2025 CYBERSECURITY REPORT

VULNERABILITY AND MATURITY CHALLENGES TO BRIDGING THE GAPS IN LATIN AMERICA AND THE CARIBBEAN

IDB

OAS | CICTE

Inter-American Development Bank (IDB)

President
Ilan Goldfajn

Project Coordination
Miguel Porrúa

Technical Team
Santiago Paz
Ariel Nowersztern
Jorge Fernando Bejarano
Maria Florencia Baudino
Maria Paula Bordese

Organization of American States (OAS)

Secretary General
Albert Ramdin

Project Coordination
Guillermo Moncayo

Technical Team
Kerry-Ann Barrett
Carlos Eduardo Baena
Mariana Jaramillo
Orlando Garces
Agustin Isidro

Global Cybersecurity Capacity Centre University of Oxford

Professor Sadie Creese
Professor Michael Goldsmith
Carolin Weisser Harris
Patricia Esteve-Gonzalez

Table of Contents

INSTITUTIONAL MESSAGE

Cybersecurity Is Trust for Development

Foreword by
Ilan Goldfajn
President of the IDB Group

Digital services are shaping everyday how governments in Latin America and the Caribbean operate, how people access public goods, and how economies grow. But the benefits of digital public services, dynamic economies, and inclusive access depend on trust — and trust depends on cybersecurity.

Most countries in the region now have national cybersecurity strategies. However, only 13 countries have institutional capacity, resources, or coordination mechanisms to implement their strategies effectively. And just 9 are equipped to protect critical infrastructure — despite the fact that attacks are already disrupting tax administrations, ports, and hospitals. The urgency is clear: institutional gaps are leaving public services exposed.

This publication — the latest in a regional series we've supported since 2016 — offers a clear, evidence-based picture of where each country stands and what's needed next. It is a tool for action: for policymakers, regulators, cybersecurity authorities, and all sectors shaping our region's digital future.

At the IDB Group, we support countries through financing, technical assistance, and knowledge. We support governments in designing national cybersecurity strategies, strengthening legal and regulatory frameworks, training specialized talent, and building institutions to coordinate responses. We also help countries develop Computer Security Incident Response Teams (CSIRTs), protect critical infrastructure, and improve incident detection and response through cross-sector collaboration.

This work is part of our broader mission to create the enabling conditions for private sector-led development. Strong and trusted cybersecurity systems are essential not just for public services, but for doing business, attracting investment, and enabling private sector innovation. The partnership behind this report — with the Organization of American States and the University of Oxford — shows how multilateral and technical institutions can come together to deliver regional public goods.

We hope this report supports national strategies, guides investments, and informs reforms to strengthen digital foundations across the region — and realize the full benefits of a secure digital economy.

Message from the Secretary General of the OAS

Albert R. Ramdin
Secretary General
OAS

The digital revolution has irrevocably transformed the Americas, driving innovation, economic growth, and social connectivity. Yet, as our reliance on digital technologies deepens, so too do the risks posed by cyber threats. Today, the Latin-American and the Caribbean region face a dual challenge: seizing the opportunities of a digital future while safeguarding our societies from cybercrime, state-sponsored attacks, and threats to critical infrastructure.

These threats are intrinsically multinational in nature: malicious actors operate seamlessly across borders, exploiting the interconnectedness of our networks. No single country can confront these risks alone; they demand an orchestrated response that matches their cross-border reach.

Cybersecurity is a cornerstone of the Organization of American States' (OAS) commitment to strengthening security and stability across the region. Because cyber threats transcend national boundaries, our response must be rooted in multilateralism—coordinated, cooperative, and regional in scope. Through the Inter-American Committee Against Terrorism (CICTE), the OAS has worked diligently to support member states in enhancing their cybersecurity policies, capabilities, and resilience. Our commitment is reflected in our ongoing efforts to provide technical assistance, capacity building, and regional cooperation mechanisms that enable countries to better protect their digital ecosystems.

This latest Cybersecurity Maturity Study, developed through a strategic collaboration between the OAS, the Inter-American Development Bank (IDB), and the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, is a vital tool for understanding where our region stands in its cybersecurity preparedness and what steps must be taken to address existing gaps. This study builds upon previous assessments, offering an updated, evidence-based evaluation of cybersecurity

capacity across OAS member states. It provides invaluable insights into how countries are progressing in key cybersecurity domains, from national strategy development to incident response and resilience-building efforts.

Since the release of the 2016 and 2020 Cybersecurity Reports, Latin America and the Caribbean have experienced significant shifts in their cybersecurity landscapes. The increased digitization driven by the COVID-19 pandemic, the surge in cybercrime, and geopolitical tensions have underscored the urgent need for a more comprehensive and proactive approach to cybersecurity. However, despite notable advancements in policy frameworks and institutional capacity, challenges remain. Many countries still lack the necessary financial resources, workforce development programs, and cross-sector coordination to effectively mitigate cyber risks.

This study serves as both a benchmark and a roadmap for strengthening cybersecurity governance in the region. It underscores the critical need for political will, inter-agency collaboration, and sustained investment in cybersecurity capacity-building efforts. The findings highlight areas of progress while also identifying key vulnerabilities that require immediate attention. By leveraging this data, governments, private sector stakeholders, and civil society actors can take informed actions to enhance cyber resilience and protect citizens in the digital space.

This OAS / IDB / GCSCC partnership exemplifies the power of multilateralism. It demonstrates how, by working together, we can orchestrate a coherent regional response to threats that no longer stop at any border. By combining the OAS's regional expertise, the IDB's development focus, and GCSCC's academic rigor, we deliver actionable insights to policymakers. We remain steadfast in our commitment to supporting OAS member states in their cybersecurity journeys. Through continued cooperation, knowledge sharing, and targeted capacity-building initiatives, we can bridge cybersecurity maturity gaps and foster a safer, more resilient digital future for the Americas.

I invite all stakeholders to utilize this report as a tool for informed decision-making and as a catalyst for further investment in cybersecurity. The digital security of our region depends on our collective action. Let us work together to ensure that Latin America and the Caribbean not only navigate the digital age securely but also thrive in it.

EXPERT INSIGHTS

Artificial Intelligence and Cybersecurity: Fostering National AI-Cybersecurity Readiness, and the Need for Collaboration

Prof Sadie Creese

Director, Global Cyber Security Capacity Centre (GCSCC), University of Oxford

Global Cyber Security Capacity Centre

AI is Here to Stay

This regional cybersecurity report by the OAS once again highlights the complexity of cybersecurity and the development of national capacity across the region made in strengthening national cybersecurity capacities across Latin America and the Caribbean. Since the last report, the world has seen a dramatic rise in Artificial Intelligence (AI) adoption. AI applications have moved from the confines of academic research and specialised applications to being embedded, visibly and invisibly, into the daily professional and personal lives of people around the world. AI is integrated into critical national infrastructures (CNI), healthcare, finance, public administration, and the apps people use daily. Large Language Models (LLMs) have gained interest from citizens globally, with capabilities available through commercial platforms and open-source tools.

This is a transformative shift, and it has taken place rapidly, driven by technological innovation, falling barriers to use, and intense international competition to lead AI development and adoption. The AI landscape continues to evolve quickly. Not only in terms of technologies themselves but also within a shifting geopolitical context. We are witnessing changes in global power dynamics, increased competition and risks in technology supply chains, and growing divides between nations leading in AI and those at risk of falling behind. These factors continue to influence how the technologies are developed, deployed and governed.
The growth of AI amplifies existing cybersecurity challenges, introduces new vulnerabilities, and raises critical questions about how strategies, regulation, and capacity-building should adapt to keep pace. Nations are at a critical point: decisions made now about how to govern AI, manage risks, and build cybersecurity capacities will shape their ability to fully harness the benefits that AI will offer for economic growth and prosperity. Responding to these shifts demands thinking about how to build and sustain resilience, both within nations and through regional and international collaboration.

Over the years, the OAS and GCSCC as part of the global cybersecurity capacity-building community have worked to advance understanding of how nations can build effective cybersecurity capacity. We build on that mission now by working towards addressing a pressing challenge: how to ensure that as AI adoption accelerates, it strengthens rather than undermines our collective cybersecurity.

The Critical Need to Consider Cybersecurity in AI

As AI technologies are increasingly used, they create opportunities for innovation, efficiency, and growth. But increasing adoption of AI also fundamentally changes the cybersecurity landscape, bringing new cybersecurity risks, and amplifying existing risks.

Enhancing the capabilities of threat actors: AI gives attackers new tools to improve their operations. AI is transforming the tools, tactics and reach of cybercriminals, with implications for law enforcement, global frameworks, and international cooperation. Developments in AI make it easier for low-skilled criminals to become more effective, while also enhancing the capabilities of sophisticated threat actors. LLMs can help write convincing phishing emails, generate malicious code, find vulnerabilities, and process stolen data. Furthermore, AI-driven obfuscation techniques can help evade traditional security measures. This does not necessarily create new attack methods, but it improves the scale, speed, and success of existing tactics. There is already evidence of known cybercriminal groups using public LLM platforms to support their activities.

Expanding the attack surface: AI systems themselves are vulnerable. Taxonomies such as the MITRE ATLAS, the NIST Adversarial Machine Learning Taxonomy, and the OWASP Top Ten for LLM applications, show the range of ways AI systems can be attacked during training time and inference time, including through adversarial attacks, data or model poisoning, or model inversion, resulting in manipulated outputs or privacy breaches. This amplifies the potential for cyber-harm including societal, potentially physical harms, where these technologies are integrated into CNI and citizen-facing services (which is occurring to varying extents across different nations), and financial and reputational harms to organisations using AI systems. The adoption of agentic AI further brings new attack vectors such as agent hi-jacking, agentic memory poisoning, privilege compromise, and vulnerabilities in agent-to-agent communication protocols.

Furthermore, AI systems rely on complex global supply chains, including models, data, cloud services, hardware, and software that cut across borders and jurisdictions. This creates the risk that threats such as data and model poisoning, could have impacts that spread internationally through components of the supply chain, and widely used AI services.

Broader digital risks: AI developments are also creating digital risks that sit outside traditional cybersecurity frameworks. Deepfakes are a clear example: as synthetic audio and video become more convincing and harder to detect, they can be used for fraud, coercion, and disinformation at scale.

What can Nations do to Withstand these Risks?

Do nations have the capacity to withstand AI-related cybersecurity risks, while maximising the benefits from its adoption? At the GCSCC, we are conducting research into what it means for a nation to build AI cybersecurity readiness. Our aim is to develop a tool that will help nations assess their current state of capability to withstand AI cybersecurity risks.[1] We have convened a series of dialogues with stakeholders from the international cybersecurity capacity-building community and conducted trials with a prototype to understand the risks that AI posed to nations, the national efforts to mitigate these risks, and the main challenges involved in building AI cybersecurity readiness.

The outcome is a set of capacities that might be affected across different domains aligned with the breadth of the Cybersecurity Capacity Maturity Model for Nations (CMM) which underpins this report. These include national cyber policy and strategy; regulation; national incident response; cybersecurity standards; the technologies and services marketplace (including the use of AI to enhance defensive technologies); risk-control practice within organisations; awareness and behaviours around AI security; building trust and confidence for users of digital services; education and professional training; criminal justice; and defence and intelligence.

Guiding the Future of AI Risk Management through Governance, Policy, and Leadership

An effective response to cybersecurity risks in the age of AI requires a solid understanding of how AI is changing the threat landscape, and of which are the most effective ways of that nations within varying contexts can build the capacities to deal with AI-cybersecurity risks. The body of knowledge on AI-cybersecurity is still developing, and many questions remain. For example, what material changes does AI create to a nation's risk landscape? Which threats are realistic and present, and which are still theoretical? What does this mean about the defensive technologies and services that need to be made available, and how can stakeholders within nations be granted access to these capabilities? How do educational and training programmes need to adapt to ensure that people within the nation are ready to face these risks? How do the answers to these questions vary based on a particular nation's context of AI adoption and existing capacities? How can governments with limited resources available for cybersecurity prioritise their actions?

This body of knowledge to support effective capacity building is being built now. Knowledge exchange critical is critical to its development as nations in varying contexts investigate the most effective ways forward.

Strengthening International and Multistakeholder Collaboration

No single nation or institution can solve these challenges alone. Cybersecurity has always required collaboration across borders, sectors and disciplines, and this need is even greater in the age of AI.

- International collaboration: The global nature of AI supply-chains makes collective action essential to manage risks, build resilience, sustain trust, and secure the benefits of digital transformation. Many countries are primarily consumers rather than developers of these technologies and face growing dependencies and inherited vulnerabilities. Yet all nations

are vulnerable to cross-border supply chains for critical components or services. Securing these supply chains is therefore vital not only for strengthening global cybersecurity but also for protecting national resilience. At the same time, AI-driven threats are amplifying existing transnational cybercrime challenges, demanding cooperation to strengthen cross-border capabilities and governance frameworks.

• Cross-sector and interdisciplinary collaboration: Closer collaboration between the AI and cybersecurity communities is critical to ensure that security considerations are built into AI systems from the outset, and that cybersecurity strategies, standards, and capabilities evolve to address the risks posed by rapid advances in AI. At the same time, AI is developing within a wider digital ecosystem that includes existing operational technologies, the growing digitisation of critical infrastructure, increased interconnectivity between sectors, reliance on cloud services, and advances in both classical and quantum computing. Interdisciplinary cooperation with other technical domains is essential to understand how AI interacts with other technologies and to manage potential cascading risks. As AI becomes embedded in critical systems and decision-making processes, cybersecurity takes on greater social, economic, and political significance: breaches or misuse could disrupt essential services and shape public trust. Addressing these challenges requires coordinated action that aligns technical standards, regulation, skills, governance, and public awareness, grounded in real evidence of risks and mitigations.

Therefore, building cybersecurity capacity in the age of AI demands fast, coordinated action across borders, sectors and ecosystems. Working across regions, sectors, and disciplines will be essential to build an inclusive and resilient global AI cybersecurity ecosystem. The choices we make now will shape the security of future generations. Regional organisations like the OAS, with their mandates, existing structures and networks, and the expertise that they have in building cybersecurity capacity, can play a vital role in sharing expertise, aligning policies, and strengthening collective responses.

Political Will and Absorptive Capacity: Fortifying Cybersecurity in Latin America and the Caribbean

Donavon Johnson and Randy Pestana,
Florida International University

Latin America and the Caribbean are at a crossroads when it comes to cybersecurity. In one sense, the onset of the COVID pandemic led to the rapid escalation of connectivity across the region. The proliferation of broadband access to large populations that were previously disconnected, and increased digitalization efforts, brought the region's maturity from the start-up and formative stages to more established and strategic digital environments. In another sense, however, the increased attack surface that accompanied increased maturity, created new avenues for threats to citizens, and an increased demand on leadership to respond to the growing threat of cybersecurity across the Americas.

A case in point is the 2022 attack on Costa Rica's Finance Ministry by the Russian hacker group Conti [2]. The group held sensitive information on citizens for a ransom and crippled the state's ability to provide services to its citizens. In response, Costa Rica became the very first country to declare a state of emergency due to a cyberattack. Conti threatened to overthrow the government while weaponizing public pressure to force government to admit that they do not have the capacity to retrieve the data and pay the ransom. Similar, albeit less dramatic cases were seen across the Americas to include Barbados, Chile, Colombia, Guatemala, Jamaica, Mexico, and Peru, among others.

Leaders in both the public and private sectors are becoming aware of the risks from cyberthreats, but many countries still lack up-to-date cybersecurity frameworks. Effective cybersecurity governance is needed to prevent and manage damages. This requires practical solutions and proactive leadership. Political leaders are at the top of the totem pole and are required to develop policies, legal and regulatory frameworks, and make key decisions on resource allocation and cybermaturity incentives. Their leadership is essential to improving cybersecurity resilience and closing the gap between technological growth and policy, especially in developing nations.

Leadership and the importance of Absorptive Capacity

As danger looms in the form of cybercrime and cyberattacks, the need for cybersecurity has increased across the globe. Consequently, countries have been placing more and more priority on the development and implementation of cybersecurity measures. By February 2019, at least 106 countries had developed and issued a policy instrument[3] However, developing countries have generally been slower to add cybersecurity to their political agendas despite the risks and dangers. Lack of security-centric foresight on the part of political leaders to develop adequate security measures in anticipation of increased cybersecurity threats put citizens across the Americas at risk. Latin America and the Caribbean boasts some of the world's highest rates of smartphone and social media usage and e-commerce gains[4] Despite this, the development of cybersecurity infrastructure and strategies have very little political priority across the region. To illustrate, in 2020, only 12 states in Latin America had a national cybersecurity strategy. A

national cybersecurity strategy is the primary policy tool for organizing a nation's preventive, response, and mitigation actions[5]. Further, in the Caribbean, local law enforcement agencies in their current state are not fully equipped to fight cybercrime[6]. These limited measures make the region an easy target for cybercriminals.

Effective cybersecurity leaders also understand that the cybersecurity landscape is dynamic and ever-changing, creating a need for constant research and development to improve strategies and keep them up to date with emerging trends. Therefore, the ability of regional leaders to foster and enhance the absorptive capacity of cybersecurity organizations and operations, is crucial to our success in cybersecurity resilience, action and capability. Absorptive capacity is a critical factor in advancing cybersecurity resilience, especially in the dynamic stage where nations and organizations can rapidly respond, adapt, and learn from evolving cyberthreats. In Latin America and the Caribbean, most countries have not yet reached this dynamic stage due to limited resources, outdated infrastructure, and a lack of comprehensive cybersecurity frameworks. To build absorptive capacity, leaders must focus on incorporating new knowledge, technologies, and best practices into their national cybersecurity strategies. This involves fostering a culture of continuous learning and adaptation, thereby enabling countries to evolve in response to the ever-changing cybersecurity landscape.

A key enabler of absorptive capacity is the establishment of strong public-private partnerships, which play a crucial role in sharing knowledge and resources for improving cybersecurity capabilities. However, in the Americas, trust gaps between public and private sectors often hinder effective collaboration. Addressing these trust issues is vital for developing a cohesive national cybersecurity strategy. International partnerships, such as those with Canada, and support from multilateral organizations like the Organization of American States (OAS) and the Caribbean Community (CARICOM) can help bolster local cybersecurity efforts through training, funding, and capacity building. These collaborations can serve as models for enhancing absorptive capacity and fostering knowledge exchange within the region.

Examples of absorptive capacity in action include post-incident evaluations, such as Costa Rica's response to the 2022 ransomware attack, which led to the creation of a centralized security operations center. This demonstrates how leaders can learn from cyber incidents to strengthen future defenses. Additionally, local research and investment in education, training, and skills development are essential for fostering long-term cybersecurity resilience. By prioritizing cybersecurity education and encouraging research that is tailored to local contexts, leaders in the LAC region can build a sustainable cybersecurity framework that addresses both current and emerging threats.

