse Act and the Data Protection Act. The former provides a comprehensive overview of the criminal acts as well as the procedural aspects of prosecuting cybercrime,[66] while the latter encompasses the definitions and procedures for both private and public data controllers to comply with.[67] Additionally, the government has put in place the Electronic Communication & Transactions Act (2006).

The IDB has been promoting and encouraging the strengthening of cybersecurity policies and actions in the Bahamas. Through a loan operation titled Government Digital Transformation to Strengthen Competitiveness, approved in 2018, the IDB is providing technical and financial support to the digital agenda of the country, which includes a specific component for cybersecurity.[68]

E-government is a part of the Bahamas' Policy Statement on Electronic Commerce and the Bahamian Digital Agenda of 2003 from the Ministry of Finance, with the aim of facilitating information exchange between all the ministries and related agencies.[69] Furthermore, the 2016 draft of the 2040 National Development Plan goes one step further and outlines the need for a "one window service-to-citizen strategy."[70] Currently, the government does provide some services online through the e-services portal for businesses, citizens/residents, and non-residents.[71]

Educational programs focused on cybersecurity are not common in the Bahamas. While the Bahamas Institute of Business and Technology offers a degree in Business Office Technology, there are no degrees specific to cybersecurity.[72] The Bahamas Institute of Financial Services also offers an Advanced Certificate in Cyber Security; however, this program is only three months.[73] Finally, in terms of national awareness efforts, in May 2018, the Bahamas Chamber of Commerce and Employers Confederation (BCCEC) held a Cyber Security Forum, and in June 2018, the Central Bank of the Bahamas held a seminar on information security to increase awareness in cybersecurity and cybercrime, among other topics.[74] In December 2019, the Government of the Bahamas and the IDB held a joint conference to share international experiences in cybersecurity.

Indicators:

Bahamas (Commonwealth of The)

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■□□□□	■□□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■□□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■□□□□	■■□□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■■□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■■□□□	■■□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■■□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■□□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■■□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Barbados

Residents

Ref: World Bank*

2017

286,233

Cell Phone Subscriptions

Ref: ITU**

2017

329,565

Persons with Internet Access

2017

234,026

Internet Penetration

Ref: ITU**

2017

82%

The Government of Barbados is in the early stages of discussion with stakeholders for the development of a national cybersecurity strategy.[75] This multi-stakeholder process provides for inputs from a number of different stakeholders, thus allowing for the development of a strategy that meets the needs of a large number of parties. Furthermore, regardless of not having a cybersecurity strategy, Barbados does have a national CSIRT under the Telecommunications Unit of the Ministry of Innovation, Science, and Smart Technology. The CSIRT is also a member of CSIRT Americas, and benefits from the collaborative nature of the platform. The IDB is cooperating with the Government of Barbados to support its cybersecurity initiatives and policies which will strengthen the capacity of the country to manage cyberthreats. As a result of the "Public Sector Modernization Program" loan operation, approved in November 2019, the IDB is providing technical and financial assistance to the country's digital agenda, which includes specific support for cybersecurity.[76]

During the Internet Governance Forum in Barbados in June of 2017, it was highlighted that more awareness campaigns for citizens were needed as there was a general consensus that citizens may not be aware of the threats they are exposed to when using the internet,[77] despite efforts from private-sector companies to make cybersecurity a priority. Interestingly, the Barbados' Data Processing Department, the Telecommunications Unit, the Defense Force, and the Barbados Investment and Development Corporation (BIDC) joined forces with the Caribbean Israel Centre for Cyber Defense (CICCD) to raise awareness on cybersecurity risks and their importance to Barbados, particularly in light of the new European General Data Protection Regulation (GDPR), which could lead to significant fines in cases of cybersecurity breaches of any institution that deals with information of EU citizens.[78] Additionally, although there are some private-sector providers of cybersecurity services, these are limited.[79]

Barbados has the Computer Misuse Act, which encompasses substantive and procedural law for cybercrime.[80] Furthermore, Barbados currently has draft legislation for data and privacy protection as the bill for the Data Protection Act, which will apply to any data controller established in Barbados or that uses equipment in Barbados for processing data.[81]

Barbados has an e-government strategy from 2006 which has as its vision "to empower the citizens of Barbados by improving the convenience, speed, efficiency, quality and variety of services and information delivered by government."[82] E-government is also mentioned in part of the National ICT Strategic Plan 2010–2015 as a tool through which the government can become a model for the use of ICTs for service delivery. The ICT Plan also calls for a steering committee to oversee the implementation of an e-government policy.[83] The prime minister announced in 2017 that a Digital Government Strategy was in the process of being launched to provide a road map for the work still needing to be done for the digitalization of services provided by the government.[84] So Barbados is on the way to having a clear path towards e-governance. Furthermore, Barbados has taken strong strides in leading technologies such as block-chain technology and has been undertaking projects for the implementation of a digital payment network.[85]

Lastly, in 2017 one of the next steps outlined at the Internet Governance Forum was for the Internet Society, the Telecommunications Unit, and the University of the West Indies to partner with the Ministry of Education, Science Technology, and Innovation to promote knowledge from an early age on how the internet works.[86] Regarding further education, there are no degrees in cybersecurity, although the University of the West Indies does provide degrees in computer science.[87]

Indicators: Barbados

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■■□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■□□□□	■□□□□

1-5 Cyberdefense

	2016	2020
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■■□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■□□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■■□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■■□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■□□□□	■■□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■□□□□	■□□□□
Uptake	■□□□□	■□□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■□□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■□□□□	■■□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■□□□□	■■■□□
5-3 Software Quality		
Software Quality	□□□□□	■□□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Belize

Residents

Ref: World Bank*

2017

375,769

Cell Phone Subscriptions

Ref: ITU**

2017

239,441

Persons with Internet Access

2017

176,922

Internet Penetration

Ref: ITU**

2017

47%

The Government of Belize is currently developing a national cybersecurity strategy through a multi-stakeholder process, namely, the National Cyber Security Task Force (CSTF). The CSTF is charged with drafting the national cybersecurity strategy through a process of consultation with national stakeholders. Further, Belize has developed new initiatives related to information technology including a national policy that intends to expand e-government services in the country. In an attempt to raise awareness about the risks and opportunities related to cybersecurity, on April 2017, the Belize Public Utilities Commission (PUC) organized the First National Cyber Security Symposium in Belize City. One of the objectives of the symposium was to identify next steps to develop a cybersecurity and cybercrime agenda, so the country is on the way to beginning the process.

Although there is a general lack of awareness and private-sector engagement regarding cybersecurity in Belize, the Cyber Security Symposium was a push in the direction of increasing awareness on the importance of cybersecurity. The participation of law enforcement, the judiciary and legal community, government, and the private sector shows the growing importance of the subject for all parties.[88] Regarding cybersecurity education and trainings, the offering remains in the hands of the private-sector firms that provide trainings. There are no cybersecurity degrees at Belizean universities, although the Faculty of Science and Technology of the University of Belize does offer a bachelor's degree in information technology.[89]

In order to develop a stronger cybersecurity mind-set, the Central Information Technology Office (CITO) promotes cybersecurity awareness among different government institutions by sending out monthly surveys with cybersecurity tips and best practices. CITO has also developed a survey that intends to improve the reporting of cyberincidents among public institutions. The IT Unit of the Belize Police Department has also made considerable efforts to improve their incident-response capabilities through the development of a forensic laboratory. Currently, Belize has four laws that relate to cybersecurity: (i) the Telecommunications Act, (ii) the Electronic Evidence Act, (iii) the Intellectual Property Act, and (iv) the Interception of Communications Act, but has no privacy and data protection legislation.[90] Additionally, the Belize Police Department has a partnership with the Internet Watch Foundation in order to report cases of child pornography. However, the lack of comprehensive cybercrime law hinders the prosecution of cyberrelated crimes.[91] There is a need for updating of the country's legislation and law-enforcement framework to be able to criminalize and prosecute such crimes, and the government has been analyzing cybercrime laws from similar countries in order to develop their own national legislation that allows for a more thorough prosecution of cyber-related crimes.

There is a comprehensive e-government plan that details the road map for the design and implementation to achieve the country's e-government vision of "an integrated, collaborative government delivering secure, quality public services that connect and empower people."[92] However, up until now an e-government portal has not been implemented.

Indicators: Belize

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■□□□□	■■□□□
Organization	■□□□□	■■□□□
Content	■□□□□	■□□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■■□□□	■■□□□
Organization	■□□□□	■■□□□
Coordination	■■□□□	■■□□□
Mode of Operation	□□□□□	■□□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■□□□□	■□□□□
Organization	■□□□□	■■□□□
Risk Management and Response	■□□□□	■□□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■□□□□	■□□□□

1-5 Cyberdefense

	2016	2020
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■■□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■■□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■□□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■■□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■□□□□	■□□□□
Administration	■□□□□	■■□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■□□□□
Child Protection Online	□□□□□	■□□□□
Consumer Protection Legislation	□□□□□	■□□□□
Intellectual Property Legislation	□□□□□	■□□□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■□□□□	■□□□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■□□□	■■□□□
Prosecution	■□□□□	■□□□□
Courts	■□□□□	■□□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■■□□□	■■■□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■□□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■■□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■□□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■■□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Bolivia

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
11,192,854	10,963,224	4,906,083	44%

In recent years, Bolivia has taken the first steps to improve the country's cybersecurity, with the Senate approving a law in 2017 that declares the development of a national cybersecurity strategy as a priority for the country.[93] Additionally, Supreme Decree No. 2514 of September 2015 established the creation of the E-government and Information and Communication Technologies Agency (AGETIC) with the aim of leading the process of development and implementation of e-government and ICTs for the transformation of public management and the construction of scientific and technological sovereignty of the Plurinational State of Bolivia.[94]

Supreme Decree No. 2514 also created the Cyber-incident Management Center (CGII), with the mission of protecting state-critical information and promoting security awareness to prevent and respond to security incidents.[95] In addition, the CGII is part of the CSIRT Americas platform developed by the OAS, the objective of which is to promote collaboration, exchange, encouragement, and participation in technical projects among national, defense, police, and government CSIRTs of the member countries.[96]

Bolivia's private sector is active in the field of cybersecurity. Several companies offer cybersecurity and security services, and in general, there is awareness of cybersecurity by the private sector.[97]

There is no specific legislation on cybercrime or protection of personal data, but there is existing legislation that can be applied to address cybercrimes,[98] access to information,[99] and other related issues. Likewise, a separate section on privacy protection was included in the 2009 constitution.

In the field of e-government, Bolivia has taken important steps to develop a plan for the implementation of e-government from 2017 to 2025. The objective of this plan is to modernize and make the country's public management more transparent and generate and establish a technological mechanism to increase participation and social awareness with the use of ICTs by the population.[100] In addition, in 2018, a law with the purpose of "establishing conditions and responsibilities for full access and exercise of digital citizenship" in Bolivia was approved.[101]

There are degree courses on topics related to cybersecurity. In addition, there are some opportunities in the public and private sector for training in e-government and cybersecurity.

Indicators: Bolivia

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■■□□□
Content	■□□□□	■■□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■■■□□
Organization	■■□□□	■■■□□
Coordination	■■□□□	■■□□□
Mode of Operation	□□□□□	■■□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■■□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■■□□□
Organization	■■□□□	■■□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■□□□□	■■□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■■□□□	■■□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■□□□□
Child Protection Online	□□□□□	■□□□□
Consumer Protection Legislation	□□□□□	■□□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■■□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■□□□□	■□□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■■□□□
Standards in Software Development	■□□□□	■■□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■■□□□

Brazil

Residents

*Ref: World Bank**

2017

207,833,831

Cell Phone Subscriptions

*Ref: ITU***

2017

218,255,041

Persons with Internet Access

2017

140,228,155

Internet Penetration

*Ref: ITU***

2017

67%

On 5 February 2020, Brazil published Federal Decree No. 10.222 ("the Decree"), approving the National Cybersecurity Strategy.[102] More specifically, the Decree seeks to guide Brazil's approach to cybersecurity and includes actions to increase its resiliency against cyberthreats, and strengthen its performance internationally. In addition, the Decree creates a centralized governance model at the national level to promote coordination among different actors related to cybersecurity, establish a national cybersecurity council, and encourage internal cybersecurity compliance checks on public and private entities.

Brazil has a multitude of CSIRTs which range from government entities to private-sector and academic facilities. Depending on the role of a CERT, these entities may be involved exclusively in managing the security of systems, enforce cybersecurity guidelines, or be responsible for coordinating efforts between national authorities and local levels.

The maturity of Brazil's capacity to protect critical infrastructure differs between public and private critical infrastructure operators. All federal institutions are required to conduct cyber risk assessments, which are updated annually based on lessons learned from major events. Public critical infrastructure stakeholders comprise telecommunication companies and transport, energy, and financial institutions, all of which cooperate and coordinate through formal channels of communication with the Ministry of Defense. There are clearly defined policies and procedures in place for all public institutions to follow based on information provided by the national CERT's situational awareness tool. The national CERT (CERT.br) continues to be the main entity responsible for handling incident reports at a national level and activities on Brazilian networks.

A national program for cybersecurity awareness raising, led by a designated organization (from any sector) which addresses a wide range of demographics, is yet to be established. Nevertheless, the government has recognized the need to prioritize cybersecurity across its institutions and a growing number of users and stakeholders within the public and private sectors are perceived to have general knowledge about how personal information is handled online and to employ good (proactive) cybersecurity practices to protect their personal information online.

The Brazilian Civil Rights Framework for the Internet (Law No. 12.965, in Portuguese the Marco Civil da Internet) was developed via a multi-stakeholder consultation process in order to regulate the use of the internet in Brazil through establishing principles, guarantees, rights, and duties for internet users. However, Brazil does not have a specific data-protection or privacy law, but relies on various provisions stated in the federal constitution,[103] the Brazilian Penal Code,[104] the Consumer Protection Code,[105] and the Brazilian Civil Rights Framework for protecting privacy on the internet.

Notably, some aspects of governmental processes and institutional structures have been designed in response to risks to cybersecurity, but initiatives are based primarily in particular leading agencies. Overall, the cybersecurity culture in Brazil varies across different parts of the country and different sectors of government and the economy. The finance sector and the IT sector are more advanced in cybersecurity, due to being frequent targets, and therefore are investing more in cybersecurity. Nevertheless, society as a whole still lacks a cybersecurity mind-set. Users might be aware of cybersecurity risks, but they often fail to act accordingly in their everyday practices.

The need for enhancing cybersecurity education in schools and universities has been identified by leading government and industry stakeholders. Qualifications for cybersecurity and a supply of educators are readily available. Specialized courses in computer science are offered at the university level. Professionals within the public sector attend IT professional qualifications abroad and receive ICT certificates authorized by international institutions such as Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

Finally, a vulnerability-disclosure framework is in place for the federal government. Organizations have established formal processes to disseminate information automatically and the national CERT receives this information and provides comprehensive reports on how to address incidents.

Indicators: Brazil

D1 Cybersecurity Policy and Strategy

D1	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Content	■■□□□	■■□□□
1-2 Incident Response		
Identification of Incidents	■■■□□	■■■■□
Organization	■■■■□	■■■■□
Coordination	■■■□□	■■■■□
Mode of Operation	□□□□□	■■■□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■■□□
Organization	■■□□□	■■■□□
Risk Management and Response	■■□□□	■■■□□
1-4 Crisis Management		
Crisis Management	■■□□□	■■■□□
1-5 Cyberdefense		
Strategy	■■■□□	■■■□□
Organization	■■■□□	■■■□□
Coordination	■■□□□	■■□□□
1-6 Communications Redundancy		
Communications Redundancy	■■□□□	■■□□□

D2 Cyberculture and Society

D2	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■□□□
Private Sector	■■■□□	■■■□□
Users	■■□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■■□□	■■■□□
User Trust in E-government Services	■■■□□	■■■□□
User Trust in E-commerce Services	■■■□□	■■■□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■■□□
Executive Awareness Raising	■■■□□	■■■□□
3-2 Framework for Education		
Provision	■■■□□	■■■□□
Administration	■■□□□	■■□□□
3-3 Framework for Professional Training		
Provision	■■■□□	■■■□□
Uptake	■■■□□	■■■□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■□□	■■■■□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■□□	■■■■□
Data Protection Legislation	□□□□□	■■■■□
Child Protection Online	□□□□□	■■■□□
Consumer Protection Legislation	□□□□□	■■■■□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■■□□	■■■■□
Procedural Cybercrime Legislation	■■■■□	■■■■□
4-2 Criminal Justice System		
Law Enforcement	■■■■□	■■■■□
Prosecution	■■□□□	■■■□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■■■□
Standards in Procurement	■■□□□	■■□□□
Standards in Software Development	■■□□□	■■□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■■□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■■□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■■□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■■■□□	■■■□□
Cybercrime Insurance	■■■□□	■■■□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■■■□□

Chile

Residents

Ref: World Bank*

2017

18,470,439

Cell Phone Subscriptions

Ref: ITU**

2017

23,013,147

Persons with Internet Access

2017

15,206,248

Internet Penetration

Ref: ITU**

2017

82%

Chile issued its National Cybersecurity Policy in April 2017, with the aim of satisfying the following objectives by the year 2022: (i) have a robust and resilient information infrastructure; (ii) have the state guarantee the rights of people in cyberspace; (iii) develop a cybersecurity strategy based on education, good practices, and responsibility in the management of digital technologies, establishing cybersecurity cooperation relationships with other actors; and (iv) promote the development of a cybersecurity industry to meet its strategic objectives.[106] In addition, in 2018, in accordance with the National Cybersecurity Policy, the president of the republic appointed a presidential adviser that informs him directly about cybersecurity issues, and a restructuring was carried out in the Subsecretariat of the Interior to carry out the measures described in the aforementioned policy through the Cybersecurity Coordination Unit (Exempt Resolution No. 5.006).

During that year, the advisor promoted a series of measures related to the strategic objectives. One of these was the strengthening of the government CSIRT that depends on the Ministry of Interior and Public Security,[107] in accordance with the National Cybersecurity Policy.[108] In addition to the above, in March 2018, a National Cyberdefense Policy was approved; one specific unit was created for coordination of national defense, which depends on the Ministry of Defense, and another for the industry/strategic sectors through the Ministry of Finance. Through the recently approved Program for Strengthening the Strategic Management of Public Security in Chile, the IDB and the Government of Chile agreed to include a specific component to strengthen the strategic management of public security to ensure "an open, safe and resilient cyberspace."[109] In parallel, the IDB supports the Chilean government with technical advice in assessing the levels of cybersecurity preparedness and response in the country with the objective of identifying, planning, and designing improvements. The CSIRT of the Government of Chile is also a member of CSIRT Americas, which gives access to all the information that the platform has to offer, including the dynamic exchange of information through the Malware Information Sharing Platform and Threat Sharing (MISP) deployed in the hemispheric network.

Additionally, the government coordinates financial regulators in cybersecurity and operational risk in general through the Operational Continuity Working Group of the Financial Stability Board. The group's mandate is to analyze the operational risks of the financial market infrastructure and its participants and main users, including banks, securities brokers, pension funds, and insurance companies, and propose the necessary legal and regulatory changes to mitigate these risks and their effects on the financial system. The members of this working group are from the Ministry of Finance, the Central Bank of Chile, the Commission for the Financial Market, and the Superintendence of Pensions, and they usually meet once a month.

One of the steps to achieve the first objective of the cybersecurity strategy is to identify and prioritize the country's critical information infrastructure. According to the strategy, "the information infrastructure of the following sectors will be considered critical: energy, telecommunications, sanitation services, health, financial services, public security, transport, public administration, civil protection and defense, among others."[110]

The strategy also orders the Ministry of Interior and Public Security to create a permanent working group to establish a regulatory framework for critical infrastructure in Chile.[111] In addition, according to the strategy, "the pertinence of creating a CSIRT of critical infrastructure should be evaluated." The private sector, academia, and civil society have also been active players, supporting the drafting of the national cybersecurity strategy after a public consultation was conducted.[112]

The recently created Chilean Cybersecurity Alliance brings together public and private organizations as well as academic institutions to promote education and the responsible use of technology and to generate communication channels between the private sector and the government, among other things.[113] However, after the 2018 cyberattacks, there has been greater concern on the part of companies, and private-sector organizations may need to strengthen their networks and systems. [114] In any case, there are several cybersecurity service providers in Chile.