Challenges and Opportunities in Cybersecurity Maturity

One of the primary challenges in advancing cybersecurity in Latin America and the Caribbean is the lack of political will, which slows the development of comprehensive cybersecurity strategies. Leaders often prioritize other pressing social and economic issues, leading to fragmented and reactive approaches to cybersecurity. Economic constraints further compound this problem, as many countries struggle to allocate adequate resources to build cybersecurity infrastructure. The result is a lack of coordinated efforts, leaving the region vulnerable to increasingly sophisticated cyber threats. Political transitions and crises, such as natural disasters or changes in government, also disrupt the continuity needed for sustained cybersecurity efforts.

However, Latin America and the Caribbean countries have a unique opportunity to view cybersecurity as a crucial development issue. Integrating cybersecurity into broader economic, social, and national security policies can support long-term growth and stability. Investments in digital infrastructure, when paired with robust cybersecurity measures, can accelerate economic development by fostering safer online environments for commerce, education, and public services. By shifting the perception of cybersecurity from a technical issue to a driver of national progress, political leaders can create a foundation for sustainable development while protecting critical national infrastructure.

There are already success stories in the region that show how countries can advance their cybersecurity capabilities. Jamaica's National Cybersecurity Strategy, for instance, emphasizes the importance of local research and partnerships with both public and private sectors. This approach enables the country to tailor its cybersecurity measures to its specific context, making them more effective and sustainable. By fostering collaboration with academia and international partners, Jamaica is advancing to the strategic and dynamic stages of cybersecurity maturity. This model serves as a blueprint for other Latin America and the Caribbean countries seeking to enhance their cybersecurity resilience while fostering economic and social development.

Conclusion

Leadership, continuous improvement, and the cultivation of absorptive capacity are fundamental to advancing cybersecurity maturity in Latin America and the Caribbean. Political leaders play a pivotal role in ensuring that cybersecurity becomes a national priority, driving the necessary investments in technology, education, and public-private partnerships. Effective leadership fosters a culture of continuous learning and adaptability, which is essential in navigating the ever-evolving cyberthreat landscape. As seen in examples like Costa Rica's post-incident evaluation and Jamaica's National Cybersecurity Strategy, successful cybersecurity initiatives rely on proactive governance and the ability to integrate new knowledge into national frameworks.

Policymakers should consider prioritizing cybersecurity as a key element of national development and investing in long-term strategies that strengthen absorptive capacity. This includes fostering collaboration across sectors, encouraging public-private partnerships, and supporting education initiatives that build the skills needed for sustainable cybersecurity resilience. By addressing these gaps, Latin America and the Caribbean countries can better protect critical infrastructure, promote economic growth, and secure the region's digital future.

Ultimately, Latin America and the Caribbean countries must transition from reactive, formative approaches to a strategic and dynamic cybersecurity governance model. By doing so, they will build the resilience needed to thrive in an increasingly digital world, safeguarding their economies, societies, and national security. The time for decisive action is now.

Advancing Cyber Equity

Tal Goldstein, Head of Strategy, Center for Cybersecurity
World Economic Forum

As the threat landscape continues to evolve in complexity and scale, cybersecurity becomes a critical concern for organizations across industries and economies. In today's digital age, cybersecurity extends beyond merely preventing cyberattacks – it also encompasses ensuring the resilience of critical infrastructure and maintaining trust in digital systems. However, the current cybersecurity environment is marked by an important cyber inequity, a widening gap between the cyber haves and have-nots.

Developed economies, large organizations, and cyber-mature industries often possess advanced capabilities to defend against these threats, while emerging economies, smaller organizations, and less mature sectors face significant challenges due to limited resources and expertise, leaving them more vulnerable in the face of growing cybersecurity risks.

Dissecting Cyber Inequity

Cyber Inequity in Developed and Emerging Economies

From the perspective of developed versus emerging economies, the World Economic Forum's Global Cybersecurity Outlook 2024 reveals that cyber inequity tends to mirror other global development indicators. The lowest number of self-reported cyber-resilient organizations are in Latin America and Africa, while the highest number comes from North America and Europe. This stark disparity in cyber resilience not only exposes organizations in developing economies to greater risks but also poses far-reaching consequences for economic stability and national security in these regions.

For example, a successful attack on critical infrastructure, such as a power grid or healthcare institution could trigger widespread disruptions, affecting the provision of essential services, undermining both economic activities and public trust. In already fragile economies, such disruptions can further impact developmental progress, exacerbate poverty, and create social unrest. Furthermore, given the interconnected nature of the global economy and supply chains, a cyber breach in one region can have a cascading effect elsewhere.

Finally, many emerging economies are beginning to adopt new technologies, oftentimes without necessarily fully understanding the cybersecurity risks that come with them. This lack of awareness and preparedness, in turn, creates significant vulnerabilities that malicious actors may exploit.

Addressing these challenges requires concerted efforts between public and private sectors. In addition, greater global cooperation is essential for facilitating the sharing of knowledge, resources, and best practices to ensure that all regions can collectively advance cyber resilience and thrive in an increasingly digital world. To that end, the World Economic Forum's Centre for Cybersecurity launched the Cyber Resilience in Industries initiative to enhance and scale forward-looking cyber resilience solutions across industry ecosystems including in electricity, manufacturing, oil and gas, and transportation.

Cyber Maturity in Industry Sectors

When observing cyber maturity at a sectoral level, finance is the most advanced. This is largely due to the environment within which the sector operates. A combination of industry- and geography-focused regulations in the U.S. and Europe, for example, drives cybersecurity advancement through compliance obligations. Not only that being unable to comply brings cybersecurity risks and regulatory scrutiny, but it also introduces competitive pressures. The fact that consumers may switch to competitors if they are not confident in the security of their data urges companies to prioritize consumer trust as a crucial part of their business strategy.
That said, profitability of implementing cybersecurity is another dimension worth examining. While cyber maturity and profitability have no direct correlation, studies show that more profitable organizations tend to be more advanced in cyber maturity. The said relation between the level of cyber maturity and profitability illustrates a significant cyber inequity in terms of organization cyber capabilities. Examining organizations that carry cyber insurance by revenue, studies show that 75% of organizations with revenue of over 5.5 billion dollars per year have cyber insurance while 25% of those with less than 250 million dollar of revenue do. High-revenue organizations with financial resources to implement needed cybersecurity measures are likely to secure their profitability. On the other hand, low-revenue organizations may struggle to compete while also being more vulnerable to growing cyber threats.

It is important to recognize the interdependence and interconnectedness of various sectors that form part of a national and global economy. A holistic approach that views cyber resilience as a matter of an ecosystem and considers the interactions among sectors allows more comprehensive understanding of the ecosystem's cybersecurity outlook and threat landscape. In addition to promoting collaboration, this further defines roles and responsibilities. Furthermore, observing cybersecurity maturity with a holistic approach includes understanding the level of cyber maturity across the supply chain which reveals valuable insights on cyber inequity between organizations of various sizes.

Cyber Resilience for Large Organizations and SMEs

According to Mckinsey, cybersecurity maturity varies more widely within sectors than it does from sector to sector. Organizations with high level of cyber resilience are mostly larger organizations. On cyber insurance, for instance, 85% of organizations with over 100,000 employees have cyber insurance compared to 21% of organizations with less than 250 employees. Studies also found that smallest-revenue organizations are three times more likely to lack cyber skills needed to meet their cyber-resilience objectives. This poses a fundamental question of how this cyber inequity threatens the integrity of the entire ecosystem and what can all involved stakeholders do about it.

This phenomenon is alarming given the interconnectedness nature of the cybersecurity ecosystem. A 2023 report from SecurityScorecard and the Cyentia Institute, found that in the last two years, 98% of organizations are connected with at least one third party that has experienced a cyber-attack. This spotlights how cyber resilience is not organization-specific, rather it is a whole-of-society responsibility to minimize cyber inequity.

Small and Medium Enterprise (SMEs) play a crucial role in most economies, particularly in developing countries. They represent around 90% of businesses generating more than 50% of employment worldwide. In emerging markets, most jobs are created by SMEs. These numbers make SMEs' cybersecurity workforce development ever more important.

Cyber Workforce Development

Cyber inequity can also be observed in the context of the workforce. Today's global demand for cybersecurity professionals exceeds the supply, leading to a talent gap of 4.8 million. This shortage encompasses significant disparities in workforce distribution, training opportunities, and career advancement between regions, sectors and demographics.

In developed economies, oftentimes, cybersecurity professionals have better access to extensive educational resources, certifications, and career development opportunities. Universities and specialized training programs in developed economies help create a pipeline of skilled professionals who are equipped to tackle the sophisticated nature of cyber threats. Moreover, developed economies can also provide higher salaries and better working conditions, attracting top talent and further strengthening their cybersecurity capabilities. It then comes as no surprise that the worlds top cybersecurity talent markets are in large part located in the Global North.

On the other hand, developing economies face a critical shortage of cybersecurity talent. To illustrate, in Africa, with a total population of more than 1.4 billion, the number of certified security professionals is estimated to be only around 20,000. Oftentimes, educational institutions in these regions lack the necessary resources to provide comprehensive cybersecurity training, leaving a gap in the local workforce. This shortage is further exacerbated by the brain drain, where skilled professionals migrate elsewhere in search of better opportunities, further depleting the talent pool. As a result, organizations in these emerging economies struggle to build effective cybersecurity teams, leaving them more vulnerable to attacks.

That said, the workforce inequity extends beyond geographic disparities. Certain sectors as well as small and medium-sized enterprises (SMEs) are disproportionately affected by the gap of cybersecurity professionals. From the sectoral point of view, the cybersecurity workforce shortage is especially apparent in sectors such as education, government and healthcare. In fact, for about 52% of public organizations the lack of resources and skills is the biggest challenge when designing for cyber resilience.

Lastly, cyber inequity also has implications on diversity and inclusion. Many underrepresented groups, including women, youth and minorities, are less likely to enter or advance in the cybersecurity field due to systemic barriers such as unequal access to education and training, pay gaps, lack of female role models in cybersecurity, as well a work-life balance challenges. To illustrate, a study by ISC2 found that only 14% of female respondents pursued cybersecurity in school while the global gender pay gap in cybersecurity stand at about 20%.

Addressing the cybersecurity workforce gap requires a global effort to improve access to education, create inclusive career pathways, and foster international collaboration to build a more balanced and effective cybersecurity workforce. To that end, the World Economic Forum's "Bridging the Cyber Skills Gap" initiative has developed a strategic Cybersecurity Talent Framework featuring actionable approaches to help grow the cybersecurity workforce.

Conclusion

Cyber inequity can be observed in various dimensions. Understanding cyber inequity from the perspective of developed and emerging economies demonstrates how structural challenges and barriers are consequential to other aspects of society if left unaddressed. When examining cyber maturity at a sectoral level, the interplay between organizations' cyber capabilities and the environment within which they operate are key factors which illustrate the architecture of inequity. Although organizations are increasingly investing in cyber resilience, the growth pace of cybersecurity often leads to uneven cybersecurity development. This leads to a discussion on affordability and accessibility to resources, tools and talents. As cybersecurity workforce development and talent distribution continues to stay in focus, understanding how intricately organizations, of all types and sizes, interlink highlights how cybersecurity shouldn't be seen as sector- or organization-specific rather it should be viewed as an ecosystem. This way it facilitates determination of roles and responsibilities among stakeholders to minimize cyber inequity and foster cyber resilience.

Measuring What Counts: Gender and Cybersecurity in Latin America and the Caribbean

Dr. Renata H. Dalaqua,
Head of the Gender and Disarmament Programme, UNIDIR
Dominique Steinbrecher,
Researcher – Security and Technology, UNIDIR

Understanding gendered dynamics is key to improving cybersecurity in the context of international security. It is also a way to advance the long-standing quest for gender equality. At a normative level, these two goals – improving cybersecurity and achieving gender equality – are aspirations shared by countries in the Americas region. At a practical level, however, states and cyberstakeholders are not always aware of how to "connect the dots" between these policy areas.

Gender refers to the socially and culturally constructed roles, behaviors and attributes associated with masculinity and femininity in a given time and place. Gender norms are changeable over time; they inform individual identities, social relations, and the distribution of resources and power in society. Although gender is often socially understood as expressing expectations regarding appropriate behavior for men and women, gender is non-binary and diverse.[7]

Gender equality is the principle that people of all gender should have equal conditions, treatment and opportunities for realizing their full potential, human right,s and dignity, and for contributing to and benefitting from economic, social, cultural and political development.[8]

A first starting point should be the realization that cybersecurity threats and ICT-related incidents are experienced differently by people of different genders. For instance, women often rely on mobile and online communications to manage their safety. Cutting off the internet through shutdowns can deprive them of these tools.[9]

Data breaches can also have gendered impacts, disproportionately impacting women and people of diverse genders. A leak of medical records, for example, can expose information about pregnancy and abortion care, which may be illegal in certain places or under certain circumstances. LGBTIQ+ people can have their lives, livelihoods and well-being endangered through non-consensual publication of personal information and involuntary "outing" of their identities.[10]

Therefore, a gendered approach to cybersecurity should recognize that traditional ICT threats have gendered implications and outcomes. It should also recognize that doxing, cyberstalking and the non-consensual dissemination of intimate images are forms of gender-based violence (GBV) that can arise from the intrusion into or disruption of personal devices and networks, or the malicious use of digital technologies.

Online GBV should not be dismissed as an issue that belongs to the private sphere, but rather be addressed as a matter of national and international security, similarly to gender-based violence committed with weapons, for example. The same is true for online violent extremism and online sex trafficking, which target men and boys as well as women and girls but in different ways.

But protecting the cyberspace is not only about avoiding the worst, it is also about developing capacity and seizing the economic and social opportunities facilitated by ICTs. In this regard, a gendered approach also has much to offer. We need well-designed policies and programs to bridge the gender digital divide, that is, the gap in access to, and intensity of the use of, digital technologies between people of different genders. Despite accounting for roughly half of the global population, women represent a disproportionate – and growing – share of the offline population. According to the ITU at a global level, women now outnumber male non-Internet users by 17 per cent, up from 11 per cent in 2019.[11]

It is imperative to bring women online and unlock opportunities for their professional development. As the latest global survey shows, only 25 per cent of cybersecurity professionals worldwide are women.[12] This lack of representation is often accompanied by various forms of inequality, with 87 per cent of women reporting unconscious discrimination and 19 per cent overt discrimination.[13]

Taking action

To address these issues, states and stakeholders in the Americas have started to develop initiatives on gender and cybersecurity. At the regional level, the Organization of American States (OAS), through the Cybersecurity Section of the Inter-American Committee against Terrorism (CICTE), delivers capacity-building and outreach programs that advance gender mainstreaming and support women's participation in cybersecurity.[14] The OAS also established a partnership with the United Nations Institute for Disarmament Research (UNIDIR), with a view to conducting a gender analysis of the framework of responsible state behavior in cyberspace, with a special focus on Latin America and the Caribbean.

To increase cooperation, predictability, transparency, and stability among States in the use of ICTs, the OAS developed a regional framework of Confidence-Building Measures (CBMs) in Cyberspace. Through CBM 7, this framework underscores the importance of promoting women's participation and gender equality in cybersecurity and also links these issues to the women, peace and security agenda.

OAS Confidence Building Measure 7 – "Encourage and promote the inclusion, leadership, and effective and meaningful participation of women in decision-making processes linked to information and communication technologies by promoting specific actions at the national and international levels, with the aim of addressing dimensions around gender equality, and the reduction of the gender digital divide, in line with the women, peace, and security agenda.".[15]

At a national level, several states have integrated gender considerations into their national cybersecurity strategies. Costa Rica and Chile, for example, acknowledged the differentiated impacts of cyberthreats based on gender and the need for cybersecurity to address inequalities and respond to the specific needs of all people.[16] Gender equity is also included as guiding principle in the cybersecurity strategies of Guatemala and Ecuador.[17] Argentina, for its part, mentioned that a gender perspective will be applied to its capacity-building efforts.[18]

Notably, states are also taking action to close the gender digital divide as part of their efforts in the field of development – such is the case of Uruguay, as stated in its Digital Agenda 2025.[19] The Dominican Republic's Digital Agenda 2030 encompasses the development of ICT policies with a gender perspective, the disaggregation of data in the ICT statistics by gender and the deconstructing of gender stereotypes in STEM careers.[20]

Finally, some states in the region have developed national ICT strategies that underscore equal access as a measure to address gender inequalities. This approach is evident in the case of Belize, Saint Kitts and Nevis, Saint Vincent and the Grenadines, and Suriname.[21]

Looking ahead

In light of these developments, it is crucial that cybersecurity assessment models adapt to reflect the ongoing gender mainstreaming efforts and to encourage further action in this area. This is not only a matter of equal rights and opportunities, but also a tried and tested way to avoid blind spots and deliver more effective policies.

The Cybersecurity Capacity Maturity Model (CMM) is certainly a useful tool that addresses different aspects of a state's cybersecurity capabilities, as the analysis in this publication demonstrates. Nevertheless, the model would benefit from integrating gender considerations into all five dimensions of cybersecurity it assesses. After all, models should measure what counts and it is evident that gender issues are a priority for many countries in the region.

For example, Dimension 1 on Cybersecurity Policy and Strategy could look at the inclusion of gender considerations into national cybersecurity strategies, threat models and cyberincident response, as well as critical infrastructure protection that is fit to tackle differentiated impacts of malicious ICT activity. Dimension 2 on Cybersecurity and Society could benefit from analyzing the cybersecurity literacy gap on the basis of gender that may be connected to existing inequalities on ICT access. Dimension 3 on Building Cybersecurity Knowledge and Capabilities

could assess, on the one hand, the development of gender-responsive cybersecurity capacity-building efforts and training programs, and, on the other hand, the level of participation of women and LGBTIQ+ people among the cybersecurity workforce. Dimension 4 on Legal and Regulatory Frameworks could analyze the incorporation of gender considerations into the national legal and regulatory frameworks, paying attention to legal responses to online gender-based crimes and leaks of private information or hacking of medical records, among other types of incidents. Finally, Dimension 5 on Standards and Technologies could measure the developments and implementation of gender-responsive digital technologies and standards development.

In order for this endeavour to be successful, we need concerted action among a range of actors. States, in consultation with wider stakeholders, would need to step up their efforts to collect gender-disaggregated data throughout cybersecurity policy and practice, including aspects such as: gendered differentiated impacts of ICT threats, gender gaps in ICT access, and gender (im)balance regarding participation in cybersecurity discussions. International and regional organizations also have important roles to play, including in the delivery of capacity-building programs and the development of policy-oriented research. Working together, we can ensure that states and citizens alike are protected from cyberthreats.

Digital Transformation and Cybersecurity in Latin America and the Caribbean

Miguel Porrúa
Principal sector specialist in digital government and coordinator of the Data and Digital Government Cluster at the IFD/ICS Unit.
IDB

Introduction

Digital transformation has emerged as a strategic imperative for nations seeking to accelerate economic development, improve public services, and foster social equity. In Latin America and the Caribbean (LAC), where institutional capacity gaps and inequality remain pervasive, the adoption of digital technologies offers a path toward more inclusive and transparent governance. This transformation is not just a matter of deploying technology—it is about reimagining how the state interacts with citizens, businesses, and itself. From health and education to transportation and energy, digital transformation is reshaping the delivery of public goods, making them more efficient, accountable, and responsive. The Inter-American Development Bank (IDB), through its Institutional Strategy 2024-2030, recognizes digital transformation as a key enabler of sustainable growth. (IDB, 2024).

Importantly, the role of cybersecurity in this digital shift has evolved from a support function to a central pillar of institutional resilience, economic prosperity, and democratic governance. In its 2023–2030 Institutional Strategy, the IDB explicitly incorporates cybersecurity within the broader development pillar of "Institutional Capacity, Rule of Law, and Citizen Security." (IDB 2023) This framing recognizes that without digital trust, no digital government reform can succeed. By integrating cybersecurity into the region's institutional development agenda, the IDB underscores its relevance not only for digital service continuity, but also for safeguarding civil liberties, enabling secure digital inclusion, and ensuring stable environments for innovation and investment.

Sectoral and Digital Government Advances in LAC

Over the past decade, LAC countries have advanced significantly in digital transformation across sectors and government. In energy, smart grids, predictive maintenance, and decentralized management with prosumers and microgrids have improved resilience (IDB 2022b). Transportation benefits from AI and IoT for logistics and mobility, while water and sanitation utilities apply digital twins and GIS for resource efficiency. Health systems accelerated telemedicine, electronic records, and digital platforms during the pandemic, as seen in Chile and Uruguay. Justice systems are adopting digital case files, virtual hearings, and AI tools to expand access and reduce backlogs.

At the government level, countries like Uruguay, Chile, Argentina, and Brazil rank highest in the UN's EGDI, reflecting progress in digital services and e-participation (UN 2024). Open data governance is strengthening in Colombia, Brazil, and Perú (OECD 2023), while the World Economic Forum's Network Readiness Index highlights Brazil, Costa Rica, Uruguay, and Chile as regional leaders. Yet disparities persist: leading nations integrate whole-of-government strategies, while others face fragmented systems, low adoption, and outdated platforms. Closing these gaps requires capacity building, inclusive access, and cybersecurity.

Cybersecurity as a Foundational Enabler

Trust is the currency of the digital age, and cybersecurity is its guarantor. Without it, even the most sophisticated platforms risk rejection or failure. The IDB, in collaboration with the Organization of American States and the University of Oxford, has supported LAC countries in assessing and improving their cybersecurity posture through the Cybersecurity Capacity Maturity Model (CMM). Analysis of the CMM assessments conducted in 2016, 2020, and this new one -2025- reveals that 12 countries showed improvement of 0.5 points or more in at least three dimensions, notably in policy frameworks, risk management, education, and legal structures.

Notably, eight of these countries also saw improvements in their standings in major digital government indices, suggesting a virtuous cycle: as cybersecurity capabilities grow, so does digital confidence and innovation. Countries such as Uruguay, Colombia, Chile, and Costa Rica exemplify this correlation, having worked consistently in national strategies, CSIRTs, skills development, and public-private coordination. This maturity not only enables secure digital services but also fosters resilient economies and robust democracies.

Several critical success factors are necessary to adopt cybersecurity as a true enabler of digital transformation. These include having a clear national strategy and legal framework, dedicated governance structures, trained cybersecurity personnel, investment in both technology and institutional capacity, and intersectoral coordination.

Only 13 countries in the region had a national cybersecurity strategy, and just 9 had plans to protect critical infrastructure as of 2020 (IDB-OAS 2020). This underscores the urgency of mainstreaming cybersecurity into broader public policy agendas. By 2025, modest progress has been observed: 15 countries in Latin America and the Caribbean have reached a maturity level of 3 or higher in the development of a national cybersecurity strategy, while 9 countries have achieved a similar level in the integration of cybersecurity into national crisis and critical infrastructure protection frameworks. These figures reveal a steady but insufficient pace of institutionalization, emphasizing the continued need for stronger alignment between digital transformation and cybersecurity governance.

Equally important is the recognition that digital transformation is a cultural transformation. In this light, cybersecurity must be embedded into the organizational culture of public institutions and private organizations. This requires sustained awareness campaigns, training all levels of staff, and placing cybersecurity as a leadership issue—not just an IT concern. Promoting a culture of information security includes positioning risks and threats at the highest decision-making levels in government and across sectors.

Regional cooperation has been vital to advancing cybersecurity in Latin America and the Caribbean. The CSIRTAméricas network, led by the Organization of American States, connects 52 Computer Security Incident Response Teams (CSIRTs) from 22 countries to facilitate incident response, information sharing, and capacity building (OEA 2025). Complementing this, CARICOM IMPACS has strengthened cybercrime legislation and investigative capabilities in the English-speaking Caribbean, supporting regional threat assessments and law enforcement training. Meanwhile, the LAC4 Cyber Competence Centre, launched in 2023 with EU support, promotes policy alignment, institutional strengthening, and joint training on cyber resilience. Other key initiatives include the Cyber Alliance for Mutual Progress (CAMP), led by Korea Internet & Security Agency (KISA), which fosters international cooperation and technical exchanges to enhance global cyber resilience (KISA 2025); the Ciberlac network, an academic cybersecurity excellence network supported by the Inter-American Development Bank, which strengthens collaboration among regional cybersecurity experts and institutions to exchange practices and knowledge (Ciberlac 2025); and RedGealc, the Latin American e-Government Network, which incorporates cybersecurity as a cross-cutting axis in digital government cooperation, advancing standards, training, and knowledge-sharing among public administrations (RedGealc 2025). These initiatives exemplify the region's growing commitment to collective cybersecurity and coordinated digital defense.

Digital transformation is not optional—it is essential, and it's not possible without Cybersecurity. For Latin America and the Caribbean, it represents an opportunity to redefine public value, bridge inequality, and catalyze sustainable development. However, this transformation must be rooted in trust, inclusion, and resilience. Cybersecurity, far from being an afterthought, is the bedrock upon which digital societies are built. With continued investment, regional cooperation, and strategic vision, LAC can lead the next wave of digital innovation with equity and security at its core.

References

IDB 2021
Vision 2025: Reinvesting in the Americas – A Decade of Opportunities

IDB 2021b
Protecting Digital Health: A Cybersecurity Guide for the Health Sector

IDB 2022
Digital Government Transformation Guide

IDB 2022b
Digital Transformation Strategy for the Infrastructure and Energy Sector 2021–2025

IDB 2024
IDB Group Institutional Strategy 2024–2030

IDB-OAS 2020
Cybersecurity: Risks, Progress, and the Way Forward in Latin America and the Caribbean

KISA 2025
The Cybersecurity Alliance for Mutual Progress (CAMP) was initiated by the Korean government with the purpose of achieving sustainable benefits and serving as a platform where members prepare themselves with collective actions to keep cyberspace safe.

Ciberlac 2025
The Latin America and Caribbean Cybersecurity Excellence Network (Ciberlac Network) is a regional network of universities and research centers in the field of cybersecurity. The Inter-American Development Bank (IDB) serves as the driving and coordinating institution of the Network.

RedGEALC 2025
The e-Government Network for Latin America and the Caribbean (RedGealc) is an initiative that seeks to promote cooperation and the exchange of experiences among the countries of the region in the field of e-government, supported by the OAS and the IDB.

OECD 2023
Open Government Data Report: Enhancing Digital Government through Open Data

UN 2024
E-Government Survey 2024: Governing in the Digital Era for Sustainable Development

WEF 2024
Network Readiness Index 2024

Oxford 2021
Cybersecurity Capacity Maturity Model for Nations (CMM), Version 2.0

OEA 2025
CSIRTAméricas Network

Cybersecurity Capacity Maturity Model: 2021 Edition | What has changed?

An Overview of the Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition and Key Improvements over Previous Versions

The Cybersecurity Capacity Maturity Model for Nations (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)[22].

The five stages are defined 34 as follows[23] (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 may be an absence of observable evidence at this Stage;

Formative

Some features of the Aspect have begun to grow and be formulated, but may be ad hoc, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated;

Established

The Indicators of the Aspect are in place, and evidence shows that they are working. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the Aspect. But the Aspect is functional and defined;

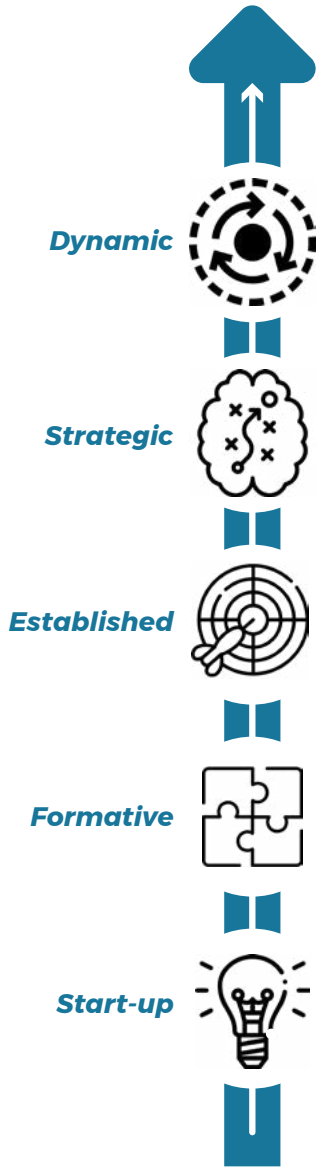
Strategic

Choices have been made about which parts of the Aspect are important, and which are less important for the particular organisation or nation. The strategic Stage reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances; and

Dynamic

At this Stage, there are clear mechanisms in place to alter national strategy depending on the prevailing circumstances, such as the technology of the threat environment, global conflict, or a significant change in one area of concern (e.g. cybercrime or privacy). There is also evidence of global leadership on cybersecurity issues. Key sectors, at least, have devised methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this Stage.

Figure 1 [24]



In 2019, the Global Cyber Security Capacity Centre (GCSCC) initiated a collaborative effort to review and update the CMM. The objective was to integrate the latest insights from the cybersecurity capacity-building community. Drawing from lessons learned in CMM deployments, the GCSCC developed change proposals and conducted consultations—both online and offline—with experts to validate findings and discuss proposed updates. Participants in these consultations included the GCSCC Expert Advisory Panel, GCSCC partners, and a broad range of experts from academia, international and regional organizations, government, private sector, and civil society. This collaborative effort allowed the GCSCC to pinpoint key areas for enhancement, ensuring the CMM's relevance in a rapidly evolving cybersecurity landscape. The updated CMM edition was launched in March 2021. 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) Cybersecurity Culture and Society; (iii) Building Cybersecurity Knowledge and Capabilities; (iv) Legal and Regulatory Frameworks; and (v) Standards, 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. This section defines each dimension and explains the main changes implied with the contributions of this new version of the CMM.[1]

Dimension One: Cybersecurity Policy and Strategy

This dimension explores the country's capacity to develop and deliver cybersecurity strategy, and to enhance its cybersecurity resilience by improving its incident response, cyber defence and critical infrastructure (CI) protection capacities. This Dimension considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.[25]

One of the major changes within Dimension 1 was merging Factor D1.4 National Crisis Management into Factor 1.2 Incident Response and Crisis Management and splitting Factor D1.6 Communications Redundancy and merging relevant parts into Factor D1.2 and other parts into Dimension 5, Factor D5.4 Communications and Internet Infrastructure Resilience.

[1]. A detailed backward conversion between the 2016 and 2021 editions of the CMM can be found at
https://gcscc.ox.ac.uk/sites/default/files/gcscc/documents/media/mapping_changes_of_the_cmm_from_versions_2016-2021.pdf?time=1642156160491

In Factor D1.1 National Cybersecurity Strategy, the Aspect D1.1.2 Organization was renamed Aspect D1.1.3 Implementation and Review to evaluate the effectiveness of the implementation of the strategy. There was a consensus to emphasize "governance" and "implementation" and to clarify that this aspect focuses on decision-making and not just "project management". Indicators were added to determine the inclusivity of the process (e.g. engagement of other stakeholders) in the development, implementation, and review of the strategy.

Also in Factor D1.1 National Cybersecurity Strategy, a new Aspect D1.1.4 International Engagement was added that explores the country's ability to participate in the international debate according to its needs. It assesses: 1) the country's contribution to the international cybersecurity norm development, 2) the country's awareness of the existence of international discussions on cybersecurity policy and related issues, 3) the establishment of international or regional standards around cybersecurity and/or data protection, and 4) how cyber is treated within regional defense alliances.

Following the merger of Factor D1.4 National Crisis Management into Factor D1.2 Incident Response, the name was changed to Factor D1.2 Incident Response and Crisis Management. Furthermore, several aspects within Factor D1.2 were merged to create a more focused view on this factor. For example, Aspect D1.2.4 Mode of Operation and Aspect D1.2.3 Coordination were merged into Aspect D1.2.2 Organization, and the new Aspect D1.2.3 Integration of Cybersecurity into National Crisis Management that identifies the extent to which the national crisis management community is equipped to deal with the unique challenges that a major cyberincident can entail. Indicators were added to assess the way cyberincident response authorities support national level crisis management and how information is shared between the relevant authorities. The previous version could be misinterpreted as assessing crisis management more generally (which is beyond the scope of the CMM), as opposed to the extent to which national crisis management procedures were fit to deal with a range of cyberthreats. In Factor D1.3 Critical Infrastructure Protection, the names of two aspects were changed: Aspect D1.3.2 Organization to Regulatory Requirements and Aspect D1.3.3 Risk Management and Response to Operational Practice. With regards to Aspect D1.3.2 Regulatory Requirements, the new version of the CMM places its focus on the relationship between government and Critical National Infrastructure (CNI) operators. Indicators were added to assess what is expected of CNI operators by regulation and to make sure that the basic regulatory requirements are met, and that cyberequirements are clear to everyone. In t Aspect D1.3.3 Operational Practice, indicators were added to examine proactive information sharing and the extent to which CNI operators were participants in national level incident response planning and exercising.

There was consensus that a strong defense and national security dimension is essential. However, there was also a risk of confusion, since the term "cyber defense" can be interpreted as referring to operational cybersecurity activities within organizations rather than to the broader efforts, needs, and contributions of the armed forces. Therefore, the name of Factor D1.5 "Cyber Defense" was changed to Factor D1.4 "Cybersecurity in Defense and National Security." The addition of "National Security" reflects the wider scope of defense efforts and the purposes they serve. For example, the national security and defense community may include intelligence agencies and, in some cases, specialized law enforcement units, as well as international defense and security alliances.

It was agreed to divide this factor into aspects that distinguish military cybersecurity capabilities from civilian functions and coordination. Aspect D1.5.2 "Organization" was renamed Aspect D1.4.2 "Defense Force Cybersecurity Capability," and its indicators were revised to assess how cyberoperations units are structured and whether the country has cybercapabilities within its defense and national security community.

Similarly, Aspect D1.5.3 "Coordination" was renamed Aspect D1.4.3 "Civil Defense Coordination," with new indicators added to examine whether the country provides defense cybercapabilities to the broader ecosystem beyond critical defense infrastructure, and to what extent defense strategies and capabilities rely on other actors within that ecosystem.

Dimension Two:
Cybersecurity Culture and Society

This Dimension reviews important elements of a responsible cybersecurity culture such as the understanding of cyberelated risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this Dimension explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this Dimension reviews the role of media and social media in shaping cybersecurity values, attitudes and behavior.[26]

Through expert consultations regarding, in Factor D2.1 Cybersecurity Mind-Set, it was suggested the indicators needed revision as well as clarification of the mind-set to refer to the perceptions of stakeholders from the government, private sector and users. There was an agreement to consider reducing the redundancy of the three aspects (government, private sector, users) and not using the word "mind-set" during the review, but rather basing the presence of a mind-set on indicators of the traits and attributes that characterise different cybersecurity mind-sets. Therefore, the titles of the three aspects were revised to address questions as to whether the users are aware of cybersecurity good practices, and to what extent the actors make cybersecurity a priority, and the level of awareness of cybersecurity of the actors. Accordingly, the new aspects focus on attributes instead of actors and were renamed to Aspect D2.1.1 Awareness of Risks, Aspect D2.1.2 *Priority of Security, and Aspect D2.1.3 Practices.*

One of the major changes within this dimension concerned Factor D2.2, which was changed to Trust and Confidence in Online Services. Two new aspects were added, one Aspect D2.2.1 *Digital Literacy and Skills* to measure s whether Internet users critically assess what they see or receive online. The other new Aspect D2.2.3 Disinformation examines whether the government, civil society, non-government actors have the tools and resources to address online disinformation. There was support to update the Factor D2.5 Media and Social Media terminology to reduce redundancy and to be more encompassing, leading it to be renamed as Factor D2.5 *Media and Online Platforms*.

Dimension Three: Building Cybersecurity Knowledge and Capabilities

This Dimension reviews the availability, quality and uptake of programs for various groups of stakeholders, including the government, private sector and the population as a whole, and relate to cybersecurity awareness-raising programs, formal cybersecurity educational programs, and professional training programs[27].

There was a consensus for a new name of the dimension to change the name of this dimension from Cybersecurity Education, Training, and Skills to Building Cybersecurity Knowledge and Capabilities. The new title of this dimension reflects both the cases where people a) need to build/enhance their knowledge about the topic and b) build specific capabilities, meaning that they apply their knowledge and build specific skills, covering the practical aspects. The name of the dimension reflects the ability to deliver that knowledge and convert it to use. There was also an agreement to ensure that this dimension includes some provision on how lessons learned are fed back into the design and delivery of awareness, education, and training programs. This was addressed by adding indicators that examine the availability/existence of some systems of metrics under each factor.

The title of Factor D3.1 Awareness Raising was changed to Building Cybersecurity Awareness. There was a consensus to support the new factor name as it aligns with the new dimension name. Furthermore, there was consensus that in the process of building cybersecurity awareness, the relevant players need to be identified more explicitly. Therefore, three new aspects were added, Aspect D3.1.1 Initiatives by Government, Aspect D3.1.2 Initiatives by Private Sector, and Aspect D3.1.2 Initiatives by Civil Society.

A substantial change was adding the new Factor D3.4 Cybersecurity Research and Innovation to highlight the importance of government investing in this area. This title was chosen because this area involves not only universities but also the private sector. Within this new factor thenew Aspect D3.4.1 Research and Development was added to examine the existence of a research and innovation culture in the country related to a national list of current and completed projects, financial support, incentives and usable research outputs.

Dimension Four:
Legal and Regulatory Frameworks

This Dimension examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this Dimension observes issues such as formal and informal co-operation frameworks to combat cybercrime.[28]

The name of Aspect D4.1.1 Legislative Frameworks for ICT Security was changed to Aspect D4.1.2 Legal and Regulatory Requirements for Cybersecurity to reflect the important role that regulation plays in incentivizing good cybersecurity practice across the economy. There was a consensus about building human rights assessment of cybersecurity measures much more explicitly into the CMM under this dimension. Therefore, the new Aspect D4.1.4 Human Rights Impact Assessment was included with indicators assessing the extent to which human rights impact assessments of substantive and procedural cybercrime legislation and cybersecurity regulations are conducted and independently verified. That leaves the broader question of whether a national cybersecurity strategy explicitly addresses broader policy issues such as privacy, freedom of speech and other human rights online – there were specific indicators relating to this in D4 of the previous version, but these have now been incorporated into D1 because they really relate tothe scope of a nation's cybersecurity strategy.