Chile has a legal framework that is undergoing modifications associated to computer-related crimes and the protection of personal data. However, in the area of cybercrime, Law No. 19.223 from 1993 which penalizes those who carry out illicit activities on information systems.[115] To protect personal data, Chile passed Law No. 19.628.[116] In addition, in 2018, a reform to numeral 4 of article 19 of the Political Constitution of the Republic of Chile was approved, which recognized the right to honor and private life, and introduced the protection of personal data.[117] Currently, two bills are being processed in Congress, one that modifies the regulations on Protection of Personal Data (Bulletin No. 11.144-07[118]) and another that adapts Chilean regulations to the Budapest Convention on Cybercrime in addition to making modifications to other legal bodies (Bulletin No. 12.192-25[119]). Finally, there are legal initiatives in financial matters — modifications to the General Law of Banks in the field of operational risk and the incorporation of specific rules of Information on Operational Incidents (RAN 20-8) and Management of Business Continuity (RAN 20-9) of the Commission for the Financial Market (CMF).

It should be noted that the government has made a commitment to introduce the Cybersecurity Framework Bill by the end of 2019. In addition to legal efforts in this area, work has been carried out on the modification of regulatory bodies with the purpose of improving cybersecurity standards within the state administration and effectively articulating the functions of the Interministerial Cybersecurity Committee.

The United Nations ranked Chile the second most-developed country in terms of e-government among the Latin American and Caribbean countries in 2018.[120] In addition, digital government is part of the 2020 Digital Agenda, which consists of "a roadmap that defines the next steps to achieve an inclusive and sustainable development policy using Information and Communication Technologies (ICT)."[121] E-government is one of the axes of the 2020 Digital Agenda, together with the Rights for Digital Development, Digital Connectivity, Digital Economy, and Digital Competencies.[122] On January 24, 2019, a Presidential Instruction on Digital Transformation was issued which includes four lines of action: Digital Identity, Zero Lines, Zero Paper, and Coordination and Monitoring.[123] On November 11, 2019, Law No. 21.180 on Digital Transformation[124] was published, which involves a comprehensive reform in the matter of administrative procedures within the state, establishing 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 bodies of the state administration.

Cybersecurity-related programs at the undergraduate, postgraduate, and specialization levels are available in public and private universities in Chile. Other initiatives are being developed, such as one by the Ministry of Education, whose *Internet Segura* ("Safe Internet") project has the purpose of "delivering tools to adults so that they can accompany children and young people in their digital journey" and delivering "guidance to primary and secondary schools, from a more pedagogical perspective, so that they can educate digital citizens aware of their rights and duties."[125] Since the enactment of the National Cybersecurity Policy, the development of several continuing education and postgraduate education programs in cybersecurity have been promoted, both from a technical and legal perspective, in order to strengthen the human resources trained in these matters.

Indicators: Chile

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■■□□□	■■■■□
Organization	■■□□□	■■■□□
Content	■■□□□	■■■□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■■□□□	■■■□□
Organization	■■□□□	■■■□□
Coordination	■■□□□	■■□□□
Mode of Operation	□□□□□	■■■□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Risk Management and Response	■■□□□	■■□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■■□□□	■■□□□

1-5 Cyberdefense

	2016	2020
Strategy	■■□□□	■■■□□
Organization	■■□□□	■■■□□
Coordination	■■□□□	■■□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■■□□□	■■□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■■□□□	■■■□□
Private Sector	■■■□□	■■■□□
Users	■■□□□	■■■□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■■□□□	■■■□□
User Trust in E-government Services	■■□□□	■■■□□
User Trust in E-commerce Services	■■■□□	■■■□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■■■□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■■■□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■■□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■■□□
Executive Awareness Raising	■■■□□	■■■□□
3-2 Framework for Education		
Provision	■■□□□	■■□□□
Administration	■□□□□	■■□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■■□□
Uptake	■■□□□	■■■□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■□□	■■■□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■■■□
Intellectual Property Legislation	□□□□□	■■■■■
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■■□□	■■■□□
4-2 Criminal Justice System		
Law Enforcement	■■■□□	■■■□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■■□□
Informal Cooperation	□□□□□	■■■□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■■□□
Standards in Procurement	■■□□□	■■■□□
Standards in Software Development	■■□□□	■■□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■■□□	■■■□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■■□□□	■■□□□
Cybercrime Insurance	■■■□□	■■■□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■■□□□

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB
Improving lives

OAS
More rights
for more people

Colombia

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
48,901,066	62,220,014	30,445,745	62%

Colombia adopted a second national cybersecurity policy in 2016, five years after the first one was introduced.[126] The policy's general objective is to strengthen the state's capacity to respond to cybersecurity and cyberdefense threats in the country. The new cybersecurity policy aims to further strengthen the capabilities of all interested parties to identify, manage, treat, and mitigate cybersecurity risks.[127] One of the main contributions of the new policy is creating the role of a National Digital Security Coordinator, housed in the Office of the President of the Republic of Colombia.

Likewise, the government created the main entity responsible for inter-sectoral cybersecurity issues, the Cybersecurity Committee, which is steered by the National Cybersecurity Coordinator.[128] Additionally, within its management and performance policies,[129] the national government included the cybersecurity policy for the first time as an integral part of public and private entities' strategic operation.

At the same time, the Ministry of Technology and Communications (MinTIC) has deployed the Security and Privacy of Information Model at the national and local levels to support the management and implementation of good practices and standards to protect critical information assets, technological infrastructure, and systems of information and communications, thus promoting continuous improvement.

Colombia also established colCERT, a national computer incident response team currently under the Ministry of National Defense that is in charge of initial response to cyberincidents and protecting the critical national cybernetic infrastructure (ICCN).[130] In addition, a plan to strengthen the protection of critical cybernetic infrastructure has been developed, using the Guide for Identification of ICCN, in addition to the sectoral protection of ICCN plans.[131] In support of the digital transformation of Colombia, at the end of 2018 the IDB approved the Program for the Improvement of Connectivity and Digitalization of the Economy through a policy-based loan (PBL).[132] This program specifies initiatives to strengthen national cybersecurity capabilities. While the government has taken significant steps to secure the country's cyberspace with the two cybersecurity policies, the private sector (particularly small and medium enterprises) still has a long way to go to be prepared for the current cyberthreats.

Colombians have ample opportunities to continue their studies in cybersecurity, both at the undergraduate and postgraduate levels. In addition, MinTIC has awarded scholarships to public servants in the areas of cybersecurity and cyberdefense.[133] MinTIC also sponsors cybersecurity courses and training for the different public service branches related to ICTs.[134] Several training programs have been conducted in collaboration with other institutions such as MinTIC, OAS, and Citi Foundation, benefiting 40 low-income engineering students.[135] Finally, MinTIC's "En TIC Confío" ("I Trust ICT") campaign seeks to promote and raise awareness about the responsible use of the internet and ICTs.[136]

Cybercrime is covered in Law No. 1273 of 2009 that modifies the criminal code to include this type of crime.[137] For the protection of data and privacy, Colombia promulgated Law No. 1581 in 2012.[138] Additionally, Colombia has a delegate office for the protection of personal data,[139] which is responsible, among other issues, for ensuring that all regulations related to data protection are followed, and for disclosing to users their rights regarding the protection of personal data. This law applies to public and private databases.

Colombia is a member of both INTERPOL and Europol[140] and has prioritized its participation in international scenarios.[141] In addition, Law No. 1928 issued on July 24, 2018, approved the Budapest Convention on Cybercrime[142] and deposited the instrument of accession on March 16, 2020.

E-government policy[143] is established in Decree 1008 of 2018. According to it, e-government policy is "the use and exploitation of information and communication technologies to consolidate a competitive, proactive, and innovative state and citizens that build public value in an environment of digital trust."

Indicators: Colombia

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■■□□	■■■■■
Organization	■■□□□	■■■■□
Content	■■■□□	■■■■□
1-2 Incident Response		
Identification of Incidents	■■□□□	■■■□□
Organization	■■□□□	■■■■□
Coordination	■■□□□	■■■■□
Mode of Operation	□□□□□	■■■■□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■■□□
Organization	■■□□□	■■■■□
Risk Management and Response	■■□□□	■■■■□
1-4 Crisis Management		
Crisis Management	■■□□□	■■■■□
1-5 Cyberdefense		
Strategy	■■□□□	■■■■□
Organization	■■■□□	■■■□□
Coordination	■■□□□	■■■□□
1-6 Communications Redundancy		
Communications Redundancy	■■□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■■■□
Private Sector	■■□□□	■■□□□
Users	■■■□□	■■■□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■■□□	■■■□□
User Trust in E-government Services	■■■□□	■■■□□
User Trust in E-commerce Services	■■□□□	■■■□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■■□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■■□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■■□□	■■■□□
Executive Awareness Raising	■■□□□	■■■□□
3-2 Framework for Education		
Provision	■■■□□	■■■□□
Administration	■■□□□	■■□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■■□□
Uptake	■■■□□	■■■□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■□□	■■■□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■■□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■■□□	■■■□□
4-2 Criminal Justice System		
Law Enforcement	■■■□□	■■■□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■■□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■■□□□	■■□□□
Standards in Software Development	■■□□□	■■■□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■■□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■■□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■■□□□	■■□□□
Cybercrime Insurance	■■□□□	■■□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■■□□□

Costa Rica

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
4,949,954	8,840,342	3,533,810	71%

The Ministry of Science, Technology, and Telecommunications of Costa Rica introduced the country's national cybersecurity strategy in 2017 with the aim of developing a framework to steer the country's actions with respect to the safe use of ICT, develop coordination and cooperation efforts among the interested parties, and promote education, prevention, and risk mitigation measures using ICTs.[144] Despite the fact that the national cybersecurity strategy was recently published, Costa Rica had already taken significant steps to secure its cyberspace. A national CSIRT was created in 2012 under the Ministry by Decree No. 37052 to coordinate everything related to information and cybersecurity among the different stakeholders and to form a team of ICT security experts to prevent and respond to cyberincidents against government institutions.[145] In addition, CSIRT-CR is a member of the CSIRT Americas network.

The national strategy defines critical infrastructure as "information systems and networks, which, in case of failure, could have a serious impact on citizens' health, physical and operational safety, economy and welfare, or on the effective functioning of the government and the country's economy." The strategy also describes the need to define the critical infrastructure of the country and create a policy-making committee, comprised of members of public and private entities that have been classified as critical infrastructure.

There seems to be limited knowledge on cybersecurity issues on the part of the private sector, but starting in 2017 companies focused on providing cybersecurity solutions and services began to proliferate.[146] Costa Ricans have many opportunities to continue studying cybersecurity, and some universities offer shorter training and certificate programs.[147] Several capacity-building events have also been carried out in collaboration with international institutions, such as the training provided by the National Cryptologic Center of Spain for public servants and professional training in collaboration with the OAS and Citi Foundation.[148]

In 2012, Costa Rica approved Legislative Decree No. 9048 that reformed the criminal code to formally introduce provisions for cybercrime.[149] Some argue that this is not enough because there are problems with the application of the framework and it is not exhaustive, which leaves crimes such as skimming (stealing credit card information), grooming (befriending a child with the intention of abusing the child), or cyberstalking[150] unregulated. Accession to the Budapest Convention on Cybercrime occurred in 2017, in addition to other conventions, and Costa Rica is developing a national strategy against cybercrime.

For privacy and data protection, Costa Rica has Law No. 8968 on the Protection of the Person against the Processing of Personal Data.[151] This law applies to private and public databases.

Costa Rica has had a draft strategy for e-government since 2010 with the vision of being a reference in Latin America in terms of e-government citizen-focused services, transparency of service, and interconnection of government institutions based on a favorable environment for ICTs and the establishment of an equal and secure society.[152]

Indicators: Costa Rica

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■□□□	■■■□□
Organization	■□□□□	■■□□□
Content	■□□□□	■■■□□
1-2 Incident Response		
Identification of Incidents	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Coordination	■■□□□	■■□□□
Mode of Operation	□□□□□	■■□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■■□□□	■■■□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■□□□
Private Sector	■■■□□	■■■□□
Users	■□□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■■□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 **Awareness Raising**		
Awareness Raising Programs	■□□□□	■■□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 **Framework for Education**		
Provision	■■□□□	■■■□□
Administration	■□□□□	■■□□□
3-3 **Framework for Professional Training**		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 **Legal Frameworks**		
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■□□	■■■□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■■□□
Consumer Protection Legislation	□□□□□	■■■□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■■□□	■■■■□
Procedural Cybercrime Legislation	■■■□□	■■■□□
4-2 **Criminal Justice System**		
Law Enforcement	■■■□□	■■■□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 **Formal and Informal Cooperation Frameworks to Combat Cybercrime**		
Formal Cooperation	□□□□□	■■■□□
Informal Cooperation	□□□□□	■■■□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 **Adherence to Standards**		
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□
5-2 **Internet Infrastructure Resilience**		
Internet Infrastructure Resilience	■□□□□	■□□□□
5-3 **Software Quality**		
Software Quality	□□□□□	■□□□□
5-4 **Technical Security Controls**		
Technical Security Controls	□□□□□	■□□□□
5-5 **Cryptographic Controls**		
Cryptographic Controls	□□□□□	■□□□□
5-6 **Cybersecurity Marketplace**		
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 **Responsible Disclosure**		
Responsible Disclosure	■□□□□	■□□□□

Dominica

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
71,458	75,230	49,749	70%

Dominica has not yet established a national cybersecurity strategy, but it has drafted one in collaboration with the OAS, the Commonwealth Cybercrime Initiative, and the Council of Europe. This draft strategy outlines four pillars: (i) Government and Legal to strengthen the capacity to govern cybersecurity mechanisms and prosecute cybercrime; (ii) Stakeholder Cooperation to distribute the cybersecurity responsibilities between all parties affected; (iii) Capacity Building and Awareness to ensure there are enough technically trained professionals to work in the cybersecurity field; and (iv) Technical Considerations, which calls for the creation of a national CSIRT. Furthermore, the draft strategy defines critical infrastructure as including the power grid, communications, financial delivery methods, water and sewage, transportation, customs, port authorities and country code top-level domain (ccTLD).

There is very limited opportunity for Dominicans to get training in cybersecurity. While there are no cyber-specific degrees offered nationally, Dominica State College does provide bachelor's degrees in computer science and IT.[153] The government, in partnership with the Republic of India, has also opened the ICT Center for Excellence to provide citizens with the opportunity to learn about ICTs. As a next step, the director of telecommunications plans to explore the establishment of a Center of Excellence in Cybersecurity. [154]

Dominica has enacted in recent times several cyber-related legislations such as the Electronic Evidence Act (2010),[155] the Electronic Filing Act (2013),[156] the Electronic Funds Transfer Act (2013),[157] and the Electronic Transactions Act (2013).[158] In relation to the criminalization of cybercrimes, Dominica does have the Electronic Crimes Bill of 2013 to provide for the "prevention and punishment of electronic crimes and for related matters." However, it has not yet been passed into law. Similarly, there is the Data Protection Bill to legislate the protection of private information processed by both public and private bodies. However, like the Electronic Crimes Bill, the Data Protection Bill is still being reviewed and considered for passage into law.

Indicators: Dominica

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■□□□	■■□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■□□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■□□□□	■□□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■□□□□	■□□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■□□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■□□□□	■■□□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■□□□□	■□□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■□□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■□□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■□□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Dominican Republic

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
10,513,131	8,769,127	7,103,852	68%

In June 2018, the Government of the Dominican Republic issued Decree 230-18, adopting its 2018–2021 National Cybersecurity Strategy.[159] This regulation aims to establish adequate cybersecurity mechanisms for the protection of the state, its inhabitants, and, in more general terms, national security and development.

Further, the national strategy is part of the Digital Republic Program created by Decree 258-16,[160] and it proposes 4 general objectives, 13 specific objectives, and 37 lines of action contained in its four pillars: (i) Legal Framework and Institutional Strengthening, (ii) Protection of National Critical Infrastructure and Government IT Infrastructure, (iii) Education and National Culture of Cybersecurity, and (iv) National and International Partnerships. These pillars, developed with the participation of the private sector, aim to establish a dialogue and cooperation mechanism among all sectors of society to promote best practices, identify common problems, and develop appropriate solutions to face cyberthreats.

Framed within the national strategy, the Protection of National Critical Infrastructure and Government IT Infrastructure aims generally: "To ensure the continuous operation and protection of the information stored in national critical infrastructure and relevant IT infrastructure of the State." To achieve this objective, its lines of action consider the establishment of the CSIRT-RD, which will contribute to improving inter-sectoral and institutional coordination for the protection of information systems and the relevant national critical and IT infrastructure of the state and the private sector.

The national strategy considers the establishment of strategic private and public alliances, both locally and internationally, with the purpose of strengthening cooperation and synchronizing efforts to respond to incidents related to cybersecurity. Therefore, it seeks to increase the participation of the private sector and civil society in cybersecurity matters. The fundamental objective of the National and International Partnerships pillar focuses on developing inter-sectoral cooperation at the local and international levels, aiming to share information on incidents, threats, best practices, directives events and initiatives to improve the country's cyberresilience.

The Dominican Republic has specific legislation that covers cybercrime in Law No. 53-07[161] on High Technology Crimes and Offenses. Along the same line is Law No. 172-13,[162] the objective of which is the "comprehensive protection of personal data recorded in archives, public records, data banks or other technical means of data processing to render reports, whether public or private." In addition, the 2010 constitution grants[163] all persons the right to access any data about their person and the right to request the corresponding judicial authority to update, rectify, or destroy any data that may unlawfully affect the rights of a person.[164]

The Dominican Republic offers opportunities for its citizens to receive education on cybersecurity and actions are planned to develop a national cybersecurity culture throughout the population, as well as to strengthen cybersecurity at all educational levels, from basic-level studies to undergraduate, graduate, and master's degrees.

Indicators:

Dominican Republic

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■■■□□
Organization	■□□□□	■■■□□
Content	■□□□□	■■■□□
1-2 Incident Response		
Identification of Incidents	■■□□□	■■□□□
Organization	■■□□□	■■■□□
Coordination	■□□□□	■■□□□
Mode of Operation	□□□□□	■■□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■■□□□	■■□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■□□□
Private Sector	■■■□□	■■■□□
Users	■□□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■■□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■□□□
Executive Awareness Raising	■■□□□	■■■□□
3-2 Framework for Education		
Provision	■■□□□	■■■□□
Administration	■□□□□	■■□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■■□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■■□	■■■■■
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■■□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■■□□
Intellectual Property Legislation	□□□□□	■■■■□
Substantive Cybercrime Legislation	■■■■■	■■■■■
Procedural Cybercrime Legislation	■■■■■	■■■■■
4-2 Criminal Justice System		
Law Enforcement	■■■■□	■■■■□
Prosecution	■■■□□	■■■□□
Courts	■■□□□	■■■□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■■□□
Informal Cooperation	□□□□□	■■■□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■■□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■■□□□	■□□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Ecuador

Residents

Ref: World Bank*

2017

16,785.361

Cell Phone Subscriptions

Ref: ITU**

2017

14,651,404

Persons with Internet Access

2017

9,613,353

Internet Penetration

Ref: ITU**

2017

57%

While Ecuador does not yet have a cybersecurity strategy, the country has made significant advances in improving its cybercapabilities such as the creation of a working group for the development of a national cybersecurity strategy. This is supported by the establishment of EcuCERT, the country's cyberincident response team that depends on the Telecommunications Regulation and Control Agency (ARCOTEL).[165] Additionally, since 2018, the IDB has been providing technical advice to Ecuador to identify, evaluate, and plan levels of preparation in national cybersecurity to set the technical, strategic, regulatory, and governance foundations for the government to use in its formulation of the national cybersecurity strategy. It is important to note that EcuCERT is a member of CSIRT Americas, so they can benefit from the organization's network of collaboration, exchange, stimulation, and participation in technical projects between national, defense, police, and government CSIRTs of the member countries. In addition, the Directorate of Technological Architecture and Information Security is responsible for the coordination of cybersecurity in the country and has as one of its tasks the formulation, evaluation, coordination, and management of government cybersecurity programs.[166]

While there is some provision of cybersecurity services by the private sector, there seems to be a need for improved awareness and preparedness to face cybersecurity threats. A study by Deloitte in 2018 found that 50 percent of companies "have implemented an employee cybersecurity awareness program." In any case, the study found that "70 percent of organizations say they are not sure of the effectiveness of their response process to cybersecurity incidents" and the budget for cybersecurity is the most important barrier for organizations.[167]

There are some courses offered at public and private universities, including training opportunities focused on cybersecurity and other important topics related to ICT. However, Ecuador currently faces a deficit in cybersecurity professionals.[168]

Law No. 2002-67 on electronic commerce, electronic signatures, and data messages penalizes cybercrime and indicates the relevant criminal code reforms. In addition, Articles 229 to 234 of the penal code [169] establish the framework for the treatment of crimes against the assets of information and communication systems.[170] With regard to data protection and privacy, there is constitutional protection.[171] The constitution stipulates that citizens have the right to the protection of their personal data. There are laws and regulations related to the protection of personal data, but there is no specific law on the subject. However, there is currently a bill on the Protection of the Privacy of Personal Data,[172] which so far has not become law.[173] In addition, the National System of Public Data Registration (SINARDAP) is creating working groups to review the preliminary draft that will be presented to the National Assembly.[174]

Regarding e-government, Ecuador established the 2014–2017 Electronic Government Plan, whose objective is to execute a model of sustainable and inclusive e-government that takes into account political, social, and environmental aspects, with the objective of consolidating a close, open, efficient, and effective government.[175] This plan was updated with the 2018–2021 National Electronic Government Plan, which takes the different aspects of the first one and determines what needs improvement.[176]

Finally, the Law on the National Public Procurement System, amended in 2018, requires information security during the entire procurement process and has created the National Public Procurement Service (SERCOP), the autonomous body responsible for, among other things, establishing the policies and conditions for the use of electronic information and tools, and for modernizing tools related to the electronic public procurement system and electronic auctions.[177]

Indicators: Ecuador

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■□□□□	■■□□□
Organization	■□□□□	■■□□□
Content	■□□□□	■□□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■■□□□	■■■□□
Organization	■■□□□	■■■□□
Coordination	■□□□□	■■□□□
Mode of Operation	□□□□□	■□□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■■□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■□□□□	■□□□□

1-5 Cyberdefense

	2016	2020
Strategy	■□□□□	■■□□□
Organization	■■□□□	■■□□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■□□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■□□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■□□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■■□□□	■■□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■□□□□	■□□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■■□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■■□□
Standards in Procurement	■□□□□	■■□□□
Standards in Software Development	■□□□□	■■□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■■□□
5-3 Software Quality		
Software Quality	□□□□□	■□□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

El Salvador

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
6,388,122	9,478,044	2,160,509	34%

Although El Salvador does not currently have a national cybersecurity strategy, one of the objectives of the 2018–2022 E-government Strategy[178] is to have a National Cybersecurity Policy, as a "result of a consultation process involving international experts, academia, government institutions, private sector and civil society organizations."[179] The country has a nationally recognized CSIRT, SalCERT, which must respond to cybersecurity incidents and coordinate with other response teams.

In recent years, the country has exchanged knowledge on topics such as the protection of critical infrastructure and the improvement of cybersecurity, with Israel, Korea, Spain, and Ecuador, among others.[180]

The private sector in El Salvador participates in the provision of cybersecurity services, ranging from analysis to training. With respect to cybersecurity education, there are some study opportunities in some universities, and some private companies offer training courses in cybersecurity.[181] Companies have also learned that there is a gap in this field in higher-education institutions.

Where El Salvador has made significant progress is in legislation regarding cybercrime. In 2016, the Special Law against Computer-Related Crimes was approved with the aim of protecting legal rights against criminal acts committed using ICTs, as well as the prevention of crimes committed against stored, processed, and/or transferred data.[182]

Articles 24–26 of Decree No. 260 of the Special Law against Computer-Related Crimes refer to protection against the use, hiring, and transfer, and the undue disclosure, of personal data. In addition, Decree No. 133[183] of the Electronic Signature Law protects the personal data needed by service providers. However, there is no comprehensive legislation on the subject, so data protection and privacy are not adequately addressed.

In addition to the development of the 2018–2022 E-government Strategy, [184] El Salvador has taken some concrete steps to establish e-government, such as the launch of the draft for the Integrated Administrative Management System, as well as the National Open Data Policy that joined the new Datos.gob.sv, a portal containing more than 20 public information databases.[185] In addition, the E-government Office was created in 2016, which is responsible for coordinating initiatives with public institutions, and a platform has been in operation since early 2017[186] to facilitate the exchange of government information following security guidelines.[187]

Indicators:

El Salvador

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■■□□□	■■□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■□□□□	■□□□□

1-5 Cyberdefense

	2016	2020
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■□□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■□□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■■□□□	■■□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■■□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■□□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■□□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Grenada

Residents

Ref: World Bank*

2017

110,874

Cell Phone Subscriptions

Ref: ITU**

2017

113,177

Persons with Internet Access

2017

65,495

Internet Penetration

Ref: ITU**

2017

59%

In 2014 the National Telecommunications Regulatory Commission of Grenada indicated that it was working with the government to establish a cybersecurity strategy which would also provide for the establishment of a national CSIRT.[188] However, to date there have been no further announcements. In this regard the government has been investing in several ICT-related projects such as “One Tablet One Child” under the Ministry of Education and a centralized database to facilitate greater ease in offering government services to citizens online. On a separate note, there is little evidence of coordination between the government and critical infrastructure asset owners. [189]

Generally, civil society and the private sector have limited knowledge and awareness of cybersecurity. With no reporting mechanisms in place, it is very difficult to bring cybercrime to light. Regarding education and training, IT education is a part of Grenada’s ICT Strategy, whose goal is to be “citizen-centric, focusing on the delivery of improved levels of customer service and enhanced citizen satisfaction.” However, there are still very limited opportunities for cybersecurity-specific training locally.

In 2013, Grenada adopted the Electronic Crimes Bill, which aimed to include electronic crimes in the criminal code. The bill defines specific offenses as well as the procedure to investigate them.[190] Although Grenada does not itself have legislation for data and privacy protection, it is a part of the Organization of Eastern Caribbean States, which has a Data Protection Act that is applicable to how data is processed in the member states.[191]

Grenada has an e-government strategy as a part of the 2006–2010 ICT Strategy.[192] Additionally, Grenada is part of the 2014 CARICOM E-government Strategy, which aims to provide sustainable improvements to public service delivery through the use of ICTs.[193] However, there is little evidence to suggest that much progress has been made in the electronic provision of public services.[194]

Indicators: Grenada

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■□□□□	■□□□□

1-5 Cyberdefense

	2016	2020
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■□□□□	■□□□□
Private Sector	■□□□□	■□□□□
Users	■□□□□	■□□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■□□□□	■□□□□
User Trust in E-government Services	■□□□□	■□□□□
User Trust in E-commerce Services	■□□□□	■□□□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■□□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■□□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■□□□□	■□□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■■□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■□□□□	■□□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■□□□□	■■□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■□□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■□□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■□□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Guatemala

Residents

Ref: World Bank*

2017

16,087,418

Cell Phone Subscriptions

Ref: ITU**

2017

19,986,482

Persons with Internet Access

2017

10,456,822

Internet Penetration

Ref: ITU**

2017

65%

Along with the Dominican Republic, Guatemala is the most recent in the region to join the group of countries with national cybersecurity strategies. In June 2018, the government launched its national cybersecurity strategy with the aim of strengthening the nation's capabilities, creating the environment and conditions necessary to guarantee the participation, development, and exercise of human rights in cyberspace.[195] In addition, Guatemala's CSIRT-gt is an incident response team under the supervision of the Ministry of the Interior[196] and is a member of the CSIRT Americas network.

Although Guatemala does not yet have a formal definition of critical infrastructure, one of the steps established in the legislative axis of the security strategy is to create, approve, and implement a Critical Infrastructure Law to identify and analyze the main characteristics of the sectors that provide essential services and establish prevention, protection, and recovery measures against threats.

Guatemala has several cybersecurity service providers as well as a CERT for the private sector.[197] In addition, some companies have been looking to raise awareness about cybersecurity.[198] Equally, the Guatemala Chapter of the Internet Society has a working group that, among other things, aims to raise awareness about cybersecurity and offer workshops on how to manage incidents.[199]

While there are not many opportunities to continue tertiary education in cybersecurity, some further education options are available. In addition, the national cybersecurity strategy has an educational axis with the purpose of increasing the offer of education and training in cybersecurity in Guatemala to meet the technical and professional demand in all sectors. There have also been several training events provided by the government, in collaboration with other entities, such as the workshop on cyberthreats,[200] or training for the first CSIRT in collaboration with the OAS.[201]

Guatemala is in the process of developing specific legislation for cyber crime. However, Legislative Initiative No. 5254 of 2017 "provides for the approval of a law against cybercrime."[202] The bill "aims to order prevention and punishment measures of cyberrelated illegal acts, committed using technological devices, data messages, computer systems or data, as well as measures to protect against exploitation, pornography and other forms of sexual abuse with minors and that are carried out through computer systems."[203] Similarly, there is a legislative initiative for data protection and privacy, which will apply to public and private-sector databases.[204]

Guatemala still does not have an e-government strategy. However, e-government is one of the action axes of the Presidential Commission of Open Public Management and Transparency, the mission of which is to support the actions of the ministries and executive power institutions to continue application of the measures originating in international conventions on transparency, e-government, the fight against corruption, and open government.[205]

The Law to Combat Cybercrime with the support of the OAS and the Council of Europe which was presented in March 2017. In April 2020, Guatemala was invited to accede to the Budapest convention.

Indicators: Guatemala

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■■■□□
Organization	■□□□□	■■□□□
Content	■□□□□	■■■□□
1-2 Incident Response		
Identification of Incidents	■■□□□	■■□□□
Organization	■□□□□	■■□□□
Coordination	■□□□□	■■□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■□□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■■□□□	■■□□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■□□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■□□□□	■■□□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■□□□	■■□□□
Prosecution	■□□□□	■■□□□
Courts	■■□□□	■■□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■□□□□	■■□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■■□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■■□□□	■■□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■■□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■□□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■■□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Guyana

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
775,221	643,210	289,358	37%

In March 2019, a National Cybersecurity Strategy Working Group was established to develop a national strategy under the guidance of the OAS. As part of this initiative and in partnership with the OAS, a national stakeholders' consultation was held in July 2019. A preliminary draft strategy is currently under review. The country established its national CSIRT, CIRT.GY, in 2013[206] with the mission to "improve national cybersecurity preparedness and response through proactive security measures and information sharing mechanisms." Services are offered to public and private sectors as well as members of civil society affiliated with Guyana. CIRT.GY falls under the framework of the Ministry of Public Telecommunications.[207] Additionally, CIRT.GY is a member of CSIRT Americas, taking advantage of the collaborative nature of that network, and has also partnered with other CERTs in Estonia, Colombia, and the Netherlands.

There are not many private-sector cybersecurity service providers available yet, and the focus of cybersecurity for executives is in the reactive phase. However, cybersecurity is beginning to be discussed more frequently at management levels. Civil-society institutions, on the other hand, are still mostly unaware of the importance of good cybersecurity practices.[208]

Some opportunities for training in cybersecurity are available in Guyana. There are some bachelor degree offerings in computer science and IT. While a program dedicated to cybersecurity does not exist, a post-graduate certificate course in Network Security is now offered at the recently launched Center for Excellence in Information Technology, the result of a bilateral agreement between the Government of India and the Government of Guyana. This program initially targeted the public sector, but plans are in place to widen the audience to include the private sector.

The government has taken several steps to raise awareness on cybersecurity. In April 2019, Guyana benefited from a one-year public awareness and sensitization campaign devised by the United Kingdom's Cyber Security Programme. Key to this was the launch of the website www.getsafeonline.gy.[209] Additionally, in September 2019, the Ministry of Public Telecommunications collaborated with Get Safe Online to host a cybersecurity awareness training workshop. Participants included 124 public servants across 50 agencies. Further, in October 2019, in celebration of cybersecurity awareness month, a national public awareness campaign was implemented which included radio talks, social media announcements, and awareness sessions at secondary and tertiary educational institutions as well as the public sector.

With respect to cybercrime, in 2017 the Guyana Police Force, in collaboration with the private sector, opened a cybersecurity center with the goal of teaching police, the business community, and the public how to respond to cybercrime.[210] In January 2019, the Guyana Police Force formally established a cybercrime unit to investigate and prosecute crimes committed using computer technology. Cybercrime legislation was enacted in 2018 after being discussed for two years.[211,212] The legislation encompasses a number of cybercrime offenses and methods of enforcement.[213] Guyana has not yet passed legislation on privacy and data protection.[214]

Guyana's e-government strategy is anchored in the Green State Development Strategy: Vision 2040. This is Guyana's 20-year national development policy that reflects the guiding vision and principles of their green agenda. The central objective is development that provides a better quality of life for all Guyanese derived from the country's natural wealth—its diversity of people and abundant natural resources (land, water, forests, mineral and aggregates, biodiversity). The appropriate utilization of ICT can improve the lives of all Guyanese and is therefore a cross-cutting component of the Green State Development Strategy: Vision 2040. ICT has the potential to make government services more widespread, effective, and responsive, as well as be a driver of new green business activity.[215]

Indicators: Guyana

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Coordination	■■□□□	■■■□□
Mode of Operation	□□□□□	■■□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■□□□□	■■□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■□□□□	■□□□□

1-5 Cyberdefense

	2016	2020
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■■□□□	■■□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■■□□□	■■■□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■■□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■□□□□	■■□□□
User Trust in E-government Services	■□□□□	■■■□□
User Trust in E-commerce Services	■■□□□	■■□□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■■■□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■■■□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■□□□□	■■■□□
Executive Awareness Raising	■□□□□	■■□□□
3-2 Framework for Education		
Provision	■□□□□	■■□□□
Administration	■□□□□	■■□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■□□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■□□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■□□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■□□□□	■□□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■□□□□	■■□□□
Courts	■□□□□	■□□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■■□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■□□□□	■■□□□
Standards in Procurement	■□□□□	■■□□□
Standards in Software Development	■□□□□	■■□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■■□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■■□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Haiti

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
10,982,366	6,305,862	1,353,698	12%

Haiti does not have a national cybersecurity strategy nor a national CSIRT. However, the government is aware that cybersecurity is of increasing importance and has taken some steps accordingly. A working group for cybersecurity and cybercrime (GTCSC) was created in 2015 by the Ministry of Public Works, Transport, and Communication with the mission of developing and implementing a national cybersecurity strategy. In 2016, this group led a workshop on draft legislation for cybersecurity, cybercrime, communication interceptions, and electronic transactions and evidence with participants from the banking sector, cell phone operators, internet service providers, the national police, the Ministry of Public Security and other state institutions, various entities of the State University of Haiti, and the presidents of permanent commissions for telecommunication, information, and communication of both chambers of parliament.[216] Moreover, in May of 2018, a delegation from the Latin America and Caribbean Network Information Center met with the general director of the National Telecommunications Council (CONATEL) to discuss, among other things, collaboration for the establishment of a national CSIRT.[217]

There is concern from the private sector that both public and private-sector institutions are unaware of the risks to their systems, and should periodically do a "technological audit" to see where there are vulnerabilities.[218] As Haitians increase their use of networks for personal or professional matters, the cyber risk increases. This leads to a need for policies and legislation to regulate cyberspace, which the country does not yet have.[219] Overall, the private sector seems to have a general awareness of the importance of cybersecurity. Furthermore, there are parties involved in the hosting of events for raising awareness and conducting workshops and trainings on cybersecurity, like the Haiti Cybercon.[220]

There are some courses offered in cybersecurity although there are no specific degrees in cybersecurity. However, Haiti has sent some participants to trainings organized by the OAS in 2017 and 2018, such as the Summer Bootcamp organized by the OAS and INCIBE or to the Subregional Workshop on Protection of Critical Infrastructure in Panama.[221]

At present, Haiti does not yet have legislation on cybercrime, nor legislation for data protection and privacy.[222] However, cybercrime legislation is in the process of being developed as shown by the 2016 workshop for the presentation of draft legislation on the topic. Regarding data and privacy protection, there is little evidence to show that it is being developed.

Although Haiti does not have a dedicated e-government strategy, part of its Strategic Development Plan 2030 is the digital modernization of the public administration.[223] Haiti has an integrated government platform;[224] however, it does not yet offer e-government services to its citizens.[225]

Indicators: Haiti

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■■□□□	■■□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■□□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■□□□□	■□□□□
User Trust in E-government Services	■□□□□	■□□□□
User Trust in E-commerce Services	■□□□□	■□□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■□□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■□□□□	■□□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■□□□□	■□□□□
Data Protection Legislation	□□□□□	■□□□□
Child Protection Online	□□□□□	■□□□□
Consumer Protection Legislation	□□□□□	■□□□□
Intellectual Property Legislation	□□□□□	■□□□□
Substantive Cybercrime Legislation	■□□□□	■□□□□
Procedural Cybercrime Legislation	■□□□□	■□□□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■□□□□	■□□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■■□□□	■■□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■□□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■□□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■□□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Honduras

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
9,429,013	8,233,499	2,988,997	32%

Honduras has developed the National Cybersecurity Law and Measures for Protection against Hate and Discrimination Acts on the Internet and Social Networks bill, which identifies the need to create a national cybersecurity strategy as well as an interinstitutional cybersecurity committee that is in charge of strategy development and implementation.[226] In addition, Honduras reached an agreement with Israel in 2016 for cooperation focused on "strengthening the capabilities of prevention, defense and reaction to possible cyberattacks to government institutions, infrastructure managers and critical services."[227] On the other hand, through the "Digital Transformation for Increased Competitiveness" program, the IDB and the Government of Honduras are working together to modernize the country's cybersecurity network.[228]

Honduras does not yet have a national CSIRT, but there are private entities providing incident response services. Although there is much to be done in terms of cybersecurity service providers, the main private-sector firms have begun to prioritize cybersecurity and take action in this regard.[229]

The Honduran government has taken several steps to strengthen training opportunities in cybersecurity for its public servants and the armed forces. To begin with, the Honduran Armed Forces signed an agreement with Mexico that is "the framework for improving the areas of cooperation in naval and military education, training and education, national security and defense, cybersecurity and cyberdefense."[230] In addition, CONATEL, the National Telecommunications Commission, organized a two-day workshop on cybersecurity as part of a national strategy,[231] and although limited, there is an offer of free virtual introductory cybersecurity courses and cybersecurity courses.

With respect to legislation, Honduras has made progress. Congress is reviewing the Cybersecurity Act, connected to the National Cybersecurity Law and Measures for Protection against Hate and Discrimination Acts on the Internet and Social Networks. To protect data and privacy, the bill on the protection of personal information was approved in National Congress after the third and last debate in April 2018.[232] This new law applies to public and private-sector databases.[233]

As it relates to advancement in technology, e-government is one of the four strategic axes of the 2014–2018 Honduras Digital Agenda. The objective is to promote ICTs to create a new model of public administration to improve service provision and information, as well as increasing the efficiency, effectiveness, and transparency of the public sector. The main initiatives are the creation of a government network that includes a government portal, a contact center, an electronic system for public procurement, a business portal, a window for the electronic customs system, a government database, and a national system for digital certification.[234]

Indicators: Honduras

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■■□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■■□□□	■■□□□
Organization	■□□□□	■■□□□
Coordination	■□□□□	■■□□□
Mode of Operation	□□□□□	■■□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■■□□□
Organization	■□□□□	■■□□□
Risk Management and Response	■□□□□	■■□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■□□□□	■□□□□
User Trust in E-government Services	■□□□□	■■□□□
User Trust in E-commerce Services	■□□□□	■□□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■□□□□	■■□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■□□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■□□□□	■□□□□
Data Protection Legislation	□□□□□	■□□□□
Child Protection Online	□□□□□	■□□□□
Consumer Protection Legislation	□□□□□	■□□□□
Intellectual Property Legislation	□□□□□	■□□□□
Substantive Cybercrime Legislation	■■□□□	■■□□□
Procedural Cybercrime Legislation	■□□□□	■□□□□
4-2 Criminal Justice System		
Law Enforcement	■□□□□	■□□□□
Prosecution	■□□□□	■□□□□
Courts	■□□□□	■□□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■□□□□	■■□□□
Standards in Procurement	■□□□□	■■□□□
Standards in Software Development	■□□□□	■□□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■□□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■□□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Jamaica

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
2,920,853	3,091,222	1,608,574	55%

Jamaica released its national cybersecurity strategy in January 2015 with four main objectives, namely establishing technical measures to effectively protect against and respond to cyberattacks; increasing human resources and capacity building in the area of information security; improving the regulatory framework; and increasing the public's education and awareness of cybersecurity.[235] As part of the technical measures and capacity building, Jamaica established a national CSIRT (JaCIRT) under the Ministry of Science, Energy, and Technology (MSET) to monitor Jamaica's cyberspace and coordinate cyber incident responses.[236] JaCIRT is a member of CSIRT Americas, and thus has access to the entire network of member CSIRTs. Additionally, Jamaica allocated specific funds in the 2018–2019 budget for different cybersecurity initiatives at the Ministry of National Security and the Ministry of Science, Energy, and Technology.[237]

Jamaica's national cybersecurity strategy also took the step of defining national critical infrastructure as "systems and assets, whether physical or virtual, so critical that the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof."[238] These can include "water and sewage networks, agriculture, health systems, emergency services, information technology and telecommunications, banking and finance, energy (electrical and wind generated), transportation (air, road, port), postal and shipping entities."[239] Accordingly, the strategy has given the lead role of protecting the national critical infrastructure to MSET, eGov Jamaica, and the operators of critical infrastructure.

The Jamaican government has taken significant steps to improve the country's cybersecurity, but many companies still lack cyber incident response plans.[240] Further, aiming at educating civil society as part of the national cybersecurity strategy, the government has launched a cybersecurity public awareness program in collaboration with the private sector.[241] Indeed, the cybersecurity strategy itself highlights the importance of the private sector in engaging in cybersecurity activities and protecting private and public resources.