The previous version of D4 includes various aspects relating to legislations on data protection, child protection, consumer protection and intellectual property protection. It was noted during the consultation that all these issues go well beyond the scope of cybersecurity. A new Factor D4.2 Related Legislative Frameworks has been created to reflect this, with aspects that explore the extent to which these related frameworks take proper account of the challenges associated with the online environment.

The title of Factor D4.2 Criminal Justice System was changed to Legal and Regulatory Capability and Capacity to reflect the important role played by regulatory authorities and their efforts to oversee regulatory compliance on cybersecurity by the organizations in the country. The new Aspect D4.3.4 Regulatory Bodies was created to examine the existence of cross-sector regulatory bodies and their capacity to oversee compliance with specific cybersecurity regulations.

In Factor D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime (now Factor D4.4) there was an agreement to make clear that the analysis under this factor focuses on interactions and relationships between actors of the criminal justice system of different jurisdictions, and between actors of the criminal justice system and actors outside of the criminal justice system, therefore it needs to specify the purpose of cooperation (beyondblanket phrase "combating cybercrime"). The distinction between formal and informal cooperation remains but is no longer reflected in the structure of the aspects. There was a consensus to welcome the addition of public-private cooperation/partnerships; therefore, the new Aspect D4.4.1 Law Enforcement Co-operation with Private Sector was created. Furthermore, as agreed, two new Aspects D4.4.2 Cooperation with Foreign Law Enforcement Counterparts and D4.4.3 Government-Criminal Justice Sector Collaboration were added.

Dimension Five:
Standards and Technologies

This Dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organizations and national infrastructure. The Dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.[29]

There was a consensus to remove the word "Organizations" from the title and only keep Standards and Technologies.

In Factor D5.1 Adherence to Standards, aspect D5.1.3 Standards in Software Development was renamed Standards for Provision of Products and Services that would relate to the inclusion and activation of cybersecurity; in other words, assessing the presence of baseline levels of security provision that providers of certain types of products or services are required to make. Therefore, indicators were revised to address the use of standards and good practices by local suppliers of goods and services, including software, hardware, managed services, and cloud services.

A substantial change was merging factor D5.5 Cryptographic Controls into Factor D5.2 Security Controls as a new aspect. Within the new Aspect D5.2.2 Cryptographic Controls there was an agreement to add to the Strategic level indicators whether the country has considered implementing digital-identity management (e.g., including PKI as a cryptographic protection of national digital identities).

Within factor D5.4 Communications and Internet Infrastructure Resilience, the new Aspect D5.4.2 Monitoring and Response was added. Indicators were added to examine whether mechanisms are in place to conduct risk assessments and monitor network resilience in both public and private sectors.

In factor D5.5 Cybersecurity Marketplace, two new aspects were introduced: aspect D5.5.2 Cybersecurity Services and Expertise and Aspect D5.5.3 Security Implications of Outsourcing. There was support to add a new aspect on cybersecurity services and expertise to examine the availability of cybersecurity consultancy services for private and public organizations. Similarly, the new aspect on security implications of outsourcing was added to determine whether risk assessments of other countries' software and cloud services are conducted to mitigate the risks of outsourcing IT to a third party or cloud services. As well as these structural changes, there is a significant change in emphasis on what constitutes a good cybersecurity posture in the marketplace: where it used to demand that a nation develop native offerings in order to attain the higher maturity stages, it now recognizes that becoming a "smart customer" of overseas products can be an equally appropriate solution (especially for small nations).

In factor D5.6, Responsible Disclosure, there was support that decomposition of the sole aspect Responsible Disclosure was needed to ensure that indicators address whether the actions are sufficiently responsible, whether information is disclosed appropriately, and if enough time is left for vendors to patch. The titles of the new aspects are D5.6.1 Sharing Vulnerability Information and D5.6.2 Policies, Processes, and Legislation for Responsible Disclosure of Security Flaws. The latter investigates whether mechanisms for responsible disclosure are in place and the right legal protections for those disclosing security flaws responsibly.

The following table details the factors that compose the dimensions:

Dimension 1: Cybersecurity Policy and Strategy

D 1.1: National Cybersecurity Strategy
D 1.2: Incident Response and Crisis Management
D 1.3: Critical Infrastructure (CI) Protection
D 1.4: Cybersecurity in Defense and National Security

Dimension 2: Cybersecurity Culture and Society

D 2.1: Cybersecurity Mindset
D 2.2: Trust and Confidence in Online Services
D 2.3: User Understanding of Personal Information Protection Online
D 2.4: Reporting Mechanisms
D 2.5: Media and Online Platforms

Dimension 3: Building Cybersecurity Knowledge and Capabilities

D 3.1: Building Cybersecurity Awareness
D 3.2: Cybersecurity Education
D 3.3: Cybersecurity Professional Training
D 3.4: Cybersecurity Research and Innovation

Dimension 4: Legal and Regulatory Frameworks

D 4.1: Legal and Regulatory Provisions
D 4.2: Related Legislative Frameworks
D 4.3: Legal and Regulatory Capability and Capacity
D 4.4: Formal and Informal Co-operation Frameworks to Combat Cybercrime

Dimension 5: Standards and Technologies

D 5.1: Adherence to Standards
D 5.2: Security Controls
D 5.3: Software Quality
D 5.4: Communications and Internet Infrastructure Resilience
D 5.5: Cybersecurity Marketplace
D 5.6: Responsible Disclosure

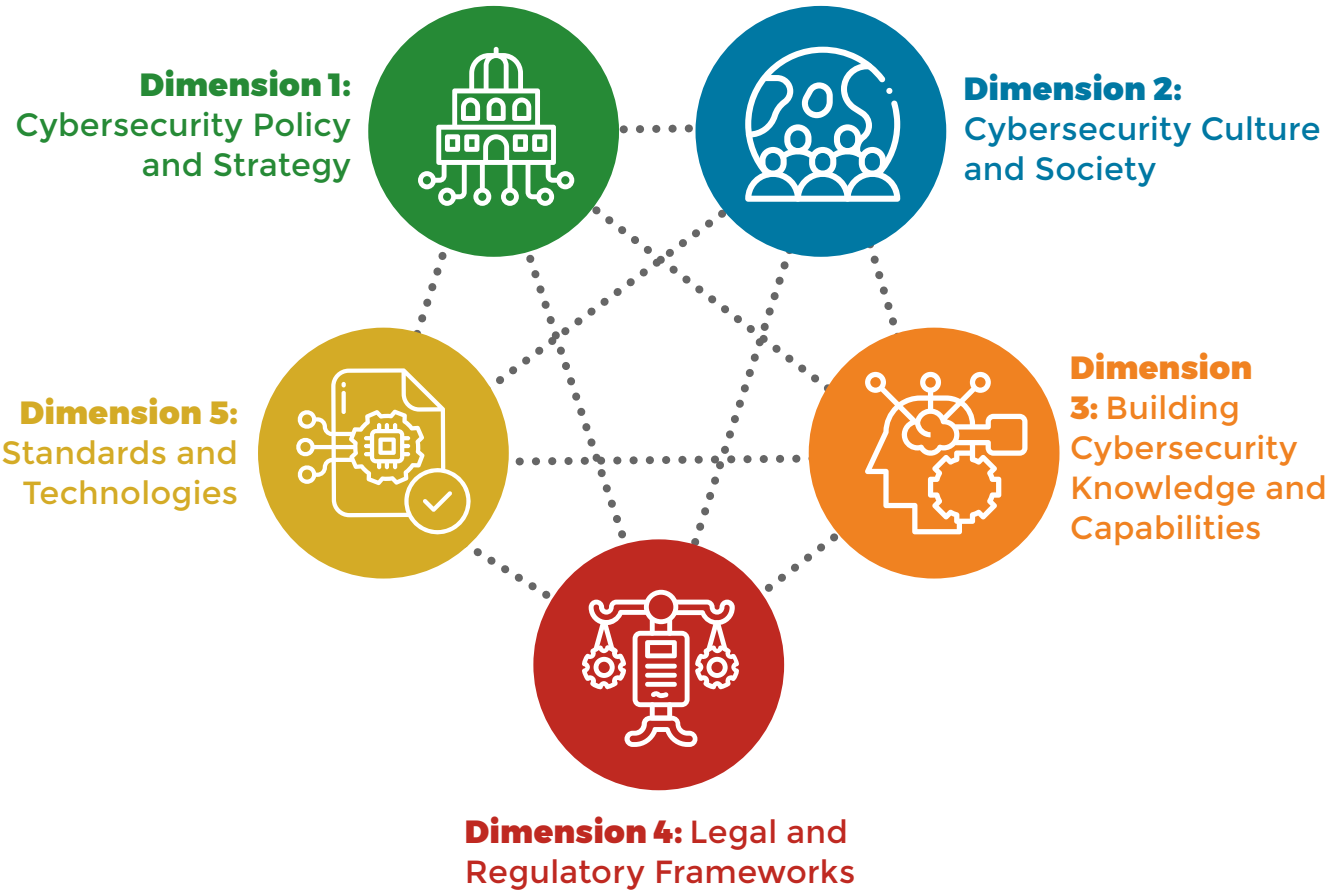
The primary data used in this report was collected through an online instrument distributed to all Member States of the Organization of American States (OAS). Following the initial data collection, the results were cross-referenced with desktop research and validated through consultations with Member States.

Using the 2021 Cybersecurity Capacity Maturity Model for Nations (CMM) [30] as a baseline, this report presents the results of the cybersecurity capacity review for Latin America and the Caribbean based on data validated as of May 2025. Each country profile concludes with a summary table outlining the five dimensions and their corresponding maturity levels as assessed in the 2016, 2020, and 2025 reports.

Maturity levels are visually represented by the number of highlighted boxes for each indicator: one box corresponds to the start-up stage, two to formative, three to established, four to strategic, and five to dynamic. Indicators marked N/A indicate that the indicator was not applicable during that year's assessment.

The 2016 and 2020 values were updated to align with the Revised Edition of the Cybersecurity Capacity Maturity Model for Nations (CMM). All assessments from the 2016 and 2020 publications remain unchanged, except for the incorporation of newly added indicators.

Figure 2[31]



Trend Analysis from 2020 to 2025

This report of the Organization of American States (OAS) documents the continued advancement of cybersecurity capacity across the Latin American and Caribbean region.

The OAS has examined capacity-building efforts to inform and raise awareness about cybersecurity capacities in Latin America and the Caribbean. The present report is based on the third wave of unique data collection on national cybersecurity capacities among its member states. As with the previous two reports in 2016 and 2020, the 2025 data is anchored in Oxford's Cybersecurity Capacity Maturity Model for Nations (CMM)[32] developed in collaboration with the OAS. This framework allows for benchmarking the maturity level of national cybersecurity capacities and enables comparisons across countries and over time.

The CMM adopts a holistic approach to cybersecurity capacity, structured around five interlinked dimensions previously described. Overall, the 2021 edition of the CMM describes maturity indicators for 62 cybersecurity aspects clustered into 23 factors across 5 dimensions, including new cybersecurity aspects that provide useful insights on how countries are adapting to a changing landscape and emerging challenges.[33]

When comparing the average results of the 2020 and 2025 studies, the main trend is a general increase in the perceived maturity of national cybersecurity capacities across all CMM dimensions (see Figure 1). Additionally, the 2025 results show a more balanced maturity across all factors compared to the previous report, indicating that overall growth has been accompanied by a reduction in maturity gaps among various capacities.

The factor with the highest growth in the region is D5.6 Responsible Disclosure, which in 2020 was among the least mature factors for most member states. This case highlights efforts to establish responsible frameworks for receiving and disseminating vulnerability information across sectors. D2.4 Reporting Mechanisms, which reflects national efforts to develop channels for reporting internet-related crime, shows the next highest growth, followed by D1.4 Cybersecurity in Defense and National Security and D4.4 Formal and Informal Cooperation Frameworks to Combat Cybercrime.

Despite the reduction of maturity gaps, several factors continue to show lower maturity in 2025, including D5.3 Software Quality, D1.3 Critical Infrastructure Protection, and D5.5 Cybersecurity Marketplace. As noted earlier, the new factor D3.4 Cybersecurity Research and Innovation is perceived as the least mature in the region.

On average, member states continue to view D4.1 Legal and Regulatory Provisions and D4.2 Related Legislative Frameworks as the most mature cybersecurity factors. Several other factors have experienced significant growth and are beginning to approach similar maturity levels, including D1.1 National Cybersecurity Strategy, D3.1 Building Cybersecurity Awareness, D1.2 Incident Response and Crisis Management, and D2.4 Reporting Mechanisms.

The first dimension introduces a new aspect on engagement in international discussions on cybersecurity policy. On average, this new aspect is perceived as one of the strongest within the factor D1.1 National Cybersecurity Strategy.

Factor D2.2 Trust and Confidence in Online Services in dimension 2 includes two new aspects assessing how nations address online disinformation and how digital literacy enables users to critically evaluate online content. The 2025 results indicate that the maturity of both aspects is still developing in the region, with disinformation at a particularly early stage.

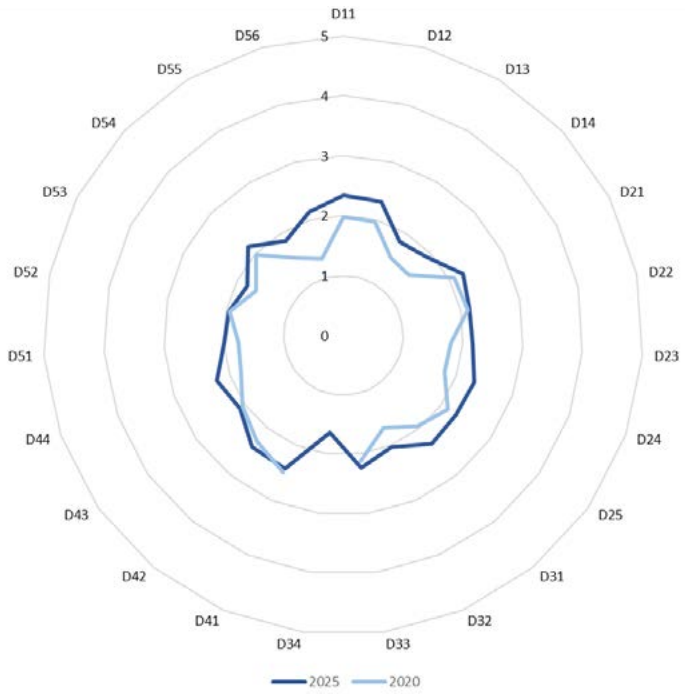
Dimension 3 includes a new aspect that forms the new factor D3.4 Cybersecurity Research and Innovation, the least mature factor on average, as investments in cybersecurity research remain nascent in many countries.

Dimension 4 introduces two new aspects: one examining human rights impact assessments of cybercrime legislation (within factor D4.1 Legal and Regulatory Provisions) and another assessing cross-sector regulatory bodies overseeing compliance with specific cybersecurity regulations (within factor D4.3 Legal and Regulatory Capability and Capacity). Both aspects are perceived as less mature than others within their respective factors.

Finally, dimension 5 includes two new aspects within factor D5.5 Cybersecurity Marketplace: the availability of cybersecurity services and expertise, and practices related to assessing risks tied to outsourcing IT to third parties. Although the region is still developing maturity in these areas, the least mature aspect in this factor continues to be cyber insurance.

Overall, these trends illustrate a solid increase in cybersecurity capacities across the Latin American and Caribbean region. The development of stronger foundations enhances overall cybersecurity, enabling trust among nations and organizations, interoperability of services, and secure social interactions within and beyond the region.

Figure 3. Average maturity stage at the Factor level in 2020 and 2025 for the 30 Member States participating in this report. The scale 1 to 5 represents the five increasing maturity stages in the CMM (from start-up to dynamic). The name of each Factor has been substituted by its numerical code in the CMM.



Footnotes

1 https://gcscc.ox.ac.uk/national-ai-cybersecurity-readiness-metric

2 Burges, "Wired Conti's Attack Against Costa Rica Sparks a New Ransomware Era", Wired. https://www.wired.com/story/costa-rica-ransomware-conti/

3 Borgeaud, "Smartphone adoption rate in Latin America in 2023 versus 2030", Statista

4 Newmeyer, "The Challenge of Cybersecurity for the Caribbean."

5 Norton, Cybercrime and Cyber-Victimization: A Caribbean Perspective. In; The Palgrave Handbook of Caribbean Criminology.

6 Haughton, "Jamaica's Cybercrime and Cyber-Security Policies, laws, and strategies". In; Routledge Companion to Global Cyber-Security Strategy

Kerttunen and Tikk, "National Cyber Security Strategies: Commitment to Development."

7 This is an expanded definition based on UN Women, "Concepts and definitions", https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm ; UNICEF Regional Office for South Asia, Gender Equality: Glossary of Terms and Concepts, November 2017,

8 This is an expanded definition based on UN Women Training Centre, "Gender Equality", Gender Equality Glossary, https://trainingcentre.unwomen.org/mod/glossary/showentry.php?eid=54

9 See Lisa Sharland, Netta Goussac, Emilia Currey, Genevieve Feely, Sarah O'Connor "System Update: Towards a Women, Peace and Cybersecurity Agenda", UNIDIR, Geneva, September 2021, available at https://unidir.org/publication/system-update-towards-a-women-peace-and-cybersecurity-agenda/

10 See Katharine Millar, James Shires and Tatiana Tropina "Gender Approaches to Cybersecurity", UNIDIR, Geneva, January 2021, available at https://unidir.org/publication/gender-approaches-to-cybersecurity/

11 International Telecommunication Union, "Facts and Figures 2023: The Gender Digital Divide," October 2023, https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-the-gender-digital-divide/

12 ISC)², "Cybersecurity Workforce Study 2023", October 2023, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

13 ISC)², "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce", 2018, https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/Innovation-Through-Inclusion-Report.pdf

14 See, for example, the course "Our Networks, Our Security" to enhance digital security from a gender perspective; the initiative "SheSecures", which comprises national cybersecurity exercises for women to enhance their technical skills; the "CyberTalents Initiative" and the recently launched "Women in Cybersecurity Empowerment Network", which promote and enhance women participation in cybersecurity addressing the existing gender digital divide. For more information, see https://shesecures.hackrocks.com/info/about; https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-038/24.

15 OAS/CICTE, List of Consolidated Cooperation and Confidence-building Measures in Cyberspace, 2024.

16 Costa Rica, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, Estrategia Nacional de Ciberseguridad 2023-2027, available at: https://www.micitt.go.cr/sites/default/files/2023-06/Estrategia-Nacional-de-Ciberseguridad-MICITT-2023-2027.pdf. Comité Interministerial de Ciberseguridad, Gobierno de Chile, Política Nacional de Ciberseguridad 2023-2028, 2023, pp. 11, 18.