For higher education in cybersecurity, there are some private cybersecurity service providers that do trainings, and the government has done several sessions and workshops (some in collaboration with JaCIRT) to provide cybersecurity skills and knowledge to government officials and the private sector.[242]

Jamaica has a strong regulatory framework for cybercrime. The Cybercrimes Act of 2010[243] provides "criminal sanction for the misuse of computer systems or data and the abuse of electronic means of completing transactions and to facilitate the investigation and prosecution of cybercrimes."[244]

This act was amended in 2015 after a comprehensive review involving not only local stakeholders but also international actors.[245] Additionally, the Data Protection Act aimed at protecting "the privacy of certain data and connected matters" is currently being discussed in parliament. The Data Protection Act will apply to both private and public data controllers, thus providing a comprehensive legislation on data and privacy protection.[246]

Jamaica has also developed the ICT Sector Plan 2009–2030[247] and an ICT Policy approved in 2011.[248] The National Identification and Registration Act, which passed in 2017, is being executed with IDB's support[249] and is "designed to house your biographic, biometric and demographic information in highly secure, standalone environments."[250]

Indicators: Jamaica

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■■□□	■■■□□
Organization	■■□□□	■■□□□
Content	■■□□□	■■■□□
1-2 Incident Response		
Identification of Incidents	■■□□□	■■□□□
Organization	■□□□□	■■□□□
Coordination	■□□□□	■■□□□
Mode of Operation	□□□□□	■■□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■■□□□	■■□□□
Executive Awareness Raising	■■■□□	■■■□□

3-2 Framework for Education

	2016	2020
Provision	■■□□□	■■□□□
Administration	■□□□□	■■□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■■■□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■■□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■■□□	■■■□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■■□□	■■■□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■■□□□
Standards in Software Development	■□□□□	■■□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■■□□□	■■□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■■□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■□□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■■□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Mexico

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
124,777,324	114,329,353	79,673,128	64%

Mexico introduced its national cybersecurity strategy in 2017 with the main objective of identifying and establishing the cybersecurity actions applicable to social, economic, and political areas, to enable citizens and private and public organizations to use ICTs responsibly for the sustainable development of the Mexican state.[251] The critical information infrastructure is defined in the national cybersecurity strategy as the information infrastructure that is considered strategic because it is linked to the provision of essential public services and its deterioration could compromise national security. Mexico established a national CSIRT, CERT-MX, years ago, to prevent and mitigate cyberthreats.[252] CERT-MX is under the Federal Police and is part of the CSIRT Americas network.

With cybercrime being a growing concern, Mexican organizations driving digital transformation projects have identified that decision-maker interest groups (C-Suite executives) have included security and privacy staff in 96 percent of the cases (91 percent globally), and 44 percent (53 percent globally) has included the proactive management of cyber risks and privacy, by design, in their project planning and budgeting as a key consideration.[253]

There are plenty of opportunities for Mexicans to continue their education in cybersecurity with options for both graduate and undergraduate students. Also, several cybersecurity events have been promoted by the government, such as the Forum on Cybersecurity with an emphasis on the financial sector[254] or the basic cybersecurity course for public servants offered by the Federal Police. [255]

Mexico does not have a dedicated law on cybercrime, but Article 211 of the criminal code involves cybercrime.[256] However, these provisions are limited and present gaps, which makes it difficult to combat cybercrime. In terms of data protection and privacy, there are two separate laws: one for public databases and the other for private databases.[257]

Mexico introduced a national digital strategy, part of the 2013–2018 National Development Plan, with a first objective focused on "increasing the digitalization of Mexico,"[258] based on the promotion of "the deployment and expansion of telecommunications infrastructure, as well as the adoption and the use of ICTs by the population to take advantage of its benefits."[259] This transformation seeks to build a new relationship between society and government, centered on the experience of the citizen as a user of public services by adoption of ICTs in government. Currently, Mexico offers its citizens the gob.mx portal, which provides identification, health, and visa services, among others.[260]

Indicators: Mexico

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■□□□	■■■□□
Organization	■■□□□	■■□□□
Content	■■□□□	■■■□□
1-2 Incident Response		
Identification of Incidents	■■■■□	■■■■□
Organization	■■■□□	■■■□□
Coordination	■■□□□	■■■□□
Mode of Operation	□□□□□	■■■□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■□□□
Organization	■□□□□	■■□□□
Risk Management and Response	■■□□□	■■□□□
1-4 Crisis Management		
Crisis Management	■■□□□	■■□□□
1-5 Cyberdefense		
Strategy	■■□□□	■■■□□
Organization	■■□□□	■■□□□
Coordination	■■□□□	■■□□□
1-6 Communications Redundancy		
Communications Redundancy	■■□□□	■■■□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■■□□
Private Sector	■■□□□	■■■□□
Users	■□□□□	■■■□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■■□□
User Trust in E-government Services	■■■□□	■■■□□
User Trust in E-commerce Services	■■■□□	■■■□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■■□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■■□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■■□□
Executive Awareness Raising	■■□□□	■■■□□
3-2 Framework for Education		
Provision	■■■□□	■■■□□
Administration	■■□□□	■■■□□
3-3 Framework for Professional Training		
Provision	■■■□□	■■■□□
Uptake	■■□□□	■■■□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■□□	■■■□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■■□□
Consumer Protection Legislation	□□□□□	■■■□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■□□□	■■■□□
4-2 Criminal Justice System		
Law Enforcement	■■■■□	■■■■□
Prosecution	■■□□□	■■■□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■■□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■■□□□	■■□□□
Standards in Software Development	■■■□□	■■■□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■■□□	■■■□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■■□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■■□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■■□□□	■■■□□
Cybercrime Insurance	■■□□□	■■□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Nicaragua

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
6,384,855	8,179,876	1,779,015	28%

Nicaragua is in the process of formulating a national cybersecurity strategy, which will contain within its axes, among others, the creation of a cybersecurity incident response center and updating of the legal, administrative, criminal, and procedural frameworks to allow for the prevention, investigation, judgment, and punishment of cybercrime.

Currently, the Cybercrime Unit of the National Police attends cybersecurity incidents together with the Specialized Unit against Organized Crime of the Public Ministry and other institutions specialized in the field. With regard to cybersecurity legislation, Nicaragua has the following legal framework:

1) Political Constitution of the Republic: protects the national communication systems and the administration and management of the radio and satellite spectrum.

2) Law No. 983 (Constitutional Justice Law): regulates the appeal of Habeas Data.

3) Law No. 919 (Sovereign Security Law): identifies threats to sovereign security, including external attacks on cybersecurity.

4) Law No. 787 (Law on Protection of Personal Data):[261] protects the automated processing of personal data of Nicaraguan society, in order to guarantee informational self-determination.

5) Law No. 641 (Criminal Code):[262] typifies some behaviors of cybercrimes.

Public institutions have strengthened their cybersecurity-oriented capabilities through specialized equipment and training. The private sector has expanded its offer of cybersecurity services, which include public and private cloud-protection services.

Regarding access to information technologies, after the implementation of the Axis of the National Human Development Program 2018–2021, which includes the promotion of science, technology, and innovation, the execution of the National Broadband Program continued with the support of the IDB. Through this program, access to telecommunications services was facilitated to remote municipalities of the country, strengthening the connectivity of the national health and agricultural system.

The expansion of access to information technologies has allowed the extension of careers and technical courses through remote methods, making use of virtual education. Online services and public procedures have also been implemented.

According to statistics from the Nicaraguan Institute of Telecommunications and Postal Services (TELCOR), in 2017 a total of 8,179,876 mobile phone subscribers were registered, with a fixed broadband coverage of 92 percent, mobile broadband of 98 percent, and 3G mobile coverage in 100 percent of the national territory.

Indicators:

Nicaragua

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■■□□□
Private Sector	■□□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■□□□□	■□□□□
User Trust in E-government Services	■□□□□	■□□□□
User Trust in E-commerce Services	■□□□□	■□□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■□□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■□□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■□□□□	■■□□□
Uptake	■□□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■□□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■□□□□	■■□□□
Procedural Cybercrime Legislation	■■■□□	■■■□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■□□□□	■■□□□
Prosecution	■□□□□	■□□□□
Courts	■□□□□	■□□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■■□□□	■■□□□
Standards in Software Development	■□□□□	■■□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■□□□□	■■□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■■□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■□□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■■□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Panama

Residents

Ref: World Bank*

2017

4,106,771

Cell Phone Subscriptions

Ref: ITU**

2017

5,280,195

Persons with Internet Access

2017

2,376,387

Internet Penetration

Ref: ITU**

2017

58%

Panama began to implement its cybersecurity strategy in March 2013 with the issuance of Resolution No. 21,[263] the National Cybersecurity Strategy and Protection of Critical Infrastructure, with the slogan "Panama, Reliable in Cyberspace: Everyone's Job."[264] The pillars of the cybersecurity strategy are protection of privacy; prevention and detention of crimes in cyberspace; strengthening of critical infrastructure; promotion of private-sector development; expansion of the culture of cybersecurity, of training, innovation, and adoption of standards; and improving the capacity of public agencies to respond to incidents.

One of the aspects of cybersecurity that stands out in the strategy is the protection of critical infrastructure, which are "vital for the welfare of the population, basic services, the operation of government and private organizations, economic well-being and people's quality of life,"[265] and which require "comprehensive protection."

CSIRT Panamá was established as the national computer incident response team in 2011 per Executive Decree 709 within the framework of the National Authority for Government Innovation.[266] In addition to preventing, treating, identifying, and solving cybersecurity incidents, CSIRT Panamá also has the task of increasing the country's general knowledge about cybersecurity.[267] To strengthen these capacities, the Government of Panamá and the IDB agreed to support specific cybersecurity initiatives through the loan operation Panama Online Program, approved in 2016.[268] In addition, CSIRT Panamá is a member of CSIRT Americas and, therefore, can benefit from all that the network has to offer.

There are private-sector providers in Panama offering a variety of cybersecurity services, from database security to a range of training courses. In addition, there is a great opportunity for Panamanian citizens to continue their education in cybersecurity and information technologies, including masters' programs. To encourage the study of cybersecurity, the National Authority for Governmental Innovation, in collaboration with Citi and the OAS, has offered scholarships in the past for cybersecurity training in order to reduce the shortage of cybersecurity professionals in the region.[269] In addition, CSIRT Panamá offers ongoing training in cybersecurity for professionals in the technology departments of government institutions.[270]

Regarding legislation, Panama's criminal code has some provisions that deal with cybercrime.[271] In addition, Bill No. 558 of 2017[272] seeks to modify the criminal code to "comply with international cybersecurity standards," including the Budapest Convention on Cybercrime, approved by Panama in 2013.[273]

There is a bill for the protection of personal data, which will apply to both the public and private sectors once it is approved.[274] Lastly, Panama has an e-government strategy and other important guidelines related to cybersecurity and ICT governance in its 2015–2019 Strategic Government Plan and in the 2014–2019 Digital Agenda.[275]

Indicators: Panama

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■■□□	■■■□□
Organization	■■□□□	■■■□□
Content	■■□□□	■■□□□
1-2 Incident Response		
Identification of Incidents	■■■□□	■■■□□
Organization	■■□□□	■■■□□
Coordination	■■□□□	■■□□□
Mode of Operation	□□□□□	■■■□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■■□□□
Organization	■□□□□	■■□□□
Risk Management and Response	■□□□□	■■□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■■□□□
1-5 Cyberdefense		
Strategy	■□□□□	■■□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■■□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■□□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■■□□□	■■■□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■■□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■■□□□
Standards in Software Development	■□□□□	■■□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■■□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Paraguay

Residents

Ref: World Bank*

2017

6,867,062

Cell Phone Subscriptions

Ref: ITU**

2017

7,468,275

Persons with Internet Access

2017

4,194,110

Internet Penetration

Ref: ITU**

2017

61%

In April 2017, Paraguay approved its National Cybersecurity Plan and integrated its National Cybersecurity Commission with representatives of different public institutions, with the aim of adopting cybersecurity measures to guarantee and promote the safe and reliable use of ICT, as well as progress and innovation in the country.[276] In addition, the plan clearly defines seven lines of action (awareness and culture; research, development, and innovation; protection of critical infrastructure; ability to respond to cyberincidents; ability to investigate and prosecute cybercrime; public administration; and national cybersecurity system), all with very clear next steps. The plan was developed as a supplement to establish initiatives in the field of cybersecurity. Paraguay's national CSIRT (CERT-PY) is a member of the CSIRT Americas network.[277]

With the objective of increasing Paraguay's capabilities, the IDB approved in 2018 the Digital Agenda Support Program loan operation that includes specific actions and components to ensure the strengthening of the national cybersecurity framework.[278]

The National Cybersecurity Plan also defines critical infrastructure as "systems and assets, physical or virtual, essential for the maintenance of vital social functions, health, physical integrity, security, and the social and economic welfare of the population, and the disruption or destruction of which would have a debilitating impact on national security, generating a cascade of negative effects that would seriously affect the country."[279] This has shown the need for cooperation between the public and private sectors in the protection of the critical infrastructure of the country.

While there are some providers in the private sector of cybersecurity services, the cybersecurity strategy seeks to increase awareness of the importance of having good cybersecurity practice in the private sector. In 2017, there were still no private-sector companies with ISO 27001 certification, an international standard for information security. It was adopted as the Paraguayan standard in November 2014 by the National Institute of Technology and Standardization, through a committee composed of representatives of public institutions, private companies, consumer associations, and universities.[280] However, the private sector participated in the development of the National Cybersecurity Plan, and the establishment of the Paraguayan standard ISO 27001, which indicates willingness to participate more and create awareness of the importance of cybersecurity.

In October 2018, the Ministry of Information Technologies and Communications (MITIC) was created, within which Cybersecurity and Information Protection was established as a strategic axis. The MITIC, through the General Directorate of Cybersecurity and Information Protection, today has the following roles and powers, established in the Law of Creation of MITIC 6207/2018:

- Construction of a secure, reliable, and resilient digital ecosystem, including the public, private, academia, and citizenship sectors

- Policies for the protection of personal and governmental information

- Protection of systems, networks, processes, and information of state agencies and entities

- Cybersecurity plans and strategies at the national level

- Authority in cybersecurity, prevention, management, and control of cyberincidents

- Definition and protection of the critical technological infrastructure

MITIC offers several online IT courses for free to anyone with a computer and internet access, including some on information security. In addition, several training programs are offered by universities and security companies, and there are limited degree opportunities in cybersecurity. The government has also carried out training campaigns aimed at educating the population about cybersecurity.[281]

Likewise, the General Directorate of Cybersecurity and Information Protection has several initiatives and offers various services, including alerts and security bulletins, cyberincident management, audits of government system vulnerabilities, security diagnoses to government institutions, and activities of awareness and training for citizens, companies, government, academia, and other sectors.

In 2011, through Law 4439/11, Paraguay modified and expanded the catalog of punishable acts existing in Law 1160/97 (the Criminal Code), which refers to certain articles that describe illegal conduct carried out through the use of technology whose essence lies in its computing nature, better known as cybercrimes.[282]

Paraguay also has within its national legislation Law No. 1682, which concerns information of a private nature and whose objective is to regulate the "collection, storage, processing and publication of personal data or characteristics."[283]

In 2017, by Law No. 5994/17, Paraguay adheres to the Budapest Convention on Cybercrime and its Additional Protocol, whose main objective is "to pursue a common criminal policy aimed at protecting society against cybercrime, especially through the adoption of adequate legislation and the promotion of international cooperation."[284] Currently, as a state party to this convention, Paraguay is a beneficiary of the GLACY+ Program (Global Action on Cybercrime Extended), carried out by the Council of Europe together with the European Union, in order to support member countries to achieve the effective implementation and harmonization of the convention to positive national legislation, through the promotion of legislative strategies against cybercrime, and capacity building for judicial officers and international legal cooperation. In December 2019, the country received the Council of Europe Committee, composed of expert consultants in the area of cybercrime, to carry out an initial mission in order to assess the state of the country in the fight against cybercrime, with the aim of setting the guidelines to be followed through a work plan with the various actors involved in the area of cybercrime.

The Public Prosecutor's Office has a Specialized Unit in Cybercrimes composed of a Deputy Prosecutor, a Delegated Prosecutor, and three criminal units in the capital, as well as specialized cybercrime agents in the main departments, to intervene in allegations of punishable acts of an electronic nature. At the same time, it has a technical support office for fiscal management, which is responsible for providing technical assistance and support with the purpose of conducting research proceedings that involve the use of computer or electronic technology. For its part, the National Police also has a specialized division to fight cybercrime, which works jointly with the Public Ministry.

The Ministry of Defense through the Institute of High Strategic Studies is undergoing a process of innovation and adaptation that requires specialized professionals, and implemented in 2019 the Program of Specialization in Cyberdefense and Strategic Cybersecurity as a way to train people to create strategies to combat the new threats that take place in cyberspace, a sign that modernity has reached the institution, which will have its first cohort of graduates.

The country also has a draft of the National ICT/Digital Agenda Strategy, which "is framed within the objectives of the 2030 Paraguay National Development Plan."[285] The axes of the Digital Agenda are (i) e-government; (ii) inclusion, appropriation, and use; and (iii) innovation and competitiveness. Law No. 4989/13 is another important instrument in the preparation of ICT policies.[286] Likewise, various cybersecurity standards and guidelines were adopted for the government sector, including the following:

- Critical Cybersecurity Controls, based on the CIS Controls, approved by SENATIC Resolution 115/2018.[287]

- Minimum Security Criteria for the Development and Acquisition of Software, approved by MITIC Resolution N° 699/2019.[288]

- Cybersecurity Directives for Official State Communication Channels, approved by MITIC Resolution 432/2019.[289]

Indicators: Paraguay

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■□□□	■■■□□
Organization	■■□□□	■■□□□
Content	■□□□□	■■■□□
1-2 Incident Response		
Identification of Incidents	■■■□□	■■■□□
Organization	■■■□□	■■■□□
Coordination	■■□□□	■■■□□
Mode of Operation	□□□□□	■■□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■■□□□
1-5 Cyberdefense		
Strategy	■□□□□	■■□□□
Organization	■□□□□	■■■□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■■□□□	■□□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■■□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■□□□
Executive Awareness Raising	■■□□□	■■■□□
3-2 Framework for Education		
Provision	■□□□□	■■□□□
Administration	■□□□□	■■□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■□□	■■■□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■■□□
Consumer Protection Legislation	□□□□□	■■■□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■■□□
Prosecution	■■■□□	■■■□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■■□□
Informal Cooperation	□□□□□	■■■□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■■□□□
Standards in Software Development	■■□□□	■■■□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■□□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■■□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■■□□□
Cybercrime Insurance	■□□□□	■■□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■■□□□

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB
Improving lives

OAS
More rights for more people

Peru

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
31,444,297	38,915,386	15,322,061	49%

Peru does not yet have a national cybersecurity strategy, but it does have a National Cybersecurity Policy that, among other things, highlights the need to create a national cybersecurity strategy and a national cybersecurity committee.[290]

Law No. 30618 of 2017 defines cybersecurity as the "situation of trust in the digital environment, in the face of threats that affect national capacities, through risk management and the application of cybersecurity measures and cyberdefense capabilities, aligned with the achievement of state objectives."[291] The law also establishes that the National Directorate of Intelligence is responsible for "carrying out activities and establishing procedures aimed at achieving cybersecurity in the area of its competence." [292]

Supreme Decree No. 106-2017-PCM "approves the Regulation for the Identification, Evaluation and Risk Management of National Critical Assets," which are "resources, infrastructure and systems that are essential and indispensable to maintain and develop national capacities or that are intended to fulfill that end." [293]

Peru has a national CSIRT, PeCERT, with the aim of coordinating 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.[294] PeCERT is under the National Office of E-government and Information Technology (ONGEI) and is a member of the CSIRT Americas network. In addition, according to the Center for Industrial Cybersecurity, Peru is developing a law for the protection of critical infrastructure.[295] The Government of Peru and the IDB, through the loan operation Project to Improve and Expand Support Services for National Service Delivery to Citizens and Enterprises, agreed to promote specific projects to strengthen the national cybersecurity posture.[296]

There are several private cybersecurity service providers in Peru, some of which also offer training in cybersecurity. Some opportunities are available in universities for Peruvians to continue their education in cybersecurity and there have also been events related to cybersecurity organized by independent associations. The Peruvian government also took the initiative in organizing cybersecurity events such as the International Conference on Challenges and Management in Digital Security in June 2018, organized by the National Intelligence Directorate and the E-government Secretariat.[297]

The issue of e-government is important for Peru, which has the E-government Law that "aims to establish the governance framework of e-government for the proper management of digital identity, digital services, digital architecture, interoperability, cybersecurity and data, as well as the legal regime applicable to the cross-cutting use of digital technologies in process digitalization and provision of digital services by Public Administration entities in the three levels of government."[298] In addition, Peru declared "national interest strategies, actions, activities and initiatives for the development of e-government, innovation and digital economy in Peru with territorial focus"[299] in 2018,[300] and also approved the "guidelines for the formulation of the E-government Plan."[301]

Regarding legislation, Law No. 30096 delivers substantive provisions on computer crime[302] and Law No. 27309 incorporates computer crime into the country's criminal code.[303] In addition, Law No. 29733 applies to protection of both public and private databases.[304]

Indicators: Peru

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Content	■□□□□	■□□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■■■□□	■■■□□
Organization	■■□□□	■■□□□
Coordination	■■□□□	■■□□□
Mode of Operation	□□□□□	■□□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Risk Management and Response	■□□□□	■□□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■□□□□	■■□□□

1-5 Cyberdefense

	2016	2020
Strategy	■■□□□	■■□□□
Organization	■□□□□	■■□□□
Coordination	■■□□□	■■□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■□□□□	■■□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■■□□□	■■□□□
Private Sector	■■■□□	■■■□□
Users	■□□□□	■■□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■■□□□	■■□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■■□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■■□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■■□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■□□□	■■□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■■□□□	■■□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■□□	■■■□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■■□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■■□□□	■■□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■■□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Saint Kitts and Nevis

Residents

Ref: World Bank*

2017

52,045

Cell Phone Subscriptions

Ref: ITU**

2017

76,878

Persons with Internet Access

2017

42,006

Internet Penetration

Ref: ITU**

2017

81%

Saint Kitts and Nevis has not yet developed a national cybersecurity strategy or established a national CSIRT. However, the government is aware of the increasing importance of cybersecurity for a country's overall national security and is working towards establishing a national CSIRT. Further, developing a national cybersecurity strategy and implementation plan, establishing a national cybersecurity committee, conducting interviews with stakeholders, and reviewing surveys assessing current needs are also steps Saint Kitts and Nevis is working towards.

In a 2017 meeting of the Council of Ministers of the Regional Security System, chaired by the prime minister of Saint Kitts and Nevis, cybersecurity was one of the main points on the agenda.[305] Furthermore, at the reopening of the ICT Center, public statements by the prime minister made clear that cybersecurity should be a priority for the country.[306] Lastly, the 2018 budget mentions the now-renovated ICT Center, an e-government network infrastructure project, and a cybersecurity project.[307]

There are some private-sector cybersecurity service providers in Saint Kitts and Nevis, however limited, with some providing technical services and others providing awareness and training services. Nevertheless, the private sector is beginning to make cybersecurity a priority and taking steps accordingly. At the national level, the government has facilitated some cybersecurity training programs for civil servants, such as ISO 31000 risk training for civil servants.[308] However, there are no opportunities to pursue higher education courses on cybersecurity yet.

Saint Kitts and Nevis has already had legislation for cybercrime as the Electronic Crimes Act of 2009, which contains both offenses related to electronic crimes as well as the procedure to prosecute them.[309] The new Data Protection Bill was enacted in 2018 and is very similar to that of the Organization of Eastern Caribbean States and applies to information held by both the private and the public sector.[310]

E-government is a part of the 2006 National Information and Communications Technology (ICT) Strategic Plan and aims to take advantage of ICT for the purpose of information and service delivery by the government.[311] In 2016, through a public-private partnership, a new government e-portal was launched, with the claim that it would increase efficiency in transactions with the government. Additionally, the portal would also connect different government ministries and agencies to facilitate the sharing of information.[312] It is expected that a National Digital Strategy will be formulated, and that there will be an increase in the deployment of interconnected information systems. Further, a new government enterprise architecture is expected to be implemented, with a security, interoperability, and service-oriented design.[313]

Indicators:

Saint Kitts and Nevis

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■□□□□	■□□□□
User Trust in E-government Services	■■□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■□□□□	■□□□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■□□□	■■□□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■□□□	■■□□□
Prosecution	■□□□□	■□□□□
Courts	■■□□□	■■□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■■□□□	■■□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■■□□□	■■□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■■□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■□□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■■□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Saint Lucia

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
180,955	176,694	91,953	51%

The Government of Saint Lucia, through the Department of Public Service, is taking steps to build resilience to cyberattacks, hence creating a more secure environment for its operations and data exchange. The Government Data Centre managed by the Government Information Technology Services (GITS) acquired ISO 27001:2013 certification in 2015.[314] Although it was due to be renewed in April 2018, due to constraints it was not renewed. Currently the Division of Public Sector Modernization (DPSM) within the Department of Public Service has engaged the services of a consultant to support GITS in preparation for recertification of their data center as ISO 27001:2013.

The Department of Public Service through the Division of Public Sector Modernization has embarked on an exercise to refresh the National ICT Policy and Sectoral Strategy. This strategy will seek to plot the way forward for the implementation of ICT across all sectors to modernize them, create new business opportunities, and foster innovation. A weeklong consultation was held with a cross section of government, private-sector, and civil-society stakeholders. Working groups were established to review each sector and make recommendations. A key focus sector is national security, which will have cybersecurity as a major focus.

There has also been support to the Royal Saint Lucia Police Force from the French government to assist in building the human resource capacity in cybersecurity through various training initiatives. The Computer Misuse Act of 2011 came into force July 6, 2018, and the eTransactions Act[315] and Data and Privacy[316] was passed by the Parliament of Saint Lucia in 2011.[317]

Further to this, the DPSM has established working groups with the E-government Task Force to develop a CSIRT Roadmap and Cybersecurity Policy and Strategy. Once completed, these will be reviewed and submitted for approval and funding.

As the Government of Saint Lucia evolves to more citizen-centric government through the implementation of key ICT initiatives, cyberthreats are even more of a reality. To this end the DPSM is also partaking in the Cyber Incident Response: Building Capacity in the Commonwealth program. This is an effort to ensure that the right capacity, support, and systems to develop, maintain, and grow a CSIRT are within the government. It must also be noted that every project that the DPSM undertakes has a major focus on security so as to ensure that ICT and data resources are protected. The DPSM has also engaged the services of a legal consultant to review current legislation, identify the gaps, make recommendations, and, in some instances, draft relevant legislation for review and implementation by the attorney general.

Indicators: Saint Lucia

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■□□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■□□□□	■□□□□
User Trust in E-government Services	■□□□□	■□□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■□□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■□□□	■■■□□
Procedural Cybercrime Legislation	■□□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■□□□□	■□□□□
Prosecution	■□□□□	■□□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■□□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■□□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Saint Vincent and the Grenadines

Residents

Ref: World Bank*

2017

109,827

Cell Phone Subscriptions

Ref: ITU**

2017

115,844

Persons with Internet Access

2017

24,167

Internet Penetration

Ref: ITU**

2017

22%

Saint Vincent and the Grenadines has recently taken steps to strengthen its cybersecurity, despite the fact that no national cybersecurity strategy has been developed. As an example of the growing attention to cybersecurity, a national cybersecurity symposium was hosted in December 2017.[318] The symposium, which drew participants from across the eastern Caribbean, was seen as a step towards a more coordinated approach to cybersecurity, with discussions ranging from education and technical capacity initiatives to increase awareness to emphasizing the steps towards establishing a CSIRT, which does not yet exist in the country.[319]

There is some presence of private-sector cybersecurity service provision and there are limited education opportunities for cybersecurity, but the government is aware of the important role education plays in cybersecurity, specifically at school and community levels.[320] Finally, the government does not seem to have provided cybersecurity training opportunities, although Saint Vincent and the Grenadines has sent representatives to several training events organized by the OAS, such as the international cybercrime training on the preservation of digital evidence and internet-based investigations in collaboration with the US State Department in 2016 and the Sub-Regional Workshop on Protection of Critical Infrastructure: Cybersecurity and Border Protection in 2017. Moreover, in May 2017 the Internet Society established a chapter in Saint Vincent and the Grenadines with the aim of promoting an open and trusted internet.[321]

Even though Saint Vincent and the Grenadines already had some legislation concerning cybersecurity, including the Electronic Evidence Act of 2004 and the Electronic Transactions Act of 2015,[322] there was no law specifically for cybercrime. In August of 2016, however, lawmakers passed the Cybercrime Bill 2016[323] into law, thus providing the country with substantive and procedural law to be able to more effectively deal with cybercrime.[324]

Saint Vincent and the Grenadines had an E-government Development Strategy Plan from 2012 until 2015, outlining the steps necessary for the program to "provide a shared technology infrastructure that is stable and secure and which embraces a set of policies and standards for the connection to and use of this shared infrastructure."[325] Furthermore, e-government is part of the SVG National Information and Communication Technology Strategy and Action Plan.[326]

Indicators: Saint Vincent and the Grenadines

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■□□□	■■□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□
1-2 Incident Response		
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■□□□□
1-5 Cyberdefense		
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
1-6 Communications Redundancy		
Communications Redundancy	■□□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■□□□□	■□□□□
User Trust in E-government Services	■□□□□	■■□□□
User Trust in E-commerce Services	■■□□□	■■□□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■□□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■□□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■□□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■□□□□	■■□□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■□□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■□□□□	■□□□□
Prosecution	■□□□□	■□□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■□□□□
5-3 Software Quality		
Software Quality	□□□□□	■□□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■□□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

Suriname

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
570,496	795,871	279,230	49%

Suriname has not yet approved a national cybersecurity strategy, but the government began the process of developing one in collaboration with the OAS in late 2014. Furthermore, the Suriname ICT Vision 2020 calls for the improvement of cybersecurity and increasing awareness of cyberthreats.[327] Regarding a national CSIRT, one has not yet been established but is being developed under the Directorate of National Security.

There are a couple of companies that provide cybersecurity services in Suriname, although these are limited. Further, there are limited opportunities to pursue higher education in cybersecurity in Suriname; the government is beginning to provide trainings on the subject, and has also received support from international organizations for technical training and discussions about cybersecurity.[328]

Since July 2019, the Government of Suriname has officially installed the National Cybersecurity Committee. Due to increasing cyberattacks and cybercrime in Suriname, it is necessary for the IT infrastructure to be improved given the continuous digitization of the world. In connection to this, the Directorate of National Security has set up this committee with the following tasks:

- Updating the cybersecurity strategic plan,
- Implementing the cybersecurity strategic plan, and
- Setting up the national CSIRT.

Suriname has started with its cybersecurity awareness sessions through infomercials, social media, radio and television programs, and official websites.

Suriname has recently added cybercrime into its legislation. The country also made progress in drafting a bill on privacy and data protection, which is still pending before parliament. In December 2018, the parliament passed an Electronic ID (E-ID) legislation.

Suriname has an e-government strategy that aims to improve service to society through a more efficient operation of the government by deploying new digital resources. To implement it, the Government of Suriname established the Commission of E-government, prioritizing the improvement of government-to-government, government-to-business, and government-to-citizen services.[329]

Indicators:
Suriname

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■■□□□	■■□□□
Organization	■□□□□	■■□□□
Content	■□□□□	■■□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□
Mode of Operation	□□□□□	■□□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■□□□□	■□□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■□□□□	■□□□□

1-5 Cyberdefense

	2016	2020
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■□□□□	■■□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■■□□□	■■□□□
Private Sector	■■□□□	■■■□□
Users	■□□□□	■□□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■□□□□	■■□□□
User Trust in E-government Services	■□□□□	■□□□□
User Trust in E-commerce Services	■■□□□	■■■□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■□□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■□□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□

3-2 Framework for Education

	2016	2020
Provision	■□□□□	■□□□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■■□□□	■■□□□
Privacy, Freedom of Speech, and Other Human Rights Online	■□□□□	■■□□□
Data Protection Legislation	□□□□□	■■□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■□□□□	■□□□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■□□□	■■□□□
Prosecution	■□□□□	■□□□□
Courts	■■□□□	■■□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■■□□□	■■□□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■□□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■■□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■■□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Trinidad and Tobago

Residents	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration
Ref: World Bank*	Ref: ITU**		Ref: ITU**
2017	2017	2017	2017
1,384,072	2,030,637	1,070,248	77%

Trinidad and Tobago released its national cybersecurity strategy in 2012 with the overall objective of creating a secure digital environment for its citizens by developing the capabilities to protect against and manage cybersecurity incidents as well as by educating the population on best practices to be able to mitigate risk to the greatest extent. Additionally, the strategy puts forth five key areas to address: governance, incident management, collaboration, culture, and legislation.[330] As a part of the incident management area, Trinidad and Tobago established the national CSIRT through the Ministry of National Security.[331] TTCSIRT is also a member of CSIRT Americas, thus allowing for international collaboration. The strategy also outlines the need for a dedicated agency to take charge of the country's cybersecurity. For the creation of this agency, a bill was proposed for "an Act to provide for the establishment of the Trinidad and Tobago Cybersecurity Agency and for matters relating thereto." However, as of yet, this bill has not been passed.

The cybersecurity strategy defines critical infrastructure as "computer systems, devices, networks, computer programs and computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on the security, defense or international in relations of the state."[332] It has not, however, established ownership of the protection of critical infrastructure but simply mentions that collaboration between government, private sector, and academia is needed to protect critical infrastructure from cyberincidents.

There are some private-sector providers of cybersecurity services, but there is a general lack of private-sector involvement. The Trinidad and Tobago Cybersecurity Agency Bill calls for the enhancement of cooperation between the public and the cybersecurity sector, but cybersecurity is only now starting to be perceived as a priority.[333]

While there is not an extensive offering of degrees in cybersecurity, higher education institutions in Trinidad and Tobago are beginning to introduce some degrees at the university level. Additionally, there are some opportunities provided by the government, like the cybersecurity capacity-building workshop implemented by the Ministry of Planning and Development where secondary and tertiary level students as well as IT professionals could learn the basics of cybersecurity.[334]

Regarding cybercrime legislation, Trinidad and Tobago has a Bill—"An Act to provide for the creation of offences related to cybercrime and related matters"—waiting to be passed. The bill provides a comprehensive definition of various cybercrime offenses as well as the enforcement of cybercrimes. Trinidad and Tobago does have legislation covering data and privacy protection in the form of Act No. 13 of 2011 to provide for the protection of personal privacy and information.[335] This act is applicable to all "who handle, store or process personal information belonging to another person."

Although Trinidad and Tobago does not have a dedicated e-government strategy, it is a part of the fastforward II National ICT Plan which is currently in draft stage. One of the strategic objectives of this plan is to enhance public service delivery, and one of its strategies is to increase government efficiency. Trinidad and Tobago already has a government portal, ttconnect.gov.tt, that provides a number of services, but is aiming to expand the number of e-services available to consumers.[336]

Indicators: Trinidad and Tobago

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■■□□	■■■□□
Organization	■■□□□	■■□□□
Content	■■■□□	■■■□□
1-2 Incident Response		
Identification of Incidents	■■□□□	■■■□□
Organization	■□□□□	■■■□□
Coordination	■■□□□	■■■□□
Mode of Operation	□□□□□	■■■□□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Risk Management and Response	■■□□□	■■□□□
1-4 Crisis Management		
Crisis Management	■□□□□	■■□□□
1-5 Cyberdefense		
Strategy	■■□□□	■■□□□
Organization	■■□□□	■■□□□
Coordination	■■■□□	■■□□□
1-6 Communications Redundancy		
Communications Redundancy	■■□□□	■■□□□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■□□□	■■■□□
Private Sector	■■□□□	■■■□□
Users	■■□□□	■■□□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■■□□	■■■□□
User Trust in E-government Services	■■□□□	■■■□□
User Trust in E-commerce Services	■■■□□	■■■□□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■□□□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■□□□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

3-1 Awareness Raising

	2016	2020
Awareness Raising Programs	■□□□□	■■□□□
Executive Awareness Raising	■■■□□	■■■□□

3-2 Framework for Education

	2016	2020
Provision	■■□□□	■■■□□
Administration	■□□□□	■□□□□

3-3 Framework for Professional Training

	2016	2020
Provision	■■□□□	■■□□□
Uptake	■■■□□	■■■□□

D4 Legal and Regulatory Frameworks

4-1 Legal Frameworks

	2016	2020
Legislative Frameworks for ICT Security	■■■□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■■□□
Data Protection Legislation	□□□□□	■■■□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■■□□
Intellectual Property Legislation	□□□□□	■■■□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■■■□□	■■■□□

4-2 Criminal Justice System

	2016	2020
Law Enforcement	■■■■□	■■□□□
Prosecution	■■□□□	■■■□□
Courts	■■□□□	■■□□□

4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime

	2016	2020
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■□□□

D5 Standards, Organizations, and Technologies

5-1 Adherence to Standards

	2016	2020
ICT Security Standards	■■□□□	■■□□□
Standards in Procurement	■□□□□	■■□□□
Standards in Software Development	■□□□□	■■□□□

5-2 Internet Infrastructure Resilience

	2016	2020
Internet Infrastructure Resilience	■■■□□	■■■□□

5-3 Software Quality

	2016	2020
Software Quality	□□□□□	■■□□□

5-4 Technical Security Controls

	2016	2020
Technical Security Controls	□□□□□	■■□□□

5-5 Cryptographic Controls

	2016	2020
Cryptographic Controls	□□□□□	■■□□□

5-6 Cybersecurity Marketplace

	2016	2020
Cybersecurity Technologies	■■□□□	■■□□□
Cybercrime Insurance	■□□□□	■□□□□

5-7 Responsible Disclosure

	2016	2020
Responsible Disclosure	■□□□□	■□□□□

Uruguay

Residents

Ref: World Bank*

2017

3,436,646

Cell Phone Subscriptions

Ref: ITU**

2017

5,097,569

Persons with Internet Access

2017

2,346,530

Internet Penetration

Ref: ITU**

2017

68%

Uruguay has a cybersecurity framework, although it is not a national cybersecurity strategy. The document is an organized framework with reference to international standards applicable to national regulations for the improvement of cybersecurity of critical infrastructure and public organizations.[337] Uruguay also has a national CSIRT, CERTuy, which is under the Agency for E-government and the Information and Knowledge Society (AGESIC).[338] Uruguay, through the Strengthening Cybersecurity in Uruguay project, became the first country in the region to access technical and financial support through an IDB loan operation focused exclusively on strengthening cybersecurity at the national level.[339] In turn, AGESIC received technical advice led by the IDB for the design of a National Cybersecurity Training Center and support for the Government Security Operations Center (GSOC). CERTuy is also a member of the CSIRT Americas network, so it can make the most of the network's collaborative nature.

Although Uruguay does not define national critical infrastructure, the responsibility for its protection rests with the D-CSIRT, the CSIRT under the Ministry of Defense according to Decree No. 36/015 that created it.[340] In addition, the 2018 AGESIC budget allocated a considerable amount of funding for the strengthening of information security.[341]

Uruguay has some cybersecurity service providers, and there seems to be a good general awareness of cybersecurity issues on the part of the private sector, but the government seems to be providing more of the cybersecurity services and training. For starters, the government offers cybersecurity and cyberdefense courses to participants in the public and private sectors.[342] In addition, CERTuy has a series of guides and best practice manuals on its website that provide resources for anyone wishing to be more informed about cybersecurity.[343] Jointly, there are several universities that offer cybersecurity training and courses.