17 Gobierno de la República de Guatemala, Estrategia Nacional de Seguridad Cibernética, 2018, p. 31, fn. 14. Ministerio de Telecomunicaciones y de la Sociedad de la Información de Ecuador, Estrategia Nacional de Ciberseguridad del Ecuador, 2022, p. 35

18 República Argentina, Poder Ejecutivo Nacional, Estrategia Nacional de Ciberseguridad de la República Argentina, 14 de julio de 2023, pp. 4 and 7.

19 Uruguay Presidencia, Agenda Uruguay Digital 2025, 2020, pp. 3, 22.

20 Gobierno de la Republica Dominicana, Agenda Digital 2030, 2022.

21 See, for example, Saint Vincent and the Grenadines National ICT Strategy (2010); Belize ICT National Strategy (2011); National ICT Strategic Plan of Saint Kitts and Nevis (2006). See similarly, The Government of Suriname National Digital Strategy 2023-2030 (2023).

22 https://publications.iadb.org/en/publications/english/viewer/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

23 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

24 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

25 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

26 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

27 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

28 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf,

29 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

30 A more detailed explanation of the 2021 CMM can be found here: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

31 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

32 https://gcscc.ox.ac.uk/cmm-2021-edition

33 https://gcscc.ox.ac.uk/development-and-evolution-of-the-cmm

---

COUNTRY REPORTS

Antigua and Barbuda

Antigua and Barbuda has made some progress its international collaboration initiatives and in training its personnel in cybersecurity. Although the country does not yet have a National Cybersecurity Strategy, it has appointed a Cybersecurity Director and as a nation actively participates in international forums such as FIRST[34] and has collaborated in regional cybersecurity exercises, such as "CyberCrabs 2022." This exercise, organized by EU CyberNet and LAC4 in cooperation with CARICOM IMPACTS, the OAS, and the Dominican Republic's CNCS, aimed to test crisis management procedures and enhance information sharing among Caribbean countries. Additionally, Antigua and Barbuda's military team participated in the "Tradewinds 2022" cyber operations exercise, reflecting the country's commitment to integrating cybersecurity practices at both military and governmental levels.[35]

Recently, Antigua and Barbuda joined LAC4, allowing the country to benefit from the European Union's technical support to strengthen its cybersecurity capabilities.[36] Through this collaboration, the government is in the process of re-establishing its Computer Emergency Response Team (CERT), which previously existed, aiming to enhance its response to incidents and cyber threats.

In line with regional cybersecurity initiatives, Antigua and Barbuda is part of the CARICOM Cyber Resilience Strategy 2030 Project, launched by the CARICOM Secretariat and USAID. This strategy aims to strengthen cybersecurity capacity across CARICOM states, fostering collaboration and resilience at both individual and collective levels. The project, directed by a Steering Committee of CARICOM and regional experts, will provide a framework to enhance information sharing, address legislative gaps, and promote a robust cybersecurity workforce to safeguard critical infrastructure and digital assets across the Caribbean.[37]

The country has shown increasing interest in promoting a cybersecurity culture through participation in awareness initiatives and training in collaboration with other Caribbean nations and international entities. Recently, Antigua and Barbuda was one of the CARICOM countries to complete an advanced course on incident response and threat hunting, organized by LAC4 in cooperation with EU CyberNet and CARICOM IMPACT.[38] This training, designed to address the unique challenges of the Caribbean region and strengthen endpoint security, prepared the country for major events like the 2024 T20 Cricket World Cup, where heightened cybersecurity needs were anticipated.

Antigua and Barbuda has increased its collaboration with the private sector in cybersecurity and has signed Memoranda of Understanding (MoUs) with India to share and implement innovative technologies. Through "India Stack," a set of APIs designed to promote digital inclusion, the country aims to strengthen its digital security capabilities and create new employment opportunities in the tech sector. Furthermore[39], the government has promoted digitalization initiatives in rural areas to bridge the digital divide, facilitating access to services and technology in key sectors such as agriculture.[40] In terms of formal training opportunities in cybersecurity, while there are no dedicated cybersecurity degrees, the Antigua and Barbuda International Institute of Technology provides degree programs in computer science and information technology.[41]

Antigua and Barbuda has a legislative framework for protection against cybercrimes and data regulation, as established by the 2013 Electronic Crimes Act.[42] This legislation addresses unauthorized access, interference, electronic fraud, cyber harassment, misuse of encryption, and child pornography, among other areas. The country also has the Data Protection Act[43] in force since 2013, which safeguards private information and establishes an independent supervisory authority, the Information Commissioner. These laws provide a regulatory foundation to address both cybercrimes and data protection, though a specific cybercrime strategy remains pending.

Antigua and Barbuda continues to advance its E-Government strategy, with digitalization efforts that include the regulation of electronic signatures under the 2013 Electronic Transactions Act[44] and online renewal of the driver's license. Additionally, the country has signed an agreement with the Latin American and Caribbean Development Bank, CAF, enabling it to access technical and financial resources to strengthen its digital infrastructure.[45] With this expansion of services, Antigua and Barbuda will be able to implement secure and efficient technology platforms for public administration, improving digital service delivery for its citizens.

CYBERSECURITY CULTURE AND SOCIETY

Antigua and Barbuda

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Antigua and Barbuda

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Antigua and Barbuda

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Antigua and Barbuda

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 | **2025**

Cryptographic Controls
2016 | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025**

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Argentina

Argentina has demonstrated a robust commitment to cybersecurity by regularly updating its National Cybersecurity Strategy (NCS), which reflects the country's evolving political, economic, social, and technological landscape. The NCS undergoes systematic review and integrates input from various stakeholders, including government entities, private sector representatives, academia, and civil society. The National Cybersecurity Committee,[46] consisting of the Ministries of Foreign Affairs, International Trade and Worship, Defense, National Security, Justice, and Human Rights, alongside the Secretariat of Public Innovation, oversees this strategy. The most recent updates were subject to public consultation, as per Resolution No. 1/2023,[47] which lays the foundations for the Second National Cybersecurity Strategy.[48]

Argentina's government is dedicated to advancing E-Government initiatives, digital service delivery, and cybersecurity standards. Recent efforts include the Digital Agenda[49], a government strategy aimed at enhancing cybersecurity capabilities within digital services, particularly through multi-factor authentication and secure digital identity[50] verification for citizens.

In addition, Argentina approved the "Cybersecurity for Critical Infrastructures" program in 2023. This USD 30M investment program develops protection, detection and incident response capabilities in the Cabinet of Ministers, as well as developing projects to strengthen the country's cybersecurity workforce. The establishment of twelve national Computer Security Incident Response Teams (CSIRTs)[51] further supports Argentina's cybersecurity infrastructure, providing incident response services across several provinces, including Buenos Aires and Córdoba. Argentina is also an active member of CSIRT Americas, FIRST[52], and other international networks, facilitating knowledge-sharing and collaborative response to regional cyber threats. Argentina also has a systematic process for reporting and managing cybersecurity incidents.[53]

To promote cybersecurity awareness across society, Argentina has implemented a series of public awareness and training programs aimed at fostering a safer digital environment. Argentina's participation in key international cybersecurity forums, such as the UN Open-ended Working Group on ICT Security[54] and the CICTE Cybersecurity Working Group at the OAS, Cybersecurity workgroup at RedGealc, Global Forum of Cyber Expertise, among others showcases its commitment to building a cooperative and secure global digital landscape. These efforts include contributions to the EU-LAC Digital Alliance[55] and the Mercosur Digital Agenda[56] , which support international dialogue and alignment on best practices. Nationally, Argentina runs public campaigns, seminars, and workshops on digital safety and security. For instance, the Buenos Aires CSIRT (BA-CSIRT)[57] leads initiatives to educate the public on cybersecurity best practices.

Argentina prioritizes cybersecurity capacity building through partnerships between public and private entities. A wide array of educational institutions, such as the University of La Plata, University of Buenos Aires, the National Institute of Public Administration and the Center for High Technology Training in Latin America and the Caribbean[58] among others, provide specialized degrees and certifications in cybersecurity. These institutions offer undergraduate and graduate programs that equip students with essential cybersecurity skills, ensuring a steady influx of qualified professionals. Argentina also promotes cybersecurity competitions[59] and professional development initiatives[60], targeting both students and active professionals to enhance digital literacy and technical proficiency.

Argentina has developed a comprehensive legal framework addressing cybercrime, data protection, and critical infrastructure security. Law No. 25.326 on Personal Data Protection[61] and Law No. 26.388 on Cybercrime[62] form the backbone of Argentina's approach to protecting personal data and preventing cybercrime. The country has ratified the Budapest Convention on Cybercrime (Law No. 27.411)[63], ensuring alignment with international standards for prosecuting cybercriminal activities. Additionally, Law No. 27.590[64], which establishes a national program to prevent grooming and cyberbullying, highlights Argentina's dedication to child online safety.

In 2022 the Ministry of Security created the "Program for the Strengthening of Cybersecurity and Cybercrime (FORCIC)" with the aim of coordinating, assisting and providing advice on digital infrastructure security techniques and investigation techniques in cybercrime and crimes involving the presence and/or use of technology.

Argentina's regulatory framework also mandates incident reporting for critical infrastructure operators, as seen in Administrative Decision DA 641/2021[65], which establishes minimum information security standards for national public sector agencies.

Furthermore, Argentina has developed national cybersecurity technologies in alignment with international coding and security guidelines, positioning itself as a growing exporter of cybersecurity solutions across Latin America.

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Argentina

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Argentina

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Bahamas, The Commonwealth of

The Bahamas has made significant progress and formalized its National Cybersecurity Strategy (NCS)[66], outlining a comprehensive approach to strengthening cybersecurity across public and private sectors in response to increasing digital dependency. The strategy envisions The Bahamas as a "secure and trusted digital society," supporting economic growth, benefiting citizens, and promoting regional and global partnerships. Cybersecurity is now part of the executive agenda, as evidenced by statements from the Minister of Economic Affairs "Cybersecurity plays a pivotal role in The Bahamas' national strategy and is crucial for advancing the nation's utilization of information and communications technology and managing cyber risks — particularly from an economic, but also from a national security perspective"[67]. Central to the NCS are principles that frame cybersecurity as a public concern essential to national security and socioeconomic prosperity, upholding human rights and employing a risk-based approach to manage digital threats. The Bahamas Computer Incident Response Team (CIRT-BS) has a pivotal role in implementing the NCS, coordinating national incident response, monitoring threats, and engaging internationally with organizations such as CSIRT Americas and FIRST[68]. The strategy's objectives focus on cybersecurity governance, protection of critical infrastructure, and high-level coordination among stakeholders.

Since 2020, Bahamas has benefited from technical and financial support through the "Government Digital Transformation to Strengthen Competitiveness" BH-L1045[69] IDB operation. This project has provided over USD 1 million for cybersecurity capacity building to strengthen CIRT-BS and other governmental entities. The Bahamas has participated in regional cybersecurity exercises like "CyberCrabs 2022." This exercise, coordinated by EU CyberNet and LAC4 in collaboration with CARICOM IMPACS, the OAS, and the CNCS of the Dominican Republic, focused on testing crisis management protocols and strengthening information exchange among Caribbean nations.[70]

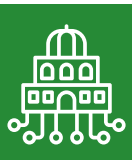
Additionally, The Bahamas contributes to the CARICOM Cyber Resilience Strategy 2030 Project, an initiative launched by the CARICOM Secretariat in cooperation with USAID to strengthen cybersecurity across CARICOM nations. This strategy promotes both national and collective resilience through enhanced collaboration and capacity building. Led by a Steering Committee of CARICOM and regional experts, the project aims to improve information sharing, close regulatory gaps, and build a skilled cybersecurity workforce to protect critical infrastructure and digital assets across the Caribbean[71]. It also participated as host in the international military cybersecurity exercises, at the Tradewinds 2024 (TW24).[72]

The Bahamas has made strides in raising cybersecurity awareness throughout society. The 2022 "Get Safe Online" campaign, which trained ambassadors and introduced the Get Safe Online Bahamas website[73], serves as a central resource for cybersecurity information. Government entities actively support awareness efforts, publishing advisories and hosting forums such as the CIRT-BS-led CIO Forum on topics like endpoint protection and intrusion detection. The private sector, particularly financial institutions, also prioritizes cybersecurity through antivirus, VPNs, and multi-factor authentication measures[74]. Nonetheless, while a culture of cybersecurity is developing, more coordinated public-private initiatives are needed to achieve comprehensive awareness across sectors.

The Bahamas is expanding its cybersecurity education offerings. The University of The Bahamas provides courses in areas such as network and system security, intrusion detection, and auditing[75]. While the country has not yet established a dedicated cybersecurity degree, the government has prioritized the field in its scholarship program to attract more talent. Additionally, the Bahamas Institute of Business Technology offers degrees in network security, and private entities like Tech Edge provide certification courses. However, research and development in cybersecurity remain limited.

Bahamas' regulatory framework includes the Computer Misuse Act[76] and the Data Protection Act,[77] offering a foundation for tackling cybercrime and ensuring data privacy. Although not a formal signatory, The Bahamas aligns its regulations with the Budapest Convention on Cybercrime as part of its ongoing legal reforms. The Royal Bahamas Police Force has a Cybersecurity Unit within its Digital Forensics and Investigation Unit, collaborating with local ISPs under court orders to access data for investigations[78], Nevertheless, further training for legal professionals is necessary to enhance the judicial handling of cybercrime cases.

The Bahamas adheres to international cybersecurity standards, especially in the financial sector, which complies with SWIFT and PCI guidelines. CIRT-BS and the Central Bank also utilize ISO 27001 and the NIST Cybersecurity Framework[79]. Despite the absence of a national cybersecurity standard for procurement, the Department of Information and Communications Technology enforces minimum software security requirements. The country's robust internet infrastructure, overseen by URCA[80], maintains high service standards essential for secure e-commerce and digital transactions. While local cybersecurity expertise is still developing, the government encourages risk assessments and security measures across sectors.



CYBERSECURITY
POLICY AND STRATEGY

Bahamas, The Commonwealth of

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | **2025**
Content
2016 | 2020 | **2025**
Implementation and Review
2016 NA | 2020 NA | **2025**
International Engagement
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | **2025**
Organization
2016 | 2020 | **2025**
Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | **2025**
Coordination
2016 | 2020 | **2025** NA
Mode of Operation
2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | **2025**
Regulatory Requirements
2016 NA | 2020 NA | **2025**
Operational Practice
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA
Risk Management and Response
2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | **2025**
Defense Force Cyber Capability
2016 NA | 2020 NA | **2025**
Civil-Defense Coordination
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA
Coordination
2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Bahamas, The Commonwealth of

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Bahamas, The Commonwealth of

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Bahamas, The Commonwealth of

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Bahamas, The Commonwealth of

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Barbados

Barbados has made important progress in developing a national cybersecurity strategy[81], actively participating in regional initiatives such as the CARICOM Cyber Resilience Strategy 2030 project. This project aims to strengthen cybersecurity capabilities across CARICOM member states by enhancing collaboration and capacity building to protect critical infrastructure and digital assets[82].

Additionally, Barbados has engaged in regional cybersecurity exercises such as the "CyberCrabs 2022" exercise, coordinated by EU CyberNet and LAC4 in collaboration with CARICOM IMPACS and the OAS, focusing on testing cyber crisis management protocols and improving information-sharing among Caribbean nations[83]. The country also collaborated with U.S. cybersecurity experts who conducted network assessments with the Barbados Defence Force (BDF) and the Regional Security System (RSS), underscoring the importance of collaborative cyber defense in response to rising national security threats[84].

The *Technology and Cyber Risk Management Guideline*[85] issued by the Central Bank of Barbados in 2023 further reinforces national cybersecurity by mandating that financial institutions implement comprehensive cyber risk governance. This framework aligns with international standards such as NIST and ISO/IEC 27000, focusing on risk management, system resilience, and strict governance by senior leadershipAlso, the Ministry of Industry, Innovation, Science and Technology, in its role as the leader of the country's digital agenda, has worked with Queen Elizabeth Hospital in activities aimed at improving cybersecurity, including maturity diagnostics, adaptation of response team equipment, among others

The Barbadian government has prioritized cybersecurity training and awareness through initiatives like the Cyber Nations Training Initiative, which has trained hundreds of citizens in skills such as security analysis and incident response, with certifications supported by international institutions. Collaborations with organizations like the Caribbean Israel Center for Cyber Defense and the University of the West Indies (UWI) further support public education on cybersecurity risks. Additionally, national guidelines require financial institutions to provide regular employee training to strengthen organizational cybersecurity culture. UWI has expanded its offerings with cybersecurity-focused courses and a master's degree developed in partnership with the University of Maryland, addressing the region's growing need for skilled professionals to protect digital infrastructure.The Technology and Cyber Risk Management Guideline encourages institutions to engage in continuous skill development for cybersecurity professionals, recommending regular penetration tests and vulnerability assessments as part of ongoing cybersecurity capacity building efforts.

Barbados has made progress in its regulatory framework with the introduction of the Cybercrime Bill 2024, which aims to combat cybercrime, protect legitimate interests in information technology use, and facilitate international cooperation on computer-related crimes. This development follows Barbados' participation in the 2019 Regional Conference on Cybercrime Strategies and Policies in Santo Domingo, where Caribbean leaders discussed elements of a regional cybercrime strategy[86]. Additionally, Barbados maintains laws such as the Computer Misuse Act and a Data Protection Bill, aligning with international standards to secure personal information and cybersecurity.

The Technology and Cyber Risk Management Guideline complements these efforts by establishing clear requirements for incident reporting in financial institutions, including mandatory reporting within four hours of detecting major cyber incidents. This regulatory standard supports rapid response and enhances coordination with national cybersecurity efforts.

Barbados has advanced its E-Government strategy, dating back to 2006, with the vision of empowering citizens through efficient and secure online services. The country has also made substantial progress in adopting advanced technologies, such as blockchain, through digital payment projects that support its digital transformation agenda. In 2024, the Tradewinds military exercise, focused on cybersecurity and co-organized with the U.S. Southern Command and the BDF, reinforces the readiness of Barbados' armed forces and promotes hemispheric cooperation in cybersecurity against emerging threats in the Caribbean[87].

Under the Technology and Cyber Risk Management Guideline, financial institutions are required to adopt advanced security controls, including multi-factor authentication, network segmentation, and real-time monitoring. These measures aim to secure Barbados' financial infrastructure and align it with international best practices, ensuring resilience and security within the broader digital ecosystem.

CYBERSECURITY CULTURE AND SOCIETY

Barbados

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Barbados

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Barbados

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

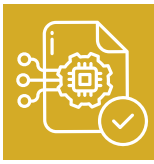
Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA



STANDARDS AND TECHNOLOGIES

Barbados

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Belize

In late 2020, Belize adopted its first National Cybersecurity Strategy for 2020-2023[i], aimed at enhancing the country's overall cybersecurity posture. This strategy identifies three key priority areas: developing a national legal framework to address cybersecurity threats, building capacity for incident response and critical infrastructure protection, implementing measures to support education, awareness, and workforce policy development in cybersecurity. The strategy's development demonstrates a multi-stakeholder approach, involving various government agencies, academia, and the private sector. In 2024, the country began the process of formulating its second National Cybersecurity Strategy with the support of the Organization of American States.