With respect to the legal and regulatory framework, Uruguay has bills on cybercrime, focused on providing both substantive and procedural law to prosecute cybercrime once it is proven.[344] On the other hand, the country has legislation on protection of personal data and privacy in Law No. 18331, which applies to public and private-sector databases. [345]

Uruguay has its 2020 E-government Plan, with the aim of creating public value through services that meet the needs, expectations, and preferences of citizens in an open, collaborative, intelligent, efficient, integrated, and reliable manner.[346] In addition, e-government was included in the 2020 Digital Agenda as part of the pillar related to innovation in the relationship between the government and its citizens.[347] Currently, Uruguay has a government portal which provides a series of services to track the status of various processes and make appointments with government institutions, for the use of e-signatures, and to obtain relevant information.[348]

Indicators: Uruguay

D1 Cybersecurity Policy and Strategy

	2016	2020
1-1 National Cybersecurity Strategy		
Strategy Development	■■■□□	■■■■□
Organization	■■■□□	■■■■□
Content	■■□□□	■■■□□
1-2 Incident Response		
Identification of Incidents	■■■■□	■■■■□
Organization	■■■■□	■■■■■
Coordination	■■■■□	■■■■■
Mode of Operation	□□□□□	■■■■□
1-3 Critical Infrastructure (CI) Protection		
Identification	■■□□□	■■□□□
Organization	■■□□□	■■■□□
Risk Management and Response	■■□□□	■■■□□
1-4 Crisis Management		
Crisis Management	■■□□□	■■■□□
1-5 Cyberdefense		
Strategy	■■□□□	■■■□□
Organization	■■■□□	■■■□□
Coordination	■■■□□	■■■□□
1-6 Communications Redundancy		
Communications Redundancy	■■■□□	■■■■□

D2 Cyberculture and Society

	2016	2020
2-1 Cybersecurity Mind-set		
Government	■■■■□	■■■■■
Private Sector	■■■□□	■■■□□
Users	■■■□□	■■■□□
2-2 Trust and Confidence on the Internet		
User Trust and Confidence on the Internet	■■■■□	■■■■□
User Trust in E-government Services	■■■■■	■■■■■
User Trust in E-commerce Services	■■■■□	■■■■□
2-3 User Understanding of Personal Information Protection Online		
User Understanding of Personal Information Protection Online	□□□□□	■■■■□
2-4 Reporting Mechanisms		
Reporting Mechanisms	□□□□□	■■■■□
2-5 Media and Social Media		
Media and Social Media	□□□□□	■■■□□

D3

Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■■■■□	■■■■□
Executive Awareness Raising	■■□□□	■■■□□
3-2 Framework for Education		
Provision	■■■□□	■■■□□
Administration	■■■□□	■■■□□
3-3 Framework for Professional Training		
Provision	■■■■□	■■■■□
Uptake	■■■□□	■■■□□

D4

Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■■□	■■■■□
Privacy, Freedom of Speech, and Other Human Rights Online	■■■■■	■■■■■
Data Protection Legislation	□□□□□	■■■■■
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■□□□□	■■□□□
Procedural Cybercrime Legislation	■■□□□	■■□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■■□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■■□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■■□□□
Informal Cooperation	□□□□□	■■■■□

D5

Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■■□□□	■■■■□
Standards in Procurement	■■■□□	■■■■□
Standards in Software Development	■■□□□	■■■■□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■■□□	■■■■□
5-3 Software Quality		
Software Quality	□□□□□	■■■■□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■■■□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■■■■
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■■□□□	■■■□□
Cybercrime Insurance	■■■□□	■■■□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■■■■□

Venezuela

Residents

Ref: World Bank*

2017

29,390,409

Cell Phone Subscriptions

Ref: ITU**

2017

24,493,687

Persons with Internet Access

2017

21,161,094

Internet Penetration

Ref: ITU**

2017

72%

According to data from 2017, Venezuela does not currently have a national cybersecurity strategy. However, there is a national cybersecurity system under the responsibility of the Superintendence of Electronic Certification Services (SUSCERTE), according to the provisions of Article 54 of the Law of E-government.[349] The objective of this system is to create conditions that build trust in the use of ICTs in the hands of those in power and to implement measures that provide adequate security levels for ICT.[350] SUSCERTE is also the headquarters of Venezuela's national CSIRT, VenCERT, the main objective of which is "to prevent, detect and manage the incidents created in the State's information systems and in the critical infrastructure of the Nation by managing cybersecurity vulnerabilities and incidents."[351]

One of the tasks of VenCERT is to provide training in cybersecurity.[352] During the Venezuela Digital 2017 international conference, the superintendent of SUSCERTE highlighted that 687 people were trained in cybersecurity in Venezuela in 2017.[353] In addition, although there do not seem to be many opportunities for Venezuelans to continue their education specifically in cybersecurity, there are many options on related topics, such as computer science or systems engineering.

Some private companies provide information security services. However, the number of companies and the scope of the services they offer are limited. In addition, there seems to be a general lack of knowledge on the part of the private sector regarding cybersecurity, although some leading companies have begun to prioritize cybersecurity.

In terms of legislation, Venezuela introduced the Special Law against Computer Crimes in 2001 with the aim of protecting systems that use information technologies, as well as the prevention and punishment of crimes committed against such systems or through the use of such systems.[354] However, there is no legislation for privacy and data protection,[355] although the articles of the constitution refer to the right to the "protection of honor, private life, privacy, self-image, confidentiality and reputation" (Article 60) and "access to information and data about the person or his/her assets in official or private records"[356] (Article 28).

Indicators: Venezuela

D1 Cybersecurity Policy and Strategy

1-1 National Cybersecurity Strategy

	2016	2020
Strategy Development	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Content	■□□□□	■□□□□

1-2 Incident Response

	2016	2020
Identification of Incidents	■■□□□	■■□□□
Organization	■■■□□	■■■□□
Coordination	■■■□□	■■■□□
Mode of Operation	□□□□□	■■□□□

1-3 Critical Infrastructure (CI) Protection

	2016	2020
Identification	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Risk Management and Response	■■□□□	■■□□□

1-4 Crisis Management

	2016	2020
Crisis Management	■■□□□	■□□□□

1-5 Cyberdefense

	2016	2020
Strategy	■□□□□	■□□□□
Organization	■□□□□	■□□□□
Coordination	■□□□□	■□□□□

1-6 Communications Redundancy

	2016	2020
Communications Redundancy	■□□□□	■□□□□

D2 Cyberculture and Society

2-1 Cybersecurity Mind-set

	2016	2020
Government	■□□□□	■■□□□
Private Sector	■■□□□	■■□□□
Users	■□□□□	■□□□□

2-2 Trust and Confidence on the Internet

	2016	2020
User Trust and Confidence on the Internet	■□□□□	■□□□□
User Trust in E-government Services	■□□□□	■□□□□
User Trust in E-commerce Services	■■□□□	■■□□□

2-3 User Understanding of Personal Information Protection Online

	2016	2020
User Understanding of Personal Information Protection Online	□□□□□	■□□□□

2-4 Reporting Mechanisms

	2016	2020
Reporting Mechanisms	□□□□□	■□□□□

2-5 Media and Social Media

	2016	2020
Media and Social Media	□□□□□	■■□□□

D3 Cybersecurity Education, Training, and Skills

	2016	2020
3-1 Awareness Raising		
Awareness Raising Programs	■□□□□	■□□□□
Executive Awareness Raising	■■□□□	■■□□□
3-2 Framework for Education		
Provision	■■□□□	■■□□□
Administration	■□□□□	■□□□□
3-3 Framework for Professional Training		
Provision	■■□□□	■■□□□
Uptake	■■□□□	■■□□□

D4 Legal and Regulatory Frameworks

	2016	2020
4-1 Legal Frameworks		
Legislative Frameworks for ICT Security	■■■□□	■■■□□
Privacy, Freedom of Speech, and Other Human Rights Online	■■□□□	■■□□□
Data Protection Legislation	□□□□□	■□□□□
Child Protection Online	□□□□□	■■□□□
Consumer Protection Legislation	□□□□□	■■□□□
Intellectual Property Legislation	□□□□□	■■□□□
Substantive Cybercrime Legislation	■■■□□	■■■□□
Procedural Cybercrime Legislation	■□□□□	■□□□□
4-2 Criminal Justice System		
Law Enforcement	■■□□□	■■□□□
Prosecution	■■□□□	■■□□□
Courts	■■□□□	■■□□□
4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime		
Formal Cooperation	□□□□□	■□□□□
Informal Cooperation	□□□□□	■□□□□

D5 Standards, Organizations, and Technologies

	2016	2020
5-1 Adherence to Standards		
ICT Security Standards	■□□□□	■□□□□
Standards in Procurement	■□□□□	■□□□□
Standards in Software Development	■□□□□	■□□□□
5-2 Internet Infrastructure Resilience		
Internet Infrastructure Resilience	■■□□□	■■□□□
5-3 Software Quality		
Software Quality	□□□□□	■■□□□
5-4 Technical Security Controls		
Technical Security Controls	□□□□□	■■□□□
5-5 Cryptographic Controls		
Cryptographic Controls	□□□□□	■■□□□
5-6 Cybersecurity Marketplace		
Cybersecurity Technologies	■□□□□	■□□□□
Cybercrime Insurance	■□□□□	■□□□□
5-7 Responsible Disclosure		
Responsible Disclosure	■□□□□	■□□□□

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

IDB
Improving lives

OAS
More rights
for more people

Appendix

List of CSIRTs

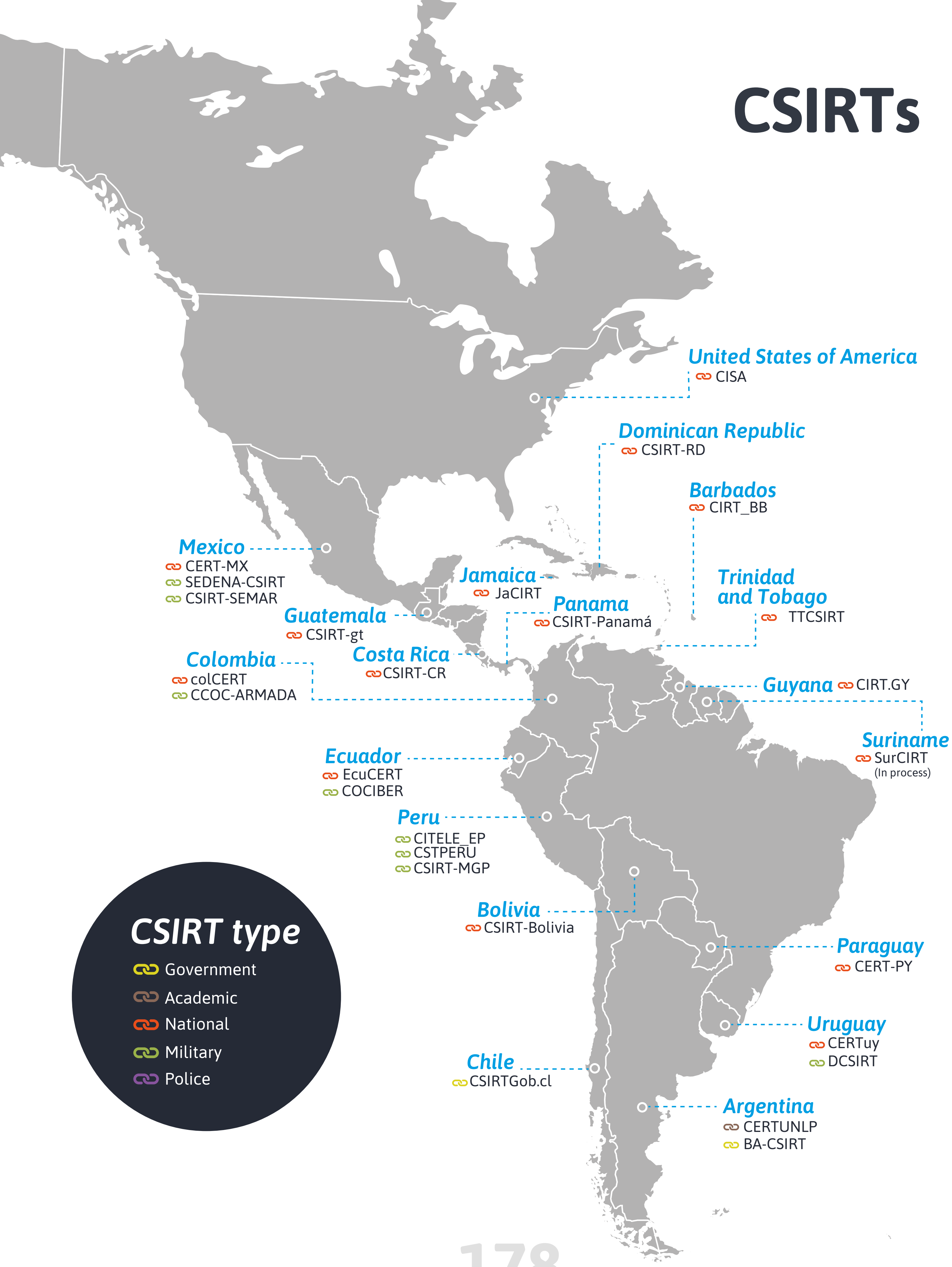
Countries With or Developing a National Cybersecurity Strategy

Members and Observers of the Budapest Convention

Acronyms

References

CSIRTs


United States of America
CISA
Dominican Republic
CSIRT-RD
Barbados
CIRT_BB
Mexico
CERT-MX
SEDENA-CSIRT
CSIRT-SEMAR
Jamaica
JaCIRT
Panama
CSIRT-Panamá
Trinidad and Tobago
TTCSIRT
Guatemala
CSIRT-gt
Colombia
colCERT
CCOC-ARMADA
Costa Rica
CSIRT-CR
Guyana
CIRT.GY
Suriname
SurCIRT
(In process)
Ecuador
EcuCERT
COCIBER
Peru
CITELE_EP
CSTPERU
CSIRT-MGP
CSIRT type
Government
Academic
National
Military
Police
Bolivia
CSIRT-Bolivia
Paraguay
CERT-PY
Uruguay
CERTuy
DCSIRT
Chile
CSIRTGob.cl
Argentina
CERTUNLP
BA-CSIRT

List of CSIRTs

Argentina

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
Government	BA-CSIRT	https://www.ba-csirt.gob.ar/	Ciudad de Buenos Aires	Yes
Academic	CERTUNLP	http://www.cespi.unlp.edu.ar/cert	Universidad Nacional de la Plata	Yes

Barbados

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CIRT_BB	n/a	Barbados National Cyber Security Incidence Response Centre	Yes

Bolivia

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CSIRT-Bolivia	http://www.csirt.gob.bo/	n/a	Yes

Chile

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
Government	CSIRTGob.cl	http://www.csirt.gob.cl/	Ministerio del Interior y Seguridad Pública	Yes

Colombia

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	colCERT	http://www.colcert.gov.co/	Ministerio de Defensa	Yes
Military	CCOC-ARMADA	https://ccoc.mil.co	Comando Conjunto Cibernético	Yes

Costa Rica

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CSIRT-CR	https://www.micit.go.cr/	Ministerio de Ciencia, Tecnología y Telecomunicaciones	Yes

Ecuador

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	EcuCERT	https://www.ecucert.gob.ec/	Agencia de Regulación y Control de las Telecomunicaciones del Ecuador	Yes
Military	COCIBER	n/a	Comando de Ciberdefensa	Yes

Dominican Republic

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CSIRT-RD	https://csirt.gob.do/	Presidencia de la República	Yes

Guatemala

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CSIRT-gt	https://www.cert.gt/	Ministerio de Gobernación	Yes

Guyana

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CIRT.GY	https://cirt.gy/	Ministry of Public Security	Yes

Jamaica

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	JaCIRT	https://www.mset.gov.jm/cyber-incident-response-team-jacirt	Ministry of Science, Energy, and Technology	Yes

Mexico

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CERT-MX	https://www.gob.mx/sspc	Comisión Nacional de Seguridad	Yes
Military	SEDENA-CSIRT	https://www.gob.mx/sedena	Secretaría de la Defensa Nacional	Yes
Military	CSIRT-SEMAR	https://www.gob.mx/semar	Secretaría de Marina	Yes

Panama

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CSIRT-Panamá	https://cert.pa/	Autoridad Nacional para la Innovación Gubernamental	Yes

Paraguay

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CERT-PY	https://www.cert.gov.py/	Ministerio de Tecnologías de la Información y Comunicación	Yes

Peru

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
Military	CITELE_EP	http://www.ejercito.mil.pe/cotele/	Comando de Telemática del Ejército del Perú	Yes
Military	CSTPERU	https://fap.mil.pe/	Comando Conjunto de las FF.AA. del Perú	Yes
Military	CSIRT-MGP	n/a	Marina de Guerra del Perú	Yes

Suriname

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	SurCIRT (In process)	www.gov.sr	De Centrale Inlichting en Veiligheidsdienst (CIVD)	Yes

Trinidad and Tobago

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	TTCSIRT	http://ttcsirt.gov.tt/	Ministry of National Security	Yes

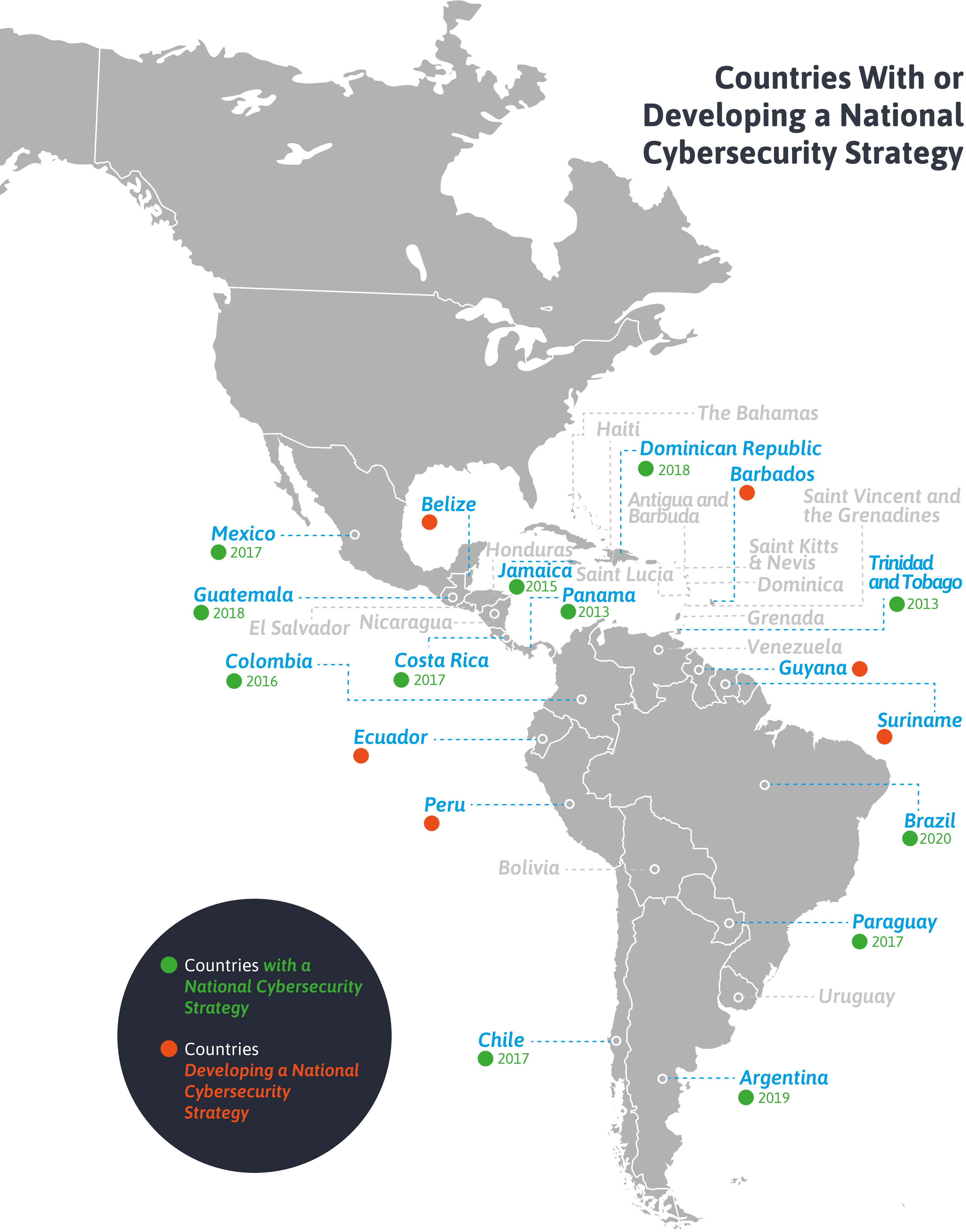
United States of America

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CISA	https://us-cert.cisa.gov/	Department of Homeland Security (DHS)	Yes

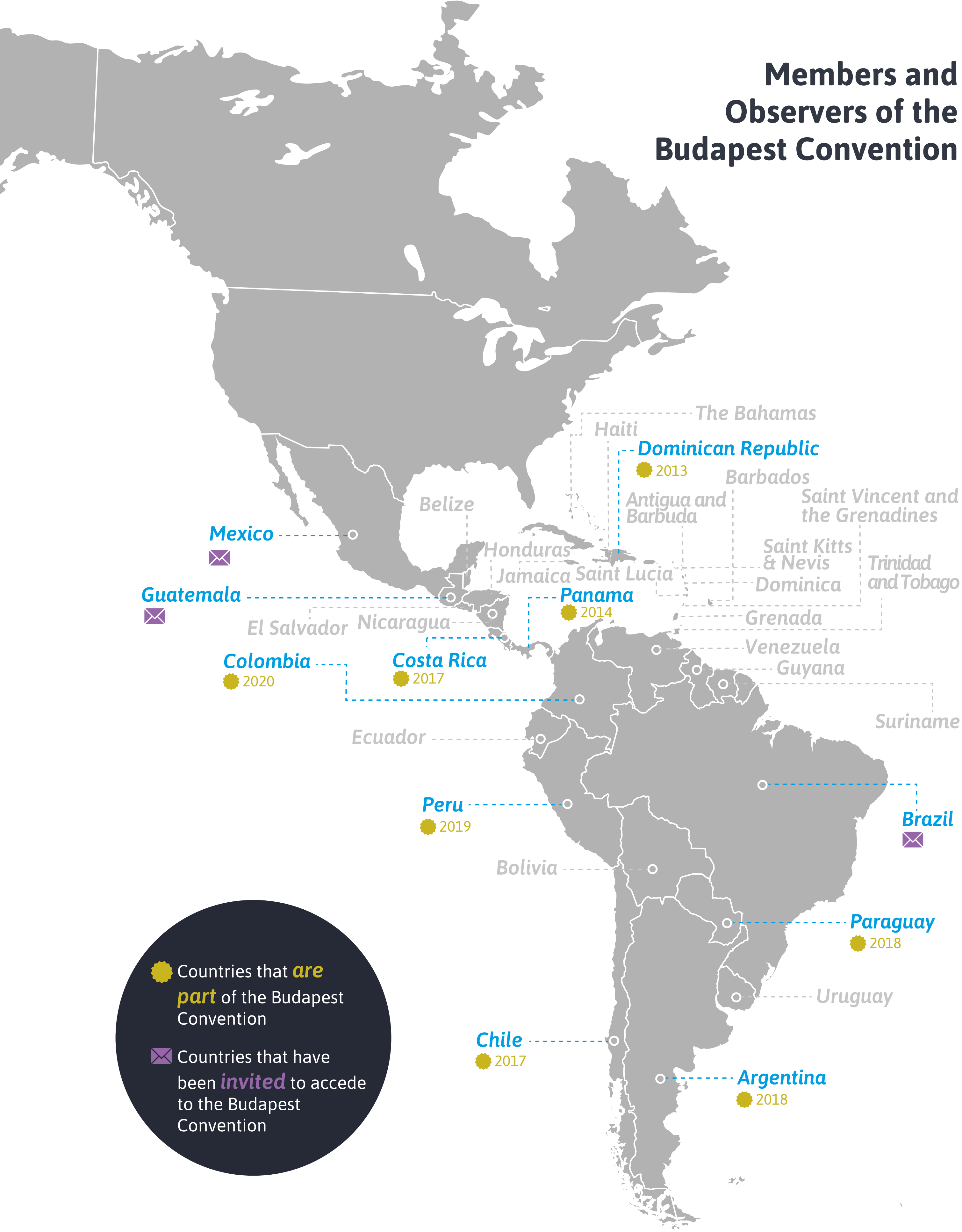
Uruguay

Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
National	CERTuy	https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/	Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento	Yes
Military	DCSIRT	https://www.gub.uy/ministerio-defensa-nacional/	Ministerio de Defensa Nacional	Yes

Countries With or Developing a National Cybersecurity Strategy



Members and Observers of the Budapest Convention



Acronyms

AGESIC
Agency for E-government and the Information and Knowledge Society of Uruguay

AGETIC
E-government and Information and Communication Technologies Agency of Bolivia

ARCOTEL
Telecommunications Regulation and Control Agency of Ecuador

BA-CSIRT
CSIRT of the City of Buenos Aires

CARICOM
Caribbean Community

ccTLD
Country code top-level domain

COE
Council of Europe

CERT
Computer emergency response team

CERT.br
National CERT of Brazil

CERT-MX
National CSIRT of Mexico

CERT-PY
National CSIRT of Paraguay

CERTuy
National CSIRT of Uruguay

CGII
Cyber Incident Management Center of Bolivia

CI
Critical infrastructure

CICCD
Caribbean Israel Centre for Cyber Defense

CIRT.GY
National CSIRT of Guyana

CISM
Certified Information Security Manager (ISACA)

CISSP
Certified Information Systems Security Professional (ISC2)

CITO
Central Information Technology Office of Belize

CMF
Commission for the Financial Market of Chile

CMM
Cybersecurity Capacity Maturity Model for Nations

colCERT
National CERT of Colombia

CONATEL
National Telecommunications Council of Haiti

CONATEL
National Telecommunications Council of Honduras

cPPP
Contractual public-private partnership

CSIRT
Cybersecurity incident Response Team

CSIRT-CR
National CSIRT of Costa Rica

CSIRT-gt
National CSIRT of Guatemala

CSIRT-RD
National CSIRT of the Dominican Republic

CSTF
National Cyber Security Task Force of Belize

D-CSIRT
CSIRT of the Ministry of Defense of Uruguay

DPSM
Division of Public Sector Modernization of Saint Lucia

ECSO
European Cyber Security Organization

EcuCERT
National CSIRT of Ecuador

E-ID
Electronic ID

EU
European Union

Europol
European Union Agency for Law Enforcement Cooperation

GCI
Global Cybersecurity Index

GCSCC
Global Cyber Security Capacity Centre

GDPR
European General Data Protection Regulation

GITS
Government Information Technology Services of Saint Lucia

GLACY+
Global Action on Cybercrime Extended

GSOC
Government Security Operations Center

GTCSC
Working group for cybersecurity and cybercrime of Haiti

HPC
High-performance computer

ICCN
Critical national cybernetic infrastructure

ICIC
National Program of Critical Infrastructures for information and Cybersecurity of Argentina

ICT
Information and communication technology

IDB
Inter-American Development Bank

INCIBE
National Cybersecurity Institute of Spain

INTERPOL
International Criminal Police Organization

ITU
International Telecommunications Union

JaCIRT
National CSIRT of Jamaica

MFF
EU Multiannual Financial Framework Programme

MICITT
Ministry of Science, Technology and Telecommunications of Costa Rica

MinTIC
Ministry of Technology and Communications of Colombia

MISP
Malware Information Sharing Platform and Threat Sharing

MITIC
Ministry of Information Technologies and Communications of Paraguay

MPTC
Ministry of Public Works, Transport, and Communication of Haiti

MSET
Ministry of Science, Energy, and Technology of Jamaica

NIS
Network and information systems

OAS
Organization of American States

ONGEI
National Office of E-government and Information Technology of Peru

OSCE
Organization for Security and Co-operation in Europe

PBL
Policy-based loan

PeCERT
National CSIRT of Peru

PUC
Belize Public Utilities Commission

PwC
PricewaterhouseCoopers

R&I
Research and innovation

SalCERT
National CSIRT of El Salvador

SERCOP
National Public Procurement Service of Ecuador

SINARDAP
National System of Public Data Registration of Ecuador

SMEs
Small- and medium-sized enterprises

SUSCERTE
Superintendence of Electronic Certification Services of Venezuela

TELCOR
Nicaraguan Institute of Telecommunications and Postal Services

TTCSIRT
National CSIRT of Trinidad and Tobago

UNGGE
United Nations Group of Governmental Experts

VenCERT
National CSIRT of Venezuela

References

1. ThreatMetrix Cybercrime Report: An Interview (November 2019). https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/.

2. www.trends.google.com.

3. The numbers represent the search interest in relation to the highest point on the graph for the given region and time. A value of 100 is the maximum popularity of the term. A value of 50 means that the term is half popular. A score of 0 means that there was not enough data for this term.

4. Refer to https://eeas.europa.eu/topics/eu-global-strategy_en.

5. European Commission. 2017. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en.

6. European Commission. 2015. The European Agenda on Security. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

7. European Commission. 2016. Joint Framework on countering hybrid threats: a European Union response. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

8. European Commission. 2017. Launching the European Defence Fund. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0295&from=EN.

9. Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016, concerning measures for a high common level of security of network and information systems across the Union.

10. Directive 2013/40/EU from the European Parliament and of the Council of August 12, 2013, relative to attacks against information systems.

11. The Convention on Cybercrime is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, and violations of network security. In 2017, 55 governments had ratified or acceded to the Council of Europe Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

12. European Commission. 2017. Digital4Development: mainstreaming digital technologies and services into EU Development Policy. Available at: https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-157-F1-EN-MAIN-PART-1.PDF.

13. In September 2017, the EU had cyberdialogues with the United States, China, Japan, the Republic of Korea, and India.

14. See http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

15. Hintermann, Francis. 2020. 3 Powerful Ways the Pandemic Is Changing Research Forever. Available at https://www.accenture.com/us-en/blogs/accenture-research/3-powerful-ways-the-pandemic-is-changing-research-forever.

16. International Data Corporation. 2019. The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. Available at https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

17. WEF (World Economic Forum) 2020. The Global Risks Report 2020. Available at https://www.weforum.org/reports/the-global-risks-report-2020.

18. WEF (World Economic Forum). 2020. COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications. Available at https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications.

19. Cybersecurity Ventures. 2019. The 2019 Official Annual Cybercrime Report. Available at https://www.herjavecgroup.com/resources/2019-official-annual-cybercrime-report/.

20. WEF (World Economic Forum). 2018. Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society. Available at http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf.

21. OECD (Organization for Economic Co-operation and Development). 2019. Shaping the Digital Transformation in Latin America: Strengthening Productivity, Improving Lives. Paris: OECD Publishing. Available at https://doi.org/10.1787/8bb3c9f1-en.

22. ECLAC. 2018. Proposed Digital Agenda for Latin America and the Caribbean (eLAC2020). Sixth Ministerial Conference on the Information Society in Latin America and the Caribbean. Available at https://repositorio.cepal.org/bitstream/handle/11362/43464/S1800206_en.pdf.

23. WEF (World Economic Forum) 2020. Incentivizing responsible and secure innovation: Principles and guidance for investors. Available at https://www.weforum.org/reports/incentivizing-responsible-and-secure-innovation-a-framework-for-entrepreneurs-and-investors.

24. AustCyber. 2019. Australia's Cyber Security Sector Competitiveness Plan 2019: Driving Growth and Global Competitiveness. Available at https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019.

25. OAS (Organization of American States) and ISA (Internet Security Alliance). 2019. Cyber-Risk Oversight Handbook for Corporate Boards. Available at https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf.

26. OECD et al. 2019. Latin American Economic Outlook 2019: Development in Transition. Paris: OECD Publishing. Available at https://doi.org/10.1787/8bb3c9f1-en.

27. The Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (GGE) established by UN General Assembly Resolution 73/266 and the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) established by UN General Assembly Resolution 73/27.

28. Inter-American Committee against Terrorism. 2017. Resolution CICTE / RES. 1/17 Establishment of a Working Group on Measures of Promotion of Cooperation and Trust in Cyberspace. Adopted at the 17th plenary session, held on April 7, 2017. Available at https://www.oas.org/en/sms/cicte/session_2017.asp.

29. IDB . 2016. Available at https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.

30. https://www.oxfordmartin.ox.ac.uk/cyber-security/.

31. https://www.dcc.uchile.cl/seguridad.

32. http://postgrados.derecho.uchile.cl/diploma-ciberseguridad-pf/.

33. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0.

34. Source: Global Cyber Security Capacity Centre.

35. https://technewstt.com/caribbean-cybersecurity-dev/.

36. https://www.caricom.org/media-center/communications/news-from-the-community/caribbean-nations-sign-off-on-cyber-crime-action-plan.

37. https://www.thecaribbeanradio.com/antigua-barbuda-to-host-ict-week-and-symposium/;
https://today.caricom.org/2017/03/01/antigua-and-barbuda-to-host-ctu-ict-week-and-symposium/.

38. https://ab.gov.ag/pdf/budget/2017_Budget_Summary.pdf.

39. OAS Online Survey.

40. https://stopthinkconnect.org.ag/.

41. https://abiit.edu.ag/programs/.

42. http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf.

43. http://laws.gov.ag/wp-content/uploads/2019/02/a2013-10.pdf.

44. https://ab.gov.ag/detail_page.php?page=30.

45. https://www.youtube.com/playlist?list=PL9-4wsDIxlCBn_AKzvPD7cBjf_Q7969IA.

46. http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm.

47. Information provided by the country.

48. Information provided by the country.

49. Project AR-L1304: https://www.iadb.org/en/project/AR-L1304.

50. https://www.state.gov/joint-statement-on-u-s-argentina-partnership-on-cyber-policy/.

51. Information provided by the country.

52. https://www.argentina.gob.ar/modernizacion/direccion-nacional-ciberseguridad/normativa.

53. https://www.pwc.com.ar/es/prensa/ciberseguridad-empresas-argentinas-no-protegen-informacion-sensible.html.

54. http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

55. Information provided by the country.

56. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/ARG?p_auth=RS1Kx55S.

57. http://www.oas.org/juridico/PDFs/arg_ley25326.pdf.

58. http://www.oas.org/juridico/PDFs/arg_ley25326.pdf.

59. http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/105829/norma.htm.

60. https://dpicuantico.com/sitio/wp-content/uploads/2017/02/87-2017.pdf.

61. http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/316036/norma.htm.

62. http://www.thebahamasweekly.com/publish/bis-news-updates/New_Cyber_Security_Strategy_to_strengthen_data_protection_capabilities34602.shtml;
http://caribbean.cepal.org/news/bahamas-embarks-new-national-cyber-security-strategy-strengthen-data-protection-capabilities.

63. https://thenassauguardian.com/2018/05/11/cybercrime-up-80-percent/.

64. https://bit.ly/2QwdUs7.

65. http://www.tribune242.com/news/2017/jul/21/bahamas-must-do-more-to-combat-cyber-crime/.

66. http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf.

67. http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf.

68. Project BH-L1045: https://www.iadb.org/en/project/BH-L1045.

69. https://www.securehost.com/wp-content/uploads/docs/EBusinessPolicy.pdf.

70. http://www.vision2040bahamas.org/media/uploads/Draft__National_Development_Plan_01.12.2016_for_public_release.pdf, p. 52.

71. https://www.bahamas.gov.bs/wps/portal/public/gov/government/eServices/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOKN3f19A51NLHwtAhxdDTwNQ_z9Ag19DP2djPULsh0VAZl2VXA!/

72. https://www.bibtbahamas.com/copy-of-mp-business.

73. https://www.bifs-edu.com/cyber-security-.

74. http://www.centralbankbahamas.com/news.php?cmd=view&id=16419.

75. http://gisbarbados.gov.bb/blog/cybersecurity-strategy-for-barbados/.

76. Project BA-L1046: https://www.iadb.org/en/project/BA-L1046.

77. https://www.intgovforum.org/multilingual/system/files/filedepot/21/barbados_igf_annual_2017_report.pdf.

78. http://gisbarbados.gov.bb/blog/stronger-cyber-security-paramount/.

79. See cybersecurity service providers such as
https://www.caribbeancsc.com/ and https://advantagecaribbean.com/cyber-security/.

80. http://www.oas.org/juridico/spanish/cyb_bbs_computer_misuse_2005.pdf.

81. https://www.barbadosparliament.com/bills/details/396.

82. https://www.barbadosparliament.com/htmlarea/uploaded/File/Resolutions/Resolution_E_Government_Strategy_2006.pdf.

83. https://www.blp.org.bb/wp-content/uploads/2017/07/bb_National_ICT_Strategic_Plan_Final_2010.pdf;
https://repositorio.cepal.org/bitstream/handle/11362/39858/S1501269_en.pdf?sequence=1.

84. http://gisbarbados.gov.bb/blog/government-pushing-digital-technology/.

85. http://www.caribbean360.com/business/barbados-moves-to-introduce-digital-payment-network.

86. https://www.intgovforum.org/multilingual/system/files/filedepot/21/barbados_igf_annual_2017_report.pdf.

87. http://www.cavehill.uwi.edu/programmes/#FacultyAnchor.

88. https://businessviewcaribbean.com/belize-cyber-crimes-security-symposum-raises-awareness/.

89. https://www.ub.edu.bz/academics/academic-faculties/faculty-of-science-and-technology/.

90. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

91. http://www.siliconcaribe.com/2017/05/05/belize-leads-caribbean-race-to-cyberattack-preparedness/.

92. https://developernetwork.azurewebsites.net/cito.gov.bz/egovpolicy/BelizeNatleGovPolicy2015.pdf.

93. https://web.senado.gob.bo/prensa/noticias/aprueban-pl-que-declara-prioridad-nacional-la-elaboraci%C3%B3n-e-implementaci%C3%B3n-de-la.

94. https://www.cgii.gob.bo/es/normativa.

95. https://www.cgii.gob.bo/es/acerca-del-cgii.

96. https://www.csirtamericas.org/.

97. OAS Online Survey.

98. Art. 363 of the Penal Code.

99. Supreme Decree No. 28168, Access to Information.
https://www.comunicacion.gob.bo/?q=20130725/decreto-supremo-n%C2%BA-28168-acceso-la-informacion.

100. https://coplutic.gob.bo/IMG/pdf/plan_gobierno_electronico_.pdf.

101. Law No. 1080/2018, Law of Digital Citizenship.

102. http://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

103. Proposed Amendment to Constitution No. 17 of 2019. Available at https://www25.senado.leg.br/web/atividade/materias/-/materia/135594

104. Brazilian Penal Code (1940) Decree-Law No. 2.848 of December 7, 1940; Available at:
http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

105. Consumer Protection Code (Law No. 8.078 / 1990); Available at:
https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf.

106. http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

107. https://www.csirt.gob.cl/.

108. https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf.

109. Project CH-L1142 - https://www.iadb.org/es/project/CH-L1142.

110. Project CH-L1142 - https://www.iadb.org/es/project/CH-L1142.

111. http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

112. http://www.ciberseguridad.gob.cl/consulta-ciudadana/.

113. https://alianzaciberseguridad.cl/.

114. https://www.latercera.com/pulso/noticia/gobierno-evalua-exigir-inversion-ciberseguridad-algunas-actividades-del-sector-privado/201537/.

115. https://www.leychile.cl/Navegar?idNorma=30590.

116. https://www.leychile.cl/Navegar?idNorma=141599.

117. http://www.senado.cl/proteccion-a-los-datos-personales-como-derecho-constitucional-sera-una/senado/2018-05-15/181511.html.

118. https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

119. https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25.

120. https://www.unescap.org/sites/default/files/E-Government%20Survey%202018_FINAL.pdf.

121. http://www.agendadigital.gob.cl/files/Agenda%20Digital%20Gobierno%20de%20Chile%20-%20Capitulo%203%20-%20Noviembre%202015.pdf.

122. http://www.agendadigital.gob.cl/files/Agenda%20Digital%20Gobierno%20de%20Chile%20-%20Capitulo%203%20-%20Noviembre%202015.pdf.

123. https://digital.gob.cl/instructivo/acerca-de.

124. https://www.leychile.cl/Navegar?idNorma=1138479.

125. http://www.internetsegura.cl/quienes-somos/.

126. CONPES 3701, 2011 Cybersecurity and Cyberdefense Guidelines, July 2011. Available at https://www.mintic.gov.co/portal/604/w3-article-3510.html.

127. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

128. The Cybersecurity Committee studies the following topics: Policy and Regulations for Cybersecurity, Protection and Defense of National Critical Cybernetic Infrastructure, Cybersecurity Risk Management, Crisis and Monitoring of Cyber Threats, Protection of Personal Data, International Cybersecurity Issues, and Strategic Communications for Cybersecurity.

129. http://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=83433; https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

130. This function is carried out collaboratively together with the Joint Cyber Command (CCOC) of the General Command of the Military Forces and the Police Cyber Center (CCP) of the National Police, the Government CSIRT, the Financial CSIRT, the Attorney General's Office of the Nation, sectoral cybersecurity connections, and other initiatives of sectoral and private CSIRTs, as well as national entities or links with response teams of other countries and international organizations which, under their mission statement, contribute to computer incident response. Likewise, and in case an incident that could lead to a national crisis is detected, ColCERT immediately reports to the National Cybersecurity Coordinator to activate the Cybersecurity Committee to handle the crisis.

131. Likewise, the Risk, Corruption, and Cybersecurity Administration Guide was issued, addressed to all entities of the executive branch providing a methodology to effectively manage the risks that affect the achievement of strategic and process objectives, including those associated with cybersecurity. Likewise, the Communications Regulation Commission (CRC) issued Resolution No. 5569 of 2018, "modifying article 5.1.2.3 of Chapter I of Title V of Resolution CRC 5050 of 2016 in matters of security management in telecommunications networks and issuing other provisions."

132. Project CO-L1233: https://www.iadb.org/en/project/CO-L1233.

133. https://www.mintic.gov.co/portal/604/w3-article-15119.html.

134. https://www.mintic.gov.co/portal/604/w3-article-11319.html.

135. http://www.oas.org/es/sap/dgpe/escuelagob/novedades_OEA-capacita-estudiantes-seguridad-digital.asp.

136. https://www.enticconfio.gov.co/quienes-somos.

137. http://www.oas.org/juridico/spanish/cyb_col_ley1273.pdf.

138. https://www.dnp.gov.co/programa-nacional-del-servicio-al-ciudadano/Paginas/Proteccion-de-datos-personales.aspx.

139. http://www.sic.gov.co/sites/default/files/files/Superintendente_Proteccion_Datos_Personales.pdf.