Inter-institutional cybersecurity task forces have been established, led by the Ministry of Home Affairs and New Growth Industries, the Public Utilities Commission (PUC), National Security Council Secretariat (NSCS), and Central Information Technology Office (CITO)[ii]. These task forces comprise stakeholders from both public and private sectors, academia, and civil society groups. The Police Information Technology Unit (PITU) of the Belize Police Department (BPD)[iii] manages investigations of cyber-related crimes and felonies involving electronic evidence. However, Belize currently lacks a national CERT/CIRT (Computer Emergency Response Team).

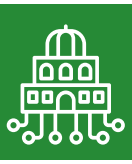
Belize is Member State of CARICOM IMPACS[88] and participant in the LAC4 Initiative[89]. In February 2024, Belize expressed its interest in joining the EU-LAC Digital Alliance during a high-level dialogue on cybersecurity held in Santo Domingo, Dominican Republic. This step indicates Belize's intention to collaborate in international initiatives related to cybersecurity[90].

BPD offers comprehensive cybersecurity awareness content[iv], providing thorough knowledge on the competent use of information technology. These training sessions, available both online and in-classroom, cover topics such as creating strong passwords, software updates, protecting sensitive data, and mobile device security. The BPD is also working to launch a cybercrime education campaign[v]. CITO has offered phishing cybersecurity awareness events like "The CITO PHISH Market" and publishes weekly cyber tips for the community[vi]. Additionally, *Get Safe Online in Belize*[vii] is dedicated to helping protect businesses from online threats and keeping individuals, families, finances, devices, and workplaces safe through free, impartial, expert, and practical advice. Some cybersecurity training and education programs are available in the country, such as the Bachelor of Science in Computer Information Systems with a concentration in Cybersecurity[viii] from St. John's College and a Professional Certificate in Cybersecurity[ix] offered by the University of Belize.

Belize passed the Cybercrime Act 2020, which is now binding law and aligns with the substantial and procedural provisions of the Budapest Convention. This act provides for combating cybercrime by creating offenses, establishing penalties, and outlining investigation and prosecution procedures. It also includes measures such as search and seizure, production orders, expedited preservation orders, forfeiture orders, mutual legal assistance, and transborder access to computer data with consent or when unsecured and publicly available. The Belize Crime Observatory (BCO)[x] collects, processes, analyzes, and stores crime data to provide timely, reliable, and relevant information to its users.

The legal framework has been further strengthened with the passage of the Belize Data Protection Act in November 2021, providing a comprehensive legal framework governing the protection of personal and sensitive data. Belize has several other pieces of legislation related to cybersecurity, including the National Security Council Act 2024, Electronic Evidence Act 2021, Electronic Transactions Act 2021, Telecommunications Act 2000, Interception of Communications Act 2011, Mutual Legal Assistance in Criminal Matters Act 2006, and Intellectual Property Act 2000.

Belize's approach to controlling cybersecurity risks through standards and technologies is evolving. The National Cybersecurity Strategy 2020-2023 emphasizes the development of capacity for incident response and critical infrastructure protection. The country is on its way to establishing or adopting specific national standards for cybersecurity[91].



CYBERSECURITY
POLICY AND STRATEGY

Belize

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | **2025**
Content
2016 | 2020 | **2025**
Implementation and Review
2016 NA | 2020 NA | **2025**
International Engagement
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | **2025**
Organization
2016 | 2020 | **2025**
Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | **2025**
Coordination
2016 | 2020 | **2025** NA
Mode of Operation
2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | **2025**
Regulatory Requirements
2016 NA | 2020 NA | **2025**
Operational Practice
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA
Risk Management and Response
2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | **2025**
Defense Force Cyber Capability
2016 NA | 2020 NA | **2025**
Civil-Defense Coordination
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA
Coordination
2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Belize

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 NA | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Belize

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Bolivia

Bolivia[92] has made substantial progress in developing a National Cybersecurity Strategy (NCS) made by the Electronic Government and Information and Communications Technologies Agency (AGETIC). The NCS is structured around critical components such as governance, technical measures, capacity-building, and international cooperation. AGETIC is currently collaborating with central government entities to refine the strategy. Consultations with academia, private sector representatives, and civil society are planned to ensure a holistic approach.

Bolivia actively participates in regional and international cybersecurity forums through AGETIC, including events organized by the Organization of American States (OAS) and the United Nations. This involvement allows Bolivia to communicate its cybersecurity stance and challenges globally. The Bolivian Government CSIRT, also called Centro de Gestión de Incidentes Informáticos (CGII), was created by the Supreme Decree No. 2514, is responsible for registering and categorizing cibersecurity incidents across the government. This center collaborates with the CSIRT Americas to bolster incident management capabilities and improve the cybersecurity in Bolivia.

There is a cyberdefense unit whitin the Command-in-Chief of the Armed Forces of the State, which coordinates with the cyberdefense Departments of the Bolivian Army, the Bolivian Air Force and the Bolivian Navy, as well as corporations and strategic companies in the defense sector, Military University and CEOS.
Bolivia has moved forward with efforts to enhance cybersecurity awareness across multiple sectors. AGETIC has “Ciberconsejos” campaign that educates the public on essential cybersecurity practices, such as secure browsing, malware defense, and data privacy. Also, there is a training called “Cibersecurity for everyday” is focused to public employed and teaches them about secure password managing, malware and how to identify phishing campaigns because it are the main vector attack in cybersecurity incidents. This training was provided to more than 2500 public employees of many national entities like the Supervisory Authority for Financial System (ASFI), National Police, Ministry of Economy and Public Finance and others. Bolivia has developed targeted awareness programs focused on fraud prevention in banking and telecommunications through platforms such as “Bloquea la Estafa” (Blocking scam) that allow citizens to report digital fraud, enhancing public vigilance against cybercrime.

The private sector has also contributed by conducting awareness campaigns, especially within the financial and telecommunications industries, which focus on phishing prevention and secure digital banking. Civil society initiatives like Bolivia Verifica and Chequea Bolivia actively combat misinformation, educating the public on fact-checking and online reliability, a crucial step in building digital trust across the population

Bolivia has significantly expanded its cybersecurity education through a range of academic programs at universities and technical institutions, offering degrees and diplomas focused on information security, vulnerability management and cyber threat response. Universities such as USFX, UMSA and UMSS provide specialized training at both undergraduate and graduate levels. The Electronic Government and Information and Communications Technologies Agency, AGETIC, supports this effort through professional development workshops for public and private sector personnel. AGETIC hosts an annual cybersecurity congress to promote knowledge exchange and skill-building among professionals and students. Bolivia is working on comprehensive data protection legislation with AGETIC facilitating the legislative drafting process through consultations with relevant stakeholders. This new law aims to establish a data privacy authority and set clear standards for data protection.

The Cybercrime direction, under the Bolivian Police's Special Force to Combat Crime, handles cybercrime issues but operates largely on general procedural law. The country's forensic capabilities are supported by the Instituto de Investigación Forense, though there is a noted need for enhanced digital crime training for prosecutors and judiciary members to manage digital evidence cases effectively. Although a national law has not yet been enacted, it is worth highlighting that on May 17, 2023, the Municipality of Coroico, located in the Sud Yungas Province of the Department of La Paz, enacted the first municipal law in Bolivia on "Digitalization and Personal Data Management", an initiative that will likely promote the development of legislation in this area.

To define and protect critical infrastructure, Bolivia has two main laws: Law 164 - General Law on Telecommunications, Information and Communication Technologies - and Law 393 - Law on Financial Services.

Bolivia has implemented ISO 27001 based Institutional Security Plans within public sector entities to ensure information protection and cybersecurity management. Additionally, telecommunications and financial services are subject to standards overseen by ASFI, although coordination for national procurement standards remains limited. Critical infrastructure operators apply security practices based on recognized international standards, but efforts to formalize inter-sector collaboration are still in development. Bolivian E-Government has also made progress by receiving services such as digital citizenship, payment gateways, an electronic invoice issuing service and an interoperability platform. Initiatives such as "Digital Citizenship," which several government entities have already joined, promote not only a state-recognized digital identity but also greater security in interactions with public institutions.

For several years, AGETIC has been sending security alerts and notices to all private enterprises, public entities and other subscribers via email. This year, AGETIC implemented a MISP node to share indicators of compromise (IoCs) and information on cyber incidents and vulnerabilities.

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Bolivia

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Bolivia

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Bolivia

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

Belize

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Brazil

In February 2020, Brazil established a National Cybersecurity Strategy to strengthen the country's cybersecurity environment. It aimed to protect critical infrastructure, promote technological resilience, and foster international cooperation. The strategy prioritized improving national capabilities in incident response, risk management, and promoting secure technology development. Additionally, it seeks to raise public awareness about cybersecurity and enhance coordination among government, private sector, and civil society stakeholders.

Since then, Brazil has looked to update the cybersecurity strategy under the coordination of the National Cybersecurity Committee (CNCiber), a multistakeholder mechanism established by Decree No. 11,856 on December 26, 2023. A thematic working group has been created to support this process, which has studied strategies and institutional models of multiple countries in the world with the purpose of finding the right model for Brazil aiming to be aligned with emerging cyber challenges. The review seeks to strengthen governance, critical infrastructure protection, and national cyber capabilities, enhancing Brazil's readiness in the face of evolving threats. The revisions emphasize collaboration among public, private, and academic sectors to create a comprehensive and forward-looking framework.

Brazil has made significant progress in its digital transformation, driven by policies such as the National Digital Government Strategy that promotes the digitization of public services and the strengthening of technological infrastructure. Brazil currently leads the region in terms of Online Services according to the UN E-Government Development Index (EGDI). Brazil was also ranked among the top two countries in the Americas in Tier 1 (Role Modeling) by the fifth edition of the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI).

Brazil's Cybersecurity and Privacy Framework developed by the eGovernment Secretariat of the Ministry of Management and Innovation integrates government, private, and academic efforts to enhance resilience and respond effectively to cyber incidents. The Institutional Security Cabinet (GSI, by its acronym in Portuguese) coordinates national policy and critical infrastructure protection, while the CTIR Gov manages public sector cybersecurity incidents through monitoring and response measures through the RedBr network. The CNCiber, created in 2023, fosters collaboration across sectors to address vulnerabilities. Sectoral and regional CSIRTs work with private and academic partners, such as the National Education and Research Network (RNP), to strengthen critical sectors, share information, and promote cybersecurity awareness nationwide.

On this matter, Brazil also leverages the capabilities of its National Computer Emergency Response Team (CERT.br), responsible for handling computer security incident reports as well as coordinating and integrating all Internet initiatives and services in the country. CERT.br also develops other activities that include raising awareness about security problems, analyzing trends and correlation between events on the Brazilian Internet, and assisting in the establishment of new CSIRTs in Brazil.

The country is also home to CAIS, a security incident response center established by the Brazilian network for education and research (RNP) with the purpose of developing preventive, educational and corrective actions specific to the incidents and threats present in the academic network, thus ensuring security in hundreds of Brazilian education and research institutions. Correspondingly, the Brazilian Digital Government Integrated Cybersecurity Center (CISC Gov.br) has the mission of promoting operational coordination of actions destined to prevent, manage and respond to cyber incidents within the scope of the national Information Technology Resources Management System (Sisp), in addition to spearheading cyber threat intelligence activities while preparing and publishing alerts and recommendations.

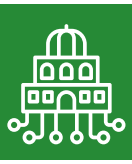
Awareness of cybersecurity efforts to protect personal information online are supported by educational campaigns and privacy policies implemented by public and private sectors. Reporting mechanisms, such as the ANPD's complaint system, are established and regularly promoted to address privacy concerns and incidents. Media and social media play a vital role in raising cybersecurity awareness. Beyond simply reporting threats, they inform the public about proactive measures and discuss the social and economic impacts of cybersecurity. Frequent online discussions encourage transparency, and examples like "Cybersecurity Metrics for Boards" highlight the importance of integrating security measures into organizational strategies. Together, these efforts reflect a multifaceted but evolving approach to strengthening Brazil's cybersecurity culture.

Brazil's cybersecurity policies also prioritize building knowledge and strengthening national capabilities through diverse initiatives. Private sector engagement is actively encouraged, with companies contributing to cybersecurity service provision and technological advancements. Collaborative frameworks, such as those supported by the CNCiber, integrate private sector expertise into the country's strategic planning. Partnerships between public and private entities also enable training programs to build capacity across sectors, ensuring a skilled and prepared workforce.

Educational and formal training initiatives are vital components of Brazil's strategy. Universities offer specialized degrees in cybersecurity, supported by institutions like the National Education and Research Network (RNP), which fosters research and development partnerships. Scholarships and public awareness campaigns aim to address the talent gap in cybersecurity, while formal workforce training programs provide certifications and integrate cybersecurity topics into educational curricula. These efforts, combined with investments in academic and technological research, strengthen Brazil's ability to tackle evolving cyber threats and build a resilient digital ecosystem.

Cybersecurity legislation in Brazil covers various critical areas, though its implementation and impact differ across sectors. Substantive norms on cybercrimes are integrated into specific legislation and general criminal law, with efforts to align national measures with international frameworks. The country has developed comprehensive data protection legislation, such as the General Data Protection Law (LGPD - Law 13709/2018), which establishes standards aligned with international best practices and designates a national agency for oversight. Similarly, online child protection is reflected in existing laws, including the Statute of the Child and Adolescent (Law 8069/1990), and proposed legislation like Bill 2628/2022, which emphasizes safety in digital services for minors. Consumer protection is addressed through the Consumer Defense Code (Law 8.078/90) and specific e-commerce regulations under Decree 7.962/2013. Institutional capacities for investigating and prosecuting cybercrimes are gradually expanding. In 2023, the structure of the Federal Police of Brazil for investigating cybercrime was significantly strengthened with the creation of the Directorate for Combating Cybercrime (DCIBER). Located at the Federal Police headquarters, this Directorate includes the national 24/7 Network Contact Point for international cooperation and four specialized units responsible for intelligence analysis and operational support to cybercrime investigations. Additionally, it comprises a Division for Special Investigations, which focuses on

high-impact or particularly complex cases requiring international cooperation. Priority areas under this division include: combating online hate crimes, particularly offenses disseminated via global computer networks that incite violence, threaten mass attacks—especially targeting educational institutions—and spread misogynistic content with cross-border implications; investigating high-tech crimes such as unlawful access to IT systems, ransomware, and denial-of-service attacks targeting public sector infrastructure; addressing cybercrimes related to child and adolescent sexual abuse, including offenses under the Child and Adolescent Statute (e.g., possession, production, and distribution of child sexual abuse material) and the Criminal Code (e.g., rape of vulnerable persons); and tackling electronic banking fraud involving illicit financial schemes, digital scams, and other cyber-enabled financial offenses. In the same vein, the Federal Prosecution Service (Ministério Público Federal) created, in 2024, the Special Task Force for Combating Cybercrime and Offenses Committed through the Use of Information Technologies (GACCTI), with the aim of supporting criminal and civil investigations and proceedings focused on the prevention and repression of cybercrime. Federal and state police have specialized cybercrime units, supported by forensic laboratories equipped for digital investigations. However, these capabilities are unevenly distributed across the country. Cooperation between public and private sectors in cybercrime investigations remains limited, with challenges in establishing effective partnerships. Internationally, Brazil has expanded its engagement in global efforts to combat cybercrime. The country is a member of the International Counter Ransomware Initiative (CRI) and, in 2023, became a Party to the Budapest Convention on Cybercrime, reinforcing its commitment to international cooperation in the cyber domain. Brazil participates in formal mechanisms for cross-border cooperation, such as mutual legal assistance agreements and extradition frameworks, and engages with global networks like Interpol to address cybercrime. Despite these developments, gaps in digital training for judges and prosecutors, as well as the lack of consistent adoption of cybersecurity standards in procurement and service delivery, indicate areas for further improvement.



CYBERSECURITY POLICY AND STRATEGY

Brazil

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Brazil

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Brazil

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Brazil

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Brazil

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 NA | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025**

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Chile

Chile has developed its second National Cybersecurity Policy (2023–2028), which builds upon the Chile has developed its second National Cybersecurity Policy (2023–2028), which builds upon the objectives of the previous strategy (2017–2022) and aims to address new and evolving cyber risks. This policy aligns cybersecurity initiatives with national priorities in governance, social inclusion, and economic growth. Notably, the policy sets clear objectives for enhancing infrastructure resilience, promoting national and international cooperation and coordination between agencies, the public sector and the industry, protecting citizen rights in cyberspace, and fostering a cybersecurity culture as well as a secure digital environment. It integrates cybersecurity into other national strategies and includes mechanisms for periodic review and updates every three years. In 2018 Chile published its first Cyberdefense Policy.

Chile has also taken strides toward establishing a National Cybersecurity Agency (ANCI, by its acronym in Spanish) which began operations in 2025 and oversees incident response, vulnerability coordination, and infrastructure protection, as mandated by the Framework Law on Cybersecurity enacted in 2024. The Agency has incident response, regulatory, oversight, and sanctioning capabilities for the public and private sectors. In addition, the Governmental CSIRT, housed under the Ministry of the Interior, has transitioned to the National CSIRT under the new agency in 2025 consolidating response capabilities and fostering interagency cooperation.

Within the framework of the new law, Chile has established an Interministerial Cybersecurity Committee, which advises the President on the conception and analysis of cybersecurity policies, proposes policy adjustments to strengthen the regulatory framework in cybersecurity, supports ANCI in preventing and responding to cyber-incidents, and coordinates the proper implementation of the National Cybersecurity Policy.The Committee includes representatives from key ministries, including the Undersecretariat of Defense and existed, created by an administrative regulation, since 2015. Additionally, a Multisector Advisory Council on Cybersecurity was created, with representatives from industry, commerce, civil society, and academia, as an advisory body to the Agency.

Chile has significantly bolstered public cybersecurity awareness, with the National Cybersecurity Month established under Law No. 21.113. During this period, government agencies conduct extensive public education initiatives and exercises, encouraging secure practices across the digital space.

ANCI and the CSIRT are supported technically and financially by the IDB through the “Program to Strengthen the Strategic Management of Public Security in Chile” CH-L1142 which includes a specific programmatic component to build the government’s central cybersecurity capacity, with a planned budget of USD 27 million.

Civil society also plays a major role, with organizations such as Alianza Chilena por la Ciberseguridad, Fundación País Digital and Fundación Educacional WHILOLAB promoting cybersecurity knowledge and providing free cybersecurity diplomas for citizens. Moreover, the establishment of the Cybersecurity

and Strategic Studies Observatory at Universidad SEK enhances research and public understanding of cybersecurity issues. Additionally, the NGO Derechos Digitales has played a key role in shaping national cybersecurity policy and public discourse, contributing to consultations and awareness-raising from a digital rights perspective.

Since 2014, Chile has developed an international agenda that includes cooperation and dialogue with partners, promoting national participation in multilateral international forums, and fostering and strengthening responsible state behaviour in cyberspace and cyber diplomacy. Chile actively participates in the Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025. Chile also activately participate and works with OAS/CICTE inititiaves. It is currently a party state of the Budapest Convention on Cybercrime, the Global Forum on Cyber Expertise, FIRST, and recently joined the Counter Ransomware Initiative. Chile also contributes to regional cooperation, especially through the AGCID initiative funded by the European Union and benefiting 12 countries in Latin America and the Caribbean.

Public-private partnerships are instrumental in awareness-building, as evidenced by campaigns organized by the Chilean-American Chamber of Commerce and sectoral entities like the Association of Banks and Financial Institutions (ABIF, by its acronym in Spanish), Mining Cybersecurity Corporation (CCMIN, by its acronym in Spanish), which promotes best practices in cybersecurity within the critical mining sector. Additionally, the Texas National Guard and the Chilean Army conducted a joint cybersecurity exercise in 2023. Moreover, as a nation, Chile also participated in the international military cybersecurity exercises conducted during Tradewinds 2024 (TW24).

Educational institutions across Chile offer a range of cybersecurity programs, from undergraduate degrees to specialized diplomas master's programs and PHD's programs. Universities like Universidad de Chile and Universidad Técnica Federico Santa María provide advanced cybersecurity training and research opportunities, while the Ministry of Education supports youth programs like Internet Segura, teaching students and parents about digital responsibility and security.

As the country faces a shortage of skilled cybersecurity professionals, the National CSIRT and private sector organizations are addressing this gap by offering scholarships, certifications, and on-the-job training for students and early-career professionals. In this regard, the Cybersecurity Engineering degree is offered at multiple universities (INACAP, AIEP, SEK, Mayor, and Andrés Bello). Chile has also made progress in cybersecurity workforce development through targeted capacity-building programs funded by international cooperation.

Chile's Framework Law on Cybersecurity (Law No. 21.663) defines critical infrastructure sectors and requires designated operators, termed Operators of Vital Importance (OIV, by its acronym in Spanish), to implement a robust Information Security Management System. Public agencies and private operators across sectors such as energy, telecommunications, finance, and healthcare are subject to cybersecurity audits and certification requirements outlined by the new agency. The law grants ANCI the authority to identify new OIVs administratively at least every three years, ensuring the framework remains responsive to changing threats. It also mandates that all critical infrastructure operators follow stringent cybersecurity standards and requires reporting of significant cyber-incidents and imposes penalties for non-compliance. Additionally, Law No. 21.459, which aligns Chile's criminal code with the Budapest Convention on Cybercrime, classifies cyber offenses and establishes penalties for unauthorized access, data breaches, and cyber fraud. It includes modern procedural tools and a forward-compatible legal

structure for investigating and prosecuting cybercrime.

A new data protection law 21.719 was approved and published in December 2024 to reinforce data privacy measures, further ensuring that both public and private entities comply with global data protection standards and meet international commitments. Moreover, the Policía de Investigaciones (PDI), or Investigations Police, created the National Cybercrime Headquarters on March 2022. This facility gathers and unites the efforts of three different Cybercrime Investigative Brigades.

In terms of standards, Chile has promoted ISO 27001 standards in cybersecurity practices, ensuring continuity and resilience in key services. In E-Government, Chile has implemented a secure digital identity system (ClaveÚnica) with over 15 million active users, enhancing secure access to online government services. Digital governance statistics reveal that over 93% of public service transactions are now conducted digitally, contributing to Chile's recognition as a regional leader in digital transformation in Latin America. These initiatives and strengthening E-Government cybersecurity are among Chile's digital agenda projects technically and financially supported by the IDB through the Digital Government Secretariat (SGD). In addition, Chile is a participant in the EU-LAC Digital Alliance, which fosters bi-regional cooperation on digital transformation and cybersecurity. Chile also maintains a growing market for cyber insurance, including products accessible to SMEs, supported by regulatory encouragement and risk-awareness measures.

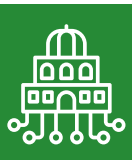
In regards to the protection of human rights and personal data in the context of cybersecurity Chile has incorporated a specific objective into its National Cybersecurity Policy (2023–2028) aimed at protecting individuals' rights online. This objective is primarily pursued through the strengthening of public institutions responsible for cybersecurity and data protection.

To advance in this area, the country has developed a robust legal framework, including the approval of both the Framework Law on Cybersecurity and the Personal Data Protection Law. The Framework Law on Cybersecurity establishes the principle of security and privacy by default and by design, which requires that all IT systems and technologies be developed with data protection considerations integrated from the outset.

Under this law, the National Cybersecurity Agency (ANCI) was created as an advisory body to the Presidency of the Republic. ANCI is responsible for ensuring that cybersecurity policies are implemented in a manner that respects fundamental rights, particularly the right to privacy and the protection of personal data. Its actions must comply with the provisions of Law No. 19.628 on the Protection of Private Life, which currently serves as the main legal instrument in this field.

This legislation will be complemented by the new Personal Data Protection Law, which will come into force on December 1, 2026. This new law strengthens data protection standards and establishes the Personal Data Protection Agency, tasked with safeguarding privacy rights and overseeing legal compliance by both public and private entities.

Through these measures, Chile consolidates a regulatory approach that acknowledges the interdependence between cybersecurity, human rights, and data protection—promoting a responsible, people-centered model of digital governance.



CYBERSECURITY POLICY AND STRATEGY

Chile

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | **2025**

Content
2016 | 2020 | **2025**

Implementation and Review
2016 NA | 2020 NA | **2025**

International Engagement
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | **2025**

Organization
2016 | 2020 | **2025**

Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | **2025**

Coordination
2016 | 2020 | **2025** NA

Mode of Operation
2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | **2025**

Regulatory Requirements
2016 NA | 2020 NA | **2025**

Operational Practice
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

Risk Management and Response
2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | **2025**

Defense Force Cyber Capability
2016 NA | 2020 NA | **2025**

Civil-Defense Coordination
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

Coordination
2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Chile

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Chile

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Chile

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Chile

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Colombia

Colombia has made significant strides in developing cybersecurity policies and strategies over the past decade. The country has adopted three national policies: CONPES 3701 (2011), CONPES 3854 (2016), and CONPES 3995 (2020)[xi], which establish a framework for enhancing digital trust and security. These policies support digital transformation while addressing cybersecurity challenges, emphasizing a multi-stakeholder approach involving government agencies, civil society, academia, and the private sector. In 2024, Colombia is formulating a National Digital Security Strategy with technical assistance from the IDB, in coordination with the National Digital Strategy 2023-2026 and policy instruments related to Artificial Intelligence. In addition, Colombia is a participant in the EU-LAC Digital Alliance, which fosters bi-regional cooperation on digital transformation and cybersecurity.

The country has established a national cybersecurity structure following a "whole-of-nation" approach, as outlined in Decree 338 of 2022[xii]. The governance model[xiii] includes various decision-making levels, such as the National Digital Security Coordinator, the National Digital Security Committee, Digital Security Working Groups, CSIRT (for private and public companies and sectoral teams) and Unified Command Posts for national crises. This structure aims to strengthen digital security, protect networks, critical infrastructures, essential services, and information systems in cyberspace. Currently, legislative initiatives are underway to create a National Digital Security Agency to manage digital security risks in Colombia.

To enhance cybersecurity literacy, Colombia has implemented multiple awareness and training campaigns. The Ministry of Information and Communications Technologies (MINTIC) offers content and training initiatives through programs like Ciberpaz[xiv] and Cibereduca[xv]. The Ministry of National Education provides courses on cybersecurity basics for students, teachers, and parents through the Colombia Aprende portal[xvi], including a course on "Fundamentals of security, compliance and identity" aimed at women[xvii].

Colombia has addressed the growing demand for cybersecurity professionals through various initiatives. The country offers a range of cybersecurity education and training programs, covering topics from basic awareness for the public to advanced technical skills for specialized professionals[xviii]. Academic programs in cybersecurity are available at the tertiary level, primarily at the postgraduate level[xix], as reported by the Ministry of Education.

In Colombia there are several laws and regulations that regulate various issues associated with digital security, data protection and cybercrime. The country has adopted comprehensive cybercrime legislation and joined the Budapest Convention in 2020. The main Substantive Cybercrime Legislation is Law 1273, complemented by other legal acts addressing various aspects of cybercrime. Colombia has established specialized units to combat cybercrime, including the Police Cybernetic Center and a specialized unit within the Attorney General's Office. While the judicial system is responsible for adjudicating cybercrime cases, there is a recognized need for more formal and systematic training for judges and magistrates in cybercrime and digital evidence collection. A new draft statutory law is currently under discussion, aiming to update the legal framework with a new General Regime for the Protection of Personal Data in Colombia.

Colombia has made progress in adopting standards and technologies for cybersecurity risk management. MINTIC has implemented the Information Security and Privacy Framework (MSPI)[xx] which was recently updated to align with the adjustments introduced in the ISO 27001:2022[93] [xxi] to strengthen public institutions' ICT infrastructure and information systems. Many public sector organizations have taken significant steps to implement these standards and improve cybersecurity. For example, the National Tax and Customs Directorate (DIAN), the Office of the Comptroller General and the National Agency for Legal Defense of the State (ANDJE) are among the organizations who significantly strengthened their cybersecurity with IDB technical and financial support.

The country has established various Computer Security Incident Response Teams (CSIRTs) across public and private sectors, with ColCERT recognized as the national computer emergency response team[xxii]. The country also has the Government Computer Security Incident Response Team (CSIRT Gov)[xxiii], the Defense CSIRT[xxiv], the CSIRT of the National Police[xxv], the Intelligence CSIRT, and sectoral CSIRTs such as those of the telecommunications, banking, and energy sectors, and more recently, a Health CSIRT was established for the entities affiliated with that administrative sector. There are 24 CSIRTs and security operations centers (COS) registered with FIRST and 8 in OAS/CICTE CSIRT Americas. However, incident response capacity among small and medium-sized enterprises remains limited. The protection of critical infrastructure is an ongoing challenge, with MINTIC recently updating its approach to identifying and protecting National Critical Cyber Infrastructures (ICCN).[94]

CYBERSECURITY CULTURE AND SOCIETY

Colombia

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Colombia

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Colombia

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Colombia

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Costa Rica

In the wake of major ransomware attacks in 2022, Costa Rica has made significant progress in developing a comprehensive cybersecurity policy and strategy framework. The 2023-2027 National Cybersecurity Strategy[95] outlines a strategic vision based on an efficient institutional model, strengthening national leadership and uniting all stakeholders under a human rights focus. The country has embraced a "whole-of-society" approach, fostering effective coordination among state and non-state actors. The National Cybersecurity Directorate, housed within the Ministry of Science, Innovation, Technology, and Telecommunications (MICITT), spearheads national cybersecurity efforts. The Computer Security Incident Response Center (CSIRT-CR) plays a crucial role in coordinating incident response, while the Security Operations Center (SOC) bolsters cybersecurity capabilities in detection, protection, response, and recovery for public institutions by implementing advanced monitoring and automated response systems, integrating emerging technologies such as artificial intelligence and machine learning to improve efficiency and effectiveness. Costa Rica collaborates with international organizations such as the UN, OAS, EU, and SICA, as well as multilateral development banks like the World Bank and the International Development Bank. The country also cooperates with other nations, including the United States, South Korea, and Spain, along with Central American and Caribbean countries like the Dominican Republic, Panama, and Honduras. Costa Rica is focusing on strengthening its national incident response capabilities by enhancing the CSIRT-CR, establishing sectoral Computer Security Incident Response Teams, and implementing a national platform for reporting and managing cybersecurity incidents. To boost national cyber resilience, the country is implementing an early warning system for cyber threats, conducting regular national cybersecurity exercises and drills, and developing business continuity and disaster recovery plans for critical infrastructures and essential services.

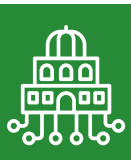
Moreover, in 2024, the country enacted the Regulation for Cybersecurity Governance and Cyber Resilience of Government Institutions (Decree No. 45061-MICITT), which establishes mandatory incident reporting within 24 hours, requires periodic technical audits, and formalizes the structure of the National Cybersecurity Directorate through the creation of the SOC-CR and CSIRT-CR departments aligned with best practices for governance, identification, detection, protection, response, and recovery.[96]

Costa Rica has launched various initiatives to foster a cybersecurity-aware culture among its citizens. These include public awareness campaigns, educational programs, workshops, and webinars aimed at improving cybersecurity hygiene and literacy. One such program is the course "Don't be a victim of hacking". The country has partnered with private sector organizations and non-governmental entities, such as Cybersec Cluster, to reach a wider audience. To build cybersecurity expertise, Costa Rica offers accredited university degrees and courses in cybersecurity and is developing a national cybersecurity education framework with training programs across all educational levels. The country is also creating specialized cybersecurity training programs for public sector employees. Collaborations with universities, research institutions, and international partners are being encouraged to support knowledge transfer and skill development in the cybersecurity domain. Moreover, Costa Rica is promoting gender equality[xxvi] and diversity in cybersecurity education and careers to create a sustainable pipeline of cybersecurity professionals[xxvii].

Costa Rica has established a robust legal and regulatory framework to address the challenges of the digital economy. Key legislation covers several areas, including the promotion of scientific and technological development, protection of personal data and privacy, online child protection, promotion of social equality for women, consumer defense, legal intervention in communications, and the adoption of digital certificates, signatures, and electronic documents. The country has also signed international agreements and treaties, such as the Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol, demonstrating its commitment to international cooperation in combating cybercrime. Costa Rica also participates in the Counter Ransomware Initiative (CRI).

The country is actively working to adjust, adapt, and harmonize its cybersecurity-related legal and regulatory landscape. This includes drafting a Costa Rican Cybersecurity Bill[xxviii] and assisting sectoral regulators in adapting their frameworks and overseeing cybersecurity-related provisions. Costa Rica is updating its regulatory framework to strengthen administrative and technical processes for the CSIRT-CR and establish standards, protocols, and technical procedures for national cybersecurity incident management. These include a national incident response process, crisis management and response procedures, and cybersecurity playbooks and infographics[xxix].

Costa Rica is taking proactive steps to control cybersecurity risks through the adoption of standards and technologies. The country is developing a comprehensive cybersecurity risk management framework at the national level, which incorporates a gender perspective with an intersectional approach. This framework includes a national cybersecurity risk assessment methodology, a catalog of cybersecurity threats and risks, and an updated inventory of national critical infrastructures and essential services. Recently, the country has been developing a National Cyber Intelligence and Digital Forensics Laboratory in cooperation with Spain's National Cryptologic Center (CCN), thereby strengthening its capabilities for early detection and advanced analysis of cyber threats. This initiative not only enhances the country's technical capacity but also reinforces international cooperation in the exchange of information and intelligence on cyber threats.[97]



CYBERSECURITY
POLICY AND STRATEGY

Costa Rica

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Costa Rica

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Costa Rica

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Costa Rica

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

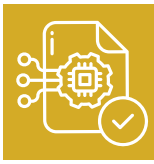
Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 NA | **2025** NA



STANDARDS AND TECHNOLOGIES

Costa Rica

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Dominica

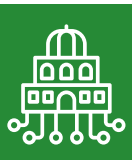
Dominica's cybersecurity landscape is evolving as the country takes steps to strengthen its digital resilience and protect critical infrastructure. With support from the World Bank, the Caribbean Digital Transformation Project (CDTP)[xxx] in Dominica includes a significant cybersecurity component aimed at bolstering the country's digital resilience and fostering trust in online transactions. The project focuses on developing a robust cybersecurity ecosystem through several key initiatives, including a review of cybersecurity policies, legislation, and institutional structures at the national level.

Plans are underway to establish a national Computer Emergency Response Team (CERT) aligned with regional models to enhance threat intelligence sharing and incident response capabilities. Dominica's involvement in regional cybersecurity initiatives, such as OAS CSIRT Americas Week[xxxi], enhances the country's cyber capabilities by providing mentorship and specialized instruction. This participation suggests potential opportunities for knowledge transfer and capacity building in collaboration with international partners. Additionally, Dominica participated in the "Final Workshop on CIRT Establishment Plan" organized by CARICOM IMPACS, reaffirming its commitment to strengthening national cybersecurity capabilities through regional cooperation.

Building cybersecurity knowledge and capabilities in Dominica is an ongoing process. As part of its broader digital transformation agenda, the country is working to incorporate cybersecurity education into its curricula and professional development programs. Some actors, such as the National Bank of Dominica[xxxii], are advancing initiatives like the Cybersecurity Awareness Competition for secondary and college students. These efforts aim to educate young people about cyber threats such as phishing, ransomware, and malware, emphasizing the importance of protecting personal data in an increasingly digital world. Additionally, Dominica Electricity Services Ltd.[xxxiii] provides key information and interactive sessions to help protect digital assets in personal and work environments.

Dominica's legal and regulatory framework for cybersecurity is in a developmental stage. The country has enacted several laws that address aspects of cybersecurity and digital transactions, including the Electronic Transactions Act 2013, Electronic Funds Transfer Act 2013, Electronic Evidence Act 2010, and Copyright Act 2003.

The integration of monitoring and detection technologies and standards across key sectors in Dominica is an area that requires further development. As the country progresses with its digital transformation, it is likely that more attention will be given to implementing technological solutions to enhance cyber resilience[98].



CYBERSECURITY POLICY AND STRATEGY

Dominica

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | **2025**

Content
2016 | 2020 | **2025**

Implementation and Review
2016 NA | 2020 NA | **2025**

International Engagement
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | **2025**

Organization
2016 | 2020 | **2025**

Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | **2025**

Coordination
2016 | 2020 | **2025** NA

Mode of Operation
2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | **2025**

Regulatory Requirements
2016 NA | 2020 NA | **2025**

Operational Practice
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

Risk Management and Response
2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | **2025**

Defense Force Cyber Capability
2016 NA | 2020 NA | **2025**

Civil-Defense Coordination
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

Coordination
2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Dominica

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Dominica

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Dominica

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

Dominica

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 NA | 2020 NA | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Dominican Republic

The Dominican Republic has strengthened its National Cybersecurity Strategy (NCS), originally established by Decree 230-18[99], with a proactive approach to align with national socio-economic and technological developments. The current strategy, -the second one- decreed under Decree 313-22[100], extends through 2030[101]. This strategic roadmap includes a detailed Implementation Plan for 2022–2024 that outlines six key objectives: enhancing institutional capabilities, protecting critical infrastructures, fostering a cybersecurity culture, building national and international partnerships, advancing cybersecurity research, and strengthening legal frameworks[102].

The National Cybersecurity Center (CNCS)[103] coordinates these efforts, actively consulting with public and private sectors, academia, and civil society through in-person and digital forums, including the CitizenLab platform[104]. Additionally, critical infrastructure operators are mandated by Decree 685-22[105] to report incidents within 24 hours, which CNCS oversees. The Dominican Republic's CSIRT network includes specialized sectoral CSIRTs, like SPRICS[106], managed by the Central Bank and dedicated to the financial sector, ensuring cybersecurity across all banking entities.

In 2024 the CNCS became part of the National Bureau of Investigations where it was integrated into the iSOC for the exchange of threat intelligence information. Additionally, it developed monitoring, detection and response capabilities to cybersecurity incidents through its SOC and carried out national risk assessment activities and identification of Critical Information Infrastructures.

Additionally, in 2021 and 2022, the Dominican Republic approved three strategic projects[107] with the IDB for the country's digital development: the Program for the Improvement of Connectivity and Digital Transformation, the Program for the Strengthening of the Ministry of Public Administration, and the Program for the Strengthening of Integrity and Transparency of the Dominican Republic, totaling more than 200 million dollars of investment. These projects promote the country's digital transformation and incorporate activities to strengthen the government's cybersecurity capabilities, including training and awareness-raising activities for society.The Dominican Republic prioritizes public awareness and education initiatives to build a robust national cybersecurity culture. Through CNCS, the country conducts monthly campaigns, such as the Multifactor Authentication Campaign[108] in June 2024 and Women in Cybersecurity Campaign[109] in March 2024 to engage diverse groups. The National Cybersecurity Awareness Portal[110] provides the public with resources and tools to increase digital literacy and resilience. International collaboration also remains a priority, with the Dominican Republic actively participating in the UN Ad Hoc Committee on Cybercrime[111] and the Counter-Ransomware Initiative (CRI)[112] with countries like the United States.

To bolster cybersecurity capabilities, the Dominican Republic has established numerous educational programs across academic institutions, including INTEC's Master's in Cybersecurity [113] and UNPHU's Cybersecurity program [114]. Additionally, the ITLA offers a Cybersecurity Technologist program to address

workforce demands[115]. The Dominican Republic is an active player in the Latin American and Caribbean cybersecurity network of excellence CiberLAC[116], of which INTEC and the University of the Caribbean are full members[117].

The LAC4 Cyber Capacity Center for Latin America and the Caribbean, a regional cybersecurity hub hosted in the Dominican Republic with EU support, promotes national and regional cyber capacity-building[118]. This center organizes training and exercises to reinforce skills in cyber threat identification, response, and resilience.

The country also participates in FIRST[119] and GLACY+ (2016-2023) and GLACY-e (2023-2026), a regional hub for Council of Europe's capacity-building projects.

The Dominican Republic has a comprehensive cybersecurity legal framework covering cybercrime, data protection, and critical infrastructure security. Law 53-07[120] addresses high-tech crimes, while Law 172-13[121] on Data Protection safeguards personal data. Additionally, the National Critical Infrastructure Protection Regulation, under Decree 685-22, mandates stringent reporting and risk management standards for critical infrastructure sectors.

In international cybersecurity cooperation, the country is a signatory of the Budapest Convention on Cybercrime, the OAS Inter-American Committee Against Terrorism (CICTE), and maintains partnerships through Cyber4Dev[122] and EU CyberNet[123] for technical support and capacity building and was recently selected as one of the member countries on the Board of Directors of the Forum of Incident Response and Security Teams (FIRST)[124]. The Dominican Republic actively collaborates with CARICOM IMPACS through various regional security initiatives, despite not being a full member of CARICOM. Example of this collaboration include its participation in the CBSI-Connect Platform, which provides training to Law Enforcement agencies across the Caribbean[125]. To promote secure digital infrastructure, the Dominican Republic adheres to international cybersecurity standards, including ISO/IEC 27001 and the NIST Cybersecurity Framework[126]. The private sector has increasingly adopted ISO 27001 certification and PCI-DSS standards in the financial and telecommunications sectors. Additionally, CNCS has issued a National Incident Reporting Guide[127] to standardize incident classification and response processes across sectors.

The government also prioritizes e-governance through services offered on the Dominican E-Government Portal[128], including digital services such as tax filing, passport renewal, and property records. This portal enhances public service efficiency and aligns with the Digital Agenda 2030 for a secure and modernized government framework[129].

CYBERSECURITY POLICY AND STRATEGY

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | 2025
- Content — 2016 | 2020 | 2025
- Implementation and Review — 2016 NA | 2020 NA | 2025
- International Engagement — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | 2025
- Organization — 2016 | 2020 | 2025
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | 2025
- Coordination — 2016 | 2020 | 2025 NA
- Mode of Operation — 2016 NA | 2020 | 2025 NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | 2025
- Regulatory Requirements — 2016 NA | 2020 NA | 2025
- Operational Practice — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA
- Risk Management and Response — 2016 | 2020 | 2025 NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | 2025
- Defense Force Cyber Capability — 2016 NA | 2020 NA | 2025
- Civil-Defense Coordination — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA
- Coordination — 2016 | 2020 | 2025 NA

CYBERSECURITY CULTURE AND SOCIETY

D2

2-1 Cybersecurity Mind-Set

- Awareness of Risks — 2016 NA | 2020 NA | 2025
- Priority of Security — 2016 NA | 2020 NA | 2025
- Practices — 2016 NA | 2020 NA | 2025
- Government — 2016 | 2020 | 2025 NA
- Private Sector — 2016 | 2020 | 2025 NA
- Users — 2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

- Digital Literacy and Skills — 2016 NA | 2020 NA | 2025
- User Trust and Confidence in Online Search and Information- — 2016 | 2020 | 2025
- Disinformation — 2016 NA | 2020 NA | 2025
- User Trust in E-Government Services — 2016 | 2020 | 2025
- User Trust in E-commerce Services — 2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

- Personal Information Protection Online — 2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

- Reporting Mechanisms — 2016 NA | 2020 | 2025

2-5 Media and Online Platforms

- Media and Social Media — 2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Dominican Republic

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Dominican Republic

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Ecuador

Ecuador published its National Cybersecurity Strategy in 2022, focusing its strategic efforts on enhancing cyber resilience, protecting critical infrastructure, and fostering a secure digital environment. It outlines goals in governance, infrastructure security, and public awareness to counter cyber threats. The strategy emphasizes collaboration across government, private sectors, and international partners, aiming for a secure digital economy and society[130]. Initiatives include capacity-building, regulatory frameworks, and a national incident response system to improve preparedness and response capabilities[131]. Ecuador's cybersecurity strategy is coordinated by the National Cybersecurity Committee which is composed of representatives from various government agencies responsible for national security, defense, telecommunications, finance, and public administration. This committee coordinates cybersecurity efforts, policy implementation, and response initiatives across sectors to enhance Ecuador's digital security infrastructure.

Ecuador's National Cybersecurity Strategy received support from several international partners, including the Organization of American States (OAS), the Inter-American Development Bank (IDB), and the European Union. These organizations assisted with technical expertise, funding, and strategic insights to strengthen Ecuador's cybersecurity capabilities and align its approach with global best practices.

The national response to cyber incidents and the protection of critical infrastructure falls under the responsibilities of EcuCERT, established in 2014 under the Agency for the Regulation and Control of Telecommunications (Arcotel),[132] its main priorities include monitoring and mitigating cyber threats, providing cybersecurity training, and developing policies to safeguard essential sectors like energy, finance, health, and telecommunications. EcuCERT collaborates with national and international entities, being part of the CSIRT Americas Network to enhance Ecuador's cybersecurity resilience and incident response capabilities. A catalog of national critical infrastructure is being created, identifying nine state ministries, the National Electoral Council, and five strategic companies responsible for digital critical infrastructure[133].

Ecuador has a range of cybersecurity awareness programs from both public and private sectors aimed at building digital security knowledge. The Ecuadorian Cybersecurity Association (AECI, by its acronym in Spanish) plays a key role in promoting cybersecurity awareness by organizing workshops, events, and collaborative educational efforts targeting both public and private entities[134].

Educational institutions and government programs further support Ecuador's cybersecurity goals. Schools such as the National Polytechnic School (EPN, by its acronym in Spanish) offer courses in information security, fostering a skilled workforce and raising awareness among students and professionals[135]. Additionally, the National Cybersecurity Strategy includes initiatives to promote secure online practices and cyber hygiene, fulfilling commitments made to international partners such as the OAS and IDB. Together, these programs enhance Ecuador's cybersecurity landscape by building knowledge and encouraging proactive digital security practices.

Regarding E-Government, Ecuador's initiatives are rooted in its Digital Transformation Agenda 2022–2025, which emphasizes reducing the digital divide, enhancing government efficiency, and expanding connectivity across the nation[136]. The agenda supports modernization efforts in public administration, e-commerce, and cybersecurity. Key components include making digital services accessible to both urban and rural areas, focusing on sectors like agriculture, which relies on digital tools to meet international trade standards.[137] This agenda includes "Digital Security and Trust" as one of its key pillars, ensuring that the implementation of digital technologies in the public sector is carried out in a secure and reliable manner.

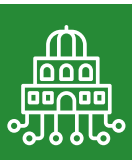
Several public sectoral organizations have benefited from technical and financial support by the IDB to improve their cybersecurity. Some recent examples include the National Customs Service (SENAE, by its acronym in Spanish)[138], the Unit for Financial and Economic Analysis (UAFE, by its acronym in Spanish), the Ministry of Economy and Finance (MEF) and the Ministry of Interior[139].

Ecuador is a participant in the EU-LAC Digital Alliance, a bi-regional initiative aimed at promoting a human-centric digital transformation[140], and has recently joined LAC4, the Latin America and Caribbean Cyber Competence Centre, as a participating nation[141].

In terms of legislation, Ecuador has established various cybersecurity laws and regulatory measures to ensure digital security and protect personal data. One great improvement in its cyber related laws is the Organic Law on the Protection of Personal Data (LOPDP, by its acronym in Spanish), introduced in 2021, which mandates guidelines for data privacy, including the need for organizations to report security breaches and designate data protection officers when handling sensitive information[142]. This law is enforced by the Superintendence of Data Protection, tasked with overseeing compliance, maintaining a national registry, and providing oversight on data protection practices. Additionally, Ecuador's cybersecurity regulations require safeguards for personal data, particularly in sectors like healthcare, transportation, and financial services, where data is processed on a large scale.

Ecuador's legal framework also includes child protection legislation, protecting minors from online risks, and intellectual property laws that address digital copyright infringements. To strengthen its digital preventative and investigative capacities, Ecuador's National Police (PNE, by its acronym in Spanish) is establishing a National Cyber Center with technical and financial support from the IDB [143].

While the country has made strides toward comprehensive cybercrime legislation, it has not yet fully joined the Budapest Convention on Cybercrime. However, Ecuador has partnered with the Council of Europe's GLACY+ project to develop its national cybercrime strategy, aligning with international standards to enhance its capacity for cybercrime investigation and prosecution.



CYBERSECURITY POLICY AND STRATEGY

Ecuador

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | **2025**
Content
2016 | 2020 | **2025**
Implementation and Review
2016 NA | 2020 NA | **2025**
International Engagement
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | **2025**
Organization
2016 | 2020 | **2025**
Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | **2025**
Coordination
2016 | 2020 | **2025** NA
Mode of Operation
2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | **2025**
Regulatory Requirements
2016 NA | 2020 NA | **2025**
Operational Practice
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA
Risk Management and Response
2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | **2025**
Defense Force Cyber Capability
2016 NA | 2020 NA | **2025**
Civil-Defense Coordination
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA
Coordination
2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Ecuador

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**
Priority of Security
2016 NA | 2020 NA | **2025**
Practices
2016 NA | 2020 NA | **2025**
Government
2016 | 2020 | **2025**
Private Sector
2016 | 2020 | **2025**
Users
2016 | 2020 | **2025**

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 | 2020 | **2025**
User Trust and Confidence in Online Search and Information
2016 | 2020 | **2025**
Disinformation
2016 NA | 2020 NA | **2025**
User Trust in E-Government Services
2016 | 2020 | **2025**
User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Ecuador

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Ecuador

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025

Informal Cooperation
2016 NA | 2020 | 2025

STANDARDS AND TECHNOLOGIES

Ecuador

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

El Salvador

El Salvador has undertaken efforts to enhance cybersecurity as part of its Digital Agenda 2020-2030, aiming to integrate public and private sectors into a secure digital environment that fosters national development through innovation and the application of ICT[144]. The nation is actively developing a National Cybersecurity Strategy, focusing on protecting digital state information by adopting international standards and establishing strong, cooperative inter-agency coordination.

Through the 2024 Cybersecurity and Information Security Law, El Salvador has established the State Cybersecurity Agency (ACE, by its acronym in Spanish), which is responsible for implementing cybersecurity policies across public sector institutions, as well as creating and maintaining a National Registry of Cybersecurity Threats and Incidents. The ACE is also tasked with formulating national cybersecurity and information security guidelines, standardizing protocols, and aligning regulations to ensure consistency and security across government entities and critical infrastructure operators [145].

Furthermore, El Salvador is implementing sector-specific Security Operations Centers (SOC) to manage and respond to threats in sensitive sectors. Its E-Government data center and SOC will be established through technical and financial support from the IDB[146], and in 2023, El Salvador became the first Central American country to establish a specialized SOC for the financial sector, underscoring the government's commitment to cybersecurity [147]. Additionally, efforts to manage the .SV domain have been bolstered to enhance the security of state portals, and comprehensive cybersecurity training has been implemented for public sector employees to ensure digital competence and preparedness for cyber incidents [148].

El Salvador is a member of the EU-LAC Digital Alliance, a bi-regional initiative aimed at fostering digital transformation and innovation[149]. The country also joined the Latin America and Caribbean Cyber Competence Centre (LAC4)[150], enhancing its cybersecurity capacities through collaboration with EU CyberNet and other international partners.

In 2023, the government also launched a nationwide cybersecurity awareness campaign, reaching over 500,000 citizens. The campaign succeeded in increasing public awareness and reporting of cyber fraud by 30%, reflecting an enhanced public understanding of the dangers of cyber threats and scams. Despite challenges posed by high levels of digital illiteracy, this campaign marked a significant step toward building a digitally informed society[151].

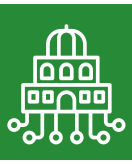
The Salvadoran government has prioritized public-private collaboration to foster cybersecurity resilience across multiple sectors. In partnership with global technology leader Cisco, the government has organized cybersecurity training sessions for public sector IT teams, aiming to enhance their skills in asset protection and cyber risk mitigation[152].

Moreover, in 2024, El Salvador expanded cybersecurity training programs targeting small and medium enterprises (SMEs), a sector identified as particularly vulnerable to cyberattacks. Over 1,200 SMEs have received cybersecurity training, with an impressive adoption rate of 85% for secure cyber practices. The government also promotes specialized educational programs, scholarships, and initiatives aimed at bridging the cybersecurity skills gap and raising awareness among professionals and the general public about cyber risks[153]. Another example for the growing cybersecurity ecosystem in El Salvador is a Public-Private Partnership led by Numu S.A. and financed by the EU and IDB Lab, called "CYBERLAMARR" which will train cybersecurity professionals with an emphasis on improving the participation of young people and women in the sector and provide services to SMEs in the country and the region [154].

El Salvador has taken notable steps to establish a strong legal framework for cybersecurity. In 2024, two key laws were approved: the Cybersecurity and Information Security Law (Decree No. 143) and the Personal Data Protection Law (Decree No. 144). The Cybersecurity and Information Security Law introduces a framework for cybersecurity policies that applies to all government entities, including autonomous bodies and municipalities. It includes specific sanctions for public sector officials who fail to implement adequate security measures, underscoring the importance of compliance.

The Personal Data Protection Law establishes standards to safeguard citizens' data and aligns El Salvador with international regulations on data privacy, ensuring that personal information is secure and responsibly managed. The ACE oversees this law, granting the agency authority to implement sanctions for non-compliance, including fines and dismissal for severe violations. Together, these legislative efforts signify a comprehensive approach to data protection and cybersecurity, reinforcing El Salvador's commitment to secure data management practices in the digital age.

As part of its commitment to digital transformation, El Salvador is advancing E-Government initiatives that streamline and secure public services through technology. Executive Order No. 163, published on May 13, 2022, set forth the Cybersecurity Policy of El Salvador, a framework that outlines critical objectives, such as developing cybersecurity capabilities to safeguard critical infrastructure, enhancing response mechanisms, and promoting cybersecurity awareness among citizens. The policy also promotes international collaboration and encourages both public and private entities to assess risks regularly as part of a proactive cybersecurity strategy[155].



CYBERSECURITY POLICY AND STRATEGY

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | **2025**

Content
2016 | 2020 | **2025**

Implementation and Review
2016 NA | 2020 NA | **2025**

International Engagement
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | **2025**

Organization
2016 | 2020 | **2025**

Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | **2025**

Coordination
2016 | 2020 | **2025** NA

Mode of Operation
2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | **2025**

Regulatory Requirements
2016 NA | 2020 NA | **2025**

Operational Practice
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

Risk Management and Response
2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | **2025**

Defense Force Cyber Capability
2016 NA | 2020 NA | **2025**

Civil-Defense Coordination
2016 NA | 2020 NA | **2025**

Organization
2016 | 2020 | **2025** NA

Coordination
2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

El Salvador

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

El Salvador

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Grenada

Grenada has taken important steps to enhance its cybersecurity capabilities through the establishment of the national Cybersecurity Incident Response Team (CSIRT)[xxxiv]. This team plays a crucial role in protecting the country's digital infrastructure and responding to cyber threats. The CSIRT offers several key services that contribute to controlling cybersecurity risks, including information sharing, cybersecurity awareness, incident management, and cyber threat intelligence. The country has not yet formulated a national cybersecurity strategy.

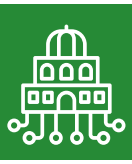
To promote a cybersecurity-aware culture among its citizens, Grenada has implemented various initiatives. The national CSIRT leads cybersecurity awareness programs aimed at constituents, stakeholders, strategic partners, and the general public about cybercrime and cybersecurity. The country has also launched the "Get Safe Online Grenada" platform[xxxv], funded through the UK Commonwealth Cybersecurity Programme. This platform includes a dedicated "Safeguarding Children" section that addresses issues such as cyberbullying and cyberstalking, demonstrating a focus on protecting vulnerable groups. Additionally, the platform provides general information on data privacy and online safety, contributing to the overall cybersecurity literacy of the population.

Grenada actively participates in key regional digital and cybersecurity initiatives. It is a member of the EU-LAC Digital Alliance, supporting efforts toward a human-centric digital transformation[156]. Grenada also engages with the Latin America and Caribbean Cyber Competence Centre (LAC4), notably through programs like the Women in CyberTech Camp@LAC4, aimed at strengthening cybersecurity skills in the Caribbea[157]. Additionally, as a full member of the Caribbean Community (CARICOM)[158], Grenada actively participates in CARICOM IMPACS, the agency responsible for coordinating regional security efforts.

Grenada has established a comprehensive legal framework to address cybersecurity challenges. The Electronic Crimes Act of 2013 (amended in 2014)[xxxvi] provides a robust legal basis for combating cybercrime, covering various offenses including unauthorized access, computer-related fraud, and malicious communication. The country has also enacted the Data Protection Act (No. 1 of 2023)[xxxvii], which aims to promote the protection of personal data processed by public and private bodies and establishes the functions of an Information Commission.

In addition to these specific cybersecurity laws, Grenada has other relevant legislation that supports its cybersecurity framework. These include the Electronic Evidence Act (2013), which facilitates the admission of electronic records into legal proceedings, and the Interception of Communication Act (2013, amended in 2014), which contains provisions for the disclosure of stored