140. https://www.interpol.int/en/Who-we-are/Member-countries/Americas/COLOMBIA; https://www.europol.europa.eu/agreements/colombia

141. For example, the United Nations Commission on Crime Prevention and Criminal Justice, Groups of Experts and of Open Members; the Confidence-Building Measures Working Group of the Organization of American States (OAS), where Colombia served as Group Chair in 2018; the Pacific Alliance; the Budapest Convention of the Council of Europe; the European Cybercrime Centre (EC3); the North Atlantic Treaty Organization (NATO); EUROPOL and INTERPOL.

142. http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf.

143. http://estrategia.gobiernoenlinea.gov.co/623/articles-7929_recurso_1.pdf; http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf.

144. https://www.micit.go.cr/files/estrategia-nacional-ciberseguridad.

145. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC.

146. OAS Online Survey.

147. https://www.tec.ac.cr/fundatec/especialista-gestion-ciberseguridad-empresarial.

148. https://presidencia.go.cr/comunicados/2018/02/expertos-espanoles-estan-en-costa-rica-para-capacitar-a-funcionarios-publicos-sobre-ciberseguridad/;
https://micit.go.cr/index.php?option=com_content&view=article&id=10337:estudiantes-costarricenses-reciben-capacitacion-en-seguridad-digital-de-la-oea&catid=40&Itemid=630.

149. https://www.imprentanacional.go.cr/pub/2012/11/06/ALCA172_06_11_2012.pdf.

150. https://www.elfinancierocr.com/economia-y-politica/costa-rica-enfrenta-el-cibercrimen-con-armas-oxidadas/RIDQNOWPORGAJEES3DRE7KKEPE/story/.

151. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

152. http://www.firma-digital.cr/plan_maestro_gob_digital.pdf.

153. https://dominicastatecollege.com/?page_id=2818.

154. https://www.dominicavibes.dm/education-175314/.

155. http://www.dominica.gov.dm/laws/2010/Electronic%20Evidence%20no.%2013.pdf.

156. http://www.dominica.gov.dm/laws/2013/Electronic%20Filing,%202013%20ACT%2020%20of%202013.pdf.

157. http://www.dominica.gov.dm/laws/2013/Electronic%20Funds%20Transfer%20Act,%202013%20ACT%2017%20of%202013.pdf.

158. http://www.dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf.

159. https://indotel.gob.do/media/10605/decreto-230-18.pdf.

160. http://optic.gob.do/wp-content/uploads/2019/02/Decreto-258-16.pdf.

161. http://www.oas.org/juridico/PDFs/repdom_ley5307.pdf.

162. https://indotel.gob.do/media/6200/ley_172_13.pdf.

163. Article 44, Paragraph 2, and Article 70 of the constitution.

164. https://indotel.gob.do/media/6200/ley_172_13.pdf.
http://dominicana.gob.do/index.php/politicas/2014-12-16-20-56-34/politicas-para-el-buen-gobierno/politica-de-privacidad.

165. https://www.ecucert.gob.ec/nosotros.html.

166. http://www.oas.org/juridico/pdfs/mesicic4_ecu_estat.pdf.

167. https://www2.deloitte.com/ec/es/pages/risk/articles/cyber-risk-2018.html.

168. https://indotel.gob.do/media/6200/ley_172_13.pdf.

169. http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf.

170. https://vlex.ec/vid/codigo-organico-integral-penal-631464447?_ga=2.104058179.2107735450.1529940398-1975001013.1529940398#section_35.

171. Article 66, Paragraph 19 of the constitution.

172. The Organic Law of Communication, the Organic Law of Telecommunications, and the Regulations to the Organic Law of Telecommunications have articles related to the protection of personal data.

173. https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/250%20protec-intimidad-grivadeneira-12-07-2016/PP-protec-intimidad-grivadeneira-12-07-2016.pdf.

174. Source: Member state.

175. https://ec.okfn.org/files/2014/12/PlanGobiernoElectronicoV1.pdf.

176. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf.

177. Article 10 (5 and 11), Organic Law of the National Public Procurement System. Available at https://www.epn.edu.ec/wp-content/uploads/2018/08/Ley-Org%C3%A1nica-de-Contrataci%C3%B3n-P%C3%BAblica.pdf.

178. https://www.gobiernoelectronico.gob.sv/wp-content/uploads/2018/09/Estrategia-de-Gobierno-Digital-2022.pdf.

179. https://www.dinero.com.sv/es/economia/el-salvador-busca-la-transformacion-digital-desde-el-gobierno.html; http://secretariatecnica.egob.sv/transformacion-del-estado/dgte-gobelectronico/.

180. Information provided by the country.

181. https://universidades.sv/carreras/administracion-de-las-tecnologias-de-la-informacion.

182. https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073646641_archivo_documento_legislativo.pdf.

183. https://www.asamblea.gob.sv/decretos/details/166.

184. https://www.gobiernoelectronico.gob.sv/wp-content/uploads/2018/09/Estrategia-de-Gobierno-Digital-2022.pdf.

185. http://www.secretariatecnica.gob.sv/gobierno-lanza-politica-de-datos-abiertos-y-presenta-portal-datos-gob-sv/; http://www.secretariatecnica.gob.sv/lanzan-el-sistema-integrado-de-gestion-administrativa-siga/.

186. http://tenoli.gobiernoelectronico.gob.sv/.

187. https://www.gobiernoelectronico.gob.sv/?p=483.

188. http://www.nowgrenada.com/2014/02/cyber-security-strategy-needed-fight-cyber-crimes/.

189. OAS Online Survey.

190. https://www.gov.gd/hop/acts.

191. https://www.oecs.org/en/procurement/e-gov/data-protection-act.

192. https://www.gov.gd/short-medium-term-ict-plan-government-ict-functions-be-ready-approval-within-months.

193. http://www.gov.gd/egov/docs/ict_egov/draft_2010_2014_CARICOM_egovernment_strategy.pdf.

194. OAS Online Survey.

195. http://mingob.gob.gt/wp-content/uploads/2018/06/version-digital.pdf.

196. https://www.cert.gt/.

197. https://www2.deloitte.com/gt/es/pages/risk/articles/cyber-risk.html; https://www.widefense.com/contacto/; https://www.cyberseg.com/.

198. https://www.linkedin.com/company/soluciones-seguras?originalSubdomain=gt ; https://www.facebook.com/events/ministerio-de-gobernaci%C3%B3n-guatemala/guatemala-mes-de-la-ciberseguridad/389628648376004/ ; https://www.solucionesseguras.com/noticias/soluciones-seguras-cybersecurity-magazine#edicion8 .

199. https://www.isoc.org.gt/ciberseguridad/grupo-de-trabajo-de-ciberseguridad/.

200. http://mingob.gob.gt/viceministerio-de-tecnologia-realiza-capacitacion-sobre-ciberamenazas/.

201. https://mingob.gob.gt/iniciativa-de-ciberdelincuencia-espera-aprobacion-del-congreso-de-la-republica/; http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf.

202. https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/Registro5254.pdf.

[203] Article 1 of initiative No. 5254 of 2017.

[204] http://www.oas.org/es/sla/ddi/docs/G7%20Iniciativa%204090-2009.pdf.

[205] http://www.transparencia.gob.gt/ejes-de-accion/gobierno-electronico/.

[206] https://cirt.gy/about.

[207] https://cirt.gy/.

[208] OAS Online Survey.

[209] https://www.kaieteurnewsonline.com/2019/04/06/guyana-gets-uk-help-to-fight-cyber-crime/.

[210] http://dpi.gov.gy/gpf-launches-zara-cyber-security-centre-lauded-as-exemplary-publicprivate-partnership/; https://guyanachronicle.com/2017/03/22/first-cyber-security-centre-to-be-launched-in-georgetown-thousands-benefit-from-ict-training.

[211] https://www.kaieteurnewsonline.com/2018/08/20/president-assents-to-cybercrime-bill/.

[212] http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

[213] http://parliament.gov.gy/documents/bills/6033-cybercrime_bill_2016_-_no._17_of_2016.doc.

[214] https://dpi.gov.gy/tag/cyber-crime-bill/.

[215] https://doe.gov.gy/gsds.

[216] http://conatel.gouv.ht/node/188.

[217] http://www.haitilibre.com/article-24457-haiti-technologie-vers-un-centre-d-alerte-en-matiere-de-cybersecurite.html.

[218] https://lenouvelliste.com/article/189514/haiti-laudit-informatique-une-necessite-pour-nos-entreprises-aujourdhui.

[219] https://www.lenouvelliste.com/article/171291/cyberattaque-sommes-nous-proteges-ou-en-sommes-nous-en-haiti.

[220] https://www.lamjol.info/index.php/INNOVARE/article/view/5571/5274.

[221] Haiti country report, cyber activities by year.

[222] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

[223] https://www.haititechnews.com/haitila-cyberlegislation-une-necessite-pour-renforcer-le-commerce-electronique/; https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_F.pdf.

[224] http://primature.gouv.ht/?page_id=36.

[225] OAS Online Survey.

[226] http://congresonacional.hn/index.php/2018/02/08/dictamen/.

[227] http://www.sre.gob.hn/portada/2016/Diciembre/08-12-16/Honduras%20da%20%E2%80%9Cun%20gran%20salto%E2%80%9D%20en%20esta%20alianza%20con%20Israel.pdf

[228] Project HO-L1202: https://www.iadb.org/en/project/HO-L1202

[229] Based on the responses received by the OAS Online Survey.

[230] http://www.latribuna.hn/2018/02/09/mexico-apoyara-honduras-materia-ciberseguridad/.

[231] https://ceabad.com/honduras-taller-local-ciberseguridad-como-estrategia-nacional/.

[232] http://www.elheraldo.hn/pais/1168270-466/congreso-nacional-honduras-continua-aprobacion-ley-de-proteccion-datos.

[233] https://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf.

[234] http://agendadigital.hn/wp-content/uploads/2013/10/AgendadigitalCOR.pdf.

[235] https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

236. https://jis.gov.jm/cyber-incident-response-team-fully-equipped-and-operational/.

237. https://mof.gov.jm/documents/documents-publications/document-centre/file/1643-estimates-of-expenditure-2018-2019.html.

238. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

239. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

240. https://www.pwc.com/jm/en/press-room/boards-and-cyber-attacks.html.

241. https://jis.gov.jm/media/Andrew-Wheatley-Sectoral-Presentation-2017.pdf.

242. https://jis.gov.jm/media/Andrew-Wheatley-Sectoral-Presentation-2017.pdf;
https://jis.gov.jm/government-employees-trained-cybersecurity/.

243. https://moj.gov.jm/sites/default/files/laws/Cybercrimes%20Act.pdf.

244. https://moj.gov.jm/laws/cybercrimes-act.

245. http://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf.

246. https://www.japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202017----.pdf.

247. https://planipolis.iiep.unesco.org/en/2009/vision-2030-jamaica-information-and-communications-technology-ict-sector-plan-2009-2030-final.

248. https://www.mset.gov.jm/documents/the-goj-ict-governance-handbook/.

249. https://japarliament.gov.jm/attachments/article/339/The%20National%20Identification%20and%20Registration%20Act,%202017--.pdf.

250. https://www.nidsfacts.com/.

251. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

252. https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es;
http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348059

253. https://www.pwc.com/mx/es/archivo/2019/20190402-digital-trust-pt1.pdf?utm_source=Website&utm_medium=SiteDTrust&utm_content=DescargaPDF1

254. https://www.gob.mx/cms/uploads/attachment/file/274782/Resumen-Ciberseguridad.pdf.

255. https://www.gob.mx/policiafederal/es/articulos/manual-basico-de-ciberseguridad-para-la-micro-pequena-y-mediana-empresa?idiom=es.

256. http://www.informatica-juridica.com/codigo/articulo-211-codigo-penal-federal-mexicano/.

257. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

258. https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf.

259. https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf.

260. https://www.gob.mx/.

261. http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d.

262. https://www.poderjudicial.gob.ni/pjupload/noticia_reciente/CP_641.pdf.

263. https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf.

264. https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf.

265. https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf.

266. https://www.gacetaoficial.gob.pa/pdfTemp/26880/34793.pdf.

267. https://cert.pa/sobre-nosotros/.

268. Project PN-L1114: https://www.iadb.org/en/project/PN-L1114

269. https://yabt.net/news.php?n=cyberseguirdad-panama-2017.

270. https://cert.pa/cursos/.

271. http://www.organojudicial.gob.pa/wp-content/uploads/2016/11/Texto-%C3%9Anico-del-C%C3%B3digo-Penal-2010.pdf.

272. http://www.asamblea.gob.pa/proyley/2017_P_558.pdf.

273. https://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2013/2013_606_1726.pdf.

274. https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf.

275. http://innovacion.gob.pa/descargas/Agenda_Digital_Estrategica_2014-2019.pdf.

276. https://www.mitic.gov.py/materiales/publicaciones/plan-nacional-de-ciberseguridad-paraguay;
https://www.presidencia.gov.py/archivos/documentos/DECRETO7052_5cq17n8g.pdf.

277. https://www.cert.gov.py/index.php;
https://www.presidencia.gov.py/archivos/documentos/DECRETO2274_30nobos1.PDF;
https://www.cert.gov.py/application/files/4115/6642/8626/MITIC_Iniciativas_Ciberseguridad_PY.pdf.

278. Project PR-L1153; https://www.iadb.org/en/project/PR-L1153; https://www.mitic.gov.py/agenda-digital/documentos.

279. National Cybersecurity Plan, p. 26.

280. National Cybersecurity Plan, p. 26.

281. http://www.paraguay.com/nacionales/lanzan-campana-de-ciberseguridad-conectate-seguro-py-105453;
https://www.conectateseguro.gov.py/.

282. http://fiadi.org/wp-content/uploads/2017/10/LEY-4439-DELITOS-INFORMATICOS.pdf.

283. http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado.

284. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

285. http://gestordocumental.senatics.gov.py/share/s/kSvUFg7rSdmez7fA8OTaOA.

286. https://www.senatics.gov.py/application/files/2414/5200/6345/ley_4989_senatics.pdf.

287. https://www.cert.gov.py/index.php/controles-criticos-seguridad.

288. https://www.cert.gov.py/index.php/criterios-minimos-de-seguridad-de-software.

289. https://www.cert.gov.py/index.php/directivas-de-ciberseguridad-para-canales-de-comunicacion-oficiales-del-estado.

290. http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf.

291. https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legisl-ley-n-30618-1548998-4/.

292. https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legisl-ley-n-30618-1548998-4/.

293. https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-para-la-identifica-decreto-supremo-n-106-2017-pcm-1585361-1/.

294. https://www.pecert.gob.pe/index.php/acerca-de-nosotros/que-es-el-pe-cert.

295. https://www.cci-es.org/web/cci/detalle-pais/-/journal_content/56/10694/301898.

296. Project PE-L1222; https://www.iadb.org/en/project/PE-L1222

297. https://elperuano.pe/noticia-expertos-analizan-desafios-y-gestion-seguridad-digital-66976.aspx.

298. Legislative Decree N° 1.412. Available at https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1/.

299. https://busquedas.elperuano.pe/normaslegales/declaran-de-interes-nacional-el-desarrollo-del-gobierno-digi-decreto-supremo-n-118-2018-pcm-1718338-2/.

300. Supreme Decree N° 118-2018. Available at http://www.gobiernodigital.gob.pe/banco/segdi_BUSQ_NORMAS.asp.

301. https://www.gob.pe/institucion/pcm/normas-legales/289706-1412.

302. http://www.leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf.

303. http://www.oas.org/juridico/spanish/cyb_per_ley_27309.pdf.

304. http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf.

305. https://www.sknvibes.com/news/newsdetails.cfm/100223.

306. https://buzz-caribbean.com/article/st-kitts-government-wants-digital-transformation-of-local-economy/.

307. http://www.mof.gov.kn/wp-content/uploads/2017/12/Estimates-2018-Volume-II-Final-Website.pdf.

308. Information received from the country.

309. https://www.unodc.org/res/cld/document/kna/Electronic_Crimes_Act._No._27_of_2009_pmd_-_Electronic_Crimes_Act_No._27_of_2009.pdf.

310. https://www.thestkittsnevisobserver.com/local-news/st-kitts-and-nevis-legislators-pass-data-protection-bill-2018/.

311. https://unstats.un.org/unsd/dnss/docViewer.aspx?docID=2297.

312. http://timescaribbeanonline.com/st-kitts-nevis-government-launches-e-government-portal-that-promises-cost-effectiveness-and-time-efficiency/.

313. Information received from the country.

314. http://www.govt.lc.

315. Electronic Transactions Act N° 16 of 2011.

316. http://www.govt.lc/news/senate-votes-on-data-protection-amendment.

317. https://stluciatimes.com/saint-lucia-to-strengthen-laws-to-protect-cyber-shoppers/.

318. Event supported by the Caribbean Network Operators Group (CaribNOG) and the SVG Chapter of the Internet Society. See http://www.isoc.vc/news-release/st-vincent-to-host-cyber-security-forum/.

319. https://www.caribjournal.com/2017/12/19/st-vincent-moves-strengthen-cybersecurity/.

320. http://finance.gov.vc/finance/images/PDF/the_role_of_education_in_cyber_security.pdf.

321. http://www.isoc.vc/about/.

322. http://www.gov.vc/images/PoliciesActsAndBills/SVG_Electronic_Transactions_Act_2015.pdf.

323. http://www.gov.vc/images/PoliciesActsAndBills/SVG_Cybercrime_Act_2016.pdf.

324. http://www.assembly.gov.vc/assembly/images/stories/cybercrime%20bill%202016.pdf.

325. http://www.gov.vc/images/pdf_documents/svg_egov_development_strategy_report.pdf.

326. http://www.gov.vc/images/PoliciesActsAndBills/SVGICTStrategyAndActionPlanFinal.pdf.

327. http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-555/14.

328. https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2017/20287.aspx; http://www.tas.sr/.

329. https://www.oas.org/es/sap/dgpe/gemgpe/suriname/suriname.pdf.

330. https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf.

331. https://ttcsirt.gov.tt/index.php/background/.

332. https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf.

333. OAS Online Survey.

334. https://www.samtt.com/index.php/programmes/anglia-ruskin-university/msc-network-sec.

335. http://www.ttparliament.org/legislations/b2017h15g.pdf;
http://www.ttparliament.org/legislations/a2011-13.pdf.

336. http://www.ttconnect.gov.tt.

337. https://www.agesic.gub.uy/innovaportal/file/5823/1/marco-de-ciberseguridad-4.0-completo.pdf.

338. https://www.cert.uy/inicio/institucional/que_es_el_cert/;
https://www.agesic.gub.uy/innovaportal/v/33/1/agesic/que-es-agesic.html?idPadre=19.

339. Project UR-L1152: https://www.iadb.org/en/project/UR-L1152.

340. https://www.impo.com.uy/bases/decretos/36-2015.

341. https://www.agesic.gub.uy/innovaportal/file/94/1/prespuesto_2018.pdf.

342. https://tramites.gub.uy/ampliados?id=3847.

343. https://www.cert.uy/seguroteconectas/recomendaciones.

344. https://parlamento.gub.uy/camarasycomisiones/representantes/documentos/repartido/48/433/0/pdf.

345. https://www.impo.com.uy/bases/leyes/18331-2008.

346. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/plan-de-gobierno-digital-uruguay-2020.

347. https://www.agesic.gub.uy/innovaportal/file/6122/1/agenda-uruguay-digital---enero-final.pdf.

348. https://www.gub.uy/.

349. http://www.suscerte.gob.ve/?p=2074.

350. https://www.mppeuct.gob.ve/actualidad/noticias/plan-nacional-de-ciberseguridad-y-ciberdefensa.

351. http://www.suscerte.gob.ve/?page_id=1736.

352. http://www.suscerte.gob.ve/?page_id=1736.

353. http://www.presidencia.gob.ve/Site/Web/Principal/paginas/classMostrarEvento3.php?id_evento=4397.

354. http://www.redipd.es/legislacion/common/legislacion/venezuela/13-leydelitosinformaticos.pdf.

355. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

356. https://web.oas.org/mla/en/Countries_Intro/Ven_intro_fundtxt_esp_1.pdf.

* https://data.worldbank.org/indicator/SP.POP.TOTL.

** https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

www.cybersecurityobservatory.org

CYBERSECURITY

RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN

2020 Cybersecurity Report

2020 Cybersecurity Report

IDB
Improving lives

OAS
More rights for more people

OBSERVATORY OF CYBERSECURITY IN LATIN AMERICA AND THE CARIBBEAN
Home
About
Institutional Information
Credits
Contributors
Contact
Final Reports
Countries data base
Select the criteria you want to explore.
1 Select option to compare
Compare countries
Compare country by year
2 Select the year you want to compare
3 Select specific indicator within each dimension
Cybersecurity Policy and Strategy
Cyber Culture and Society
Cybersecurity Education, Training and Skills
Legal and Regulatory Frameworks
Standards, Organizations, and Technologies
Download
Back to map
© Copyright 2020

www.cybersecurityobservatory.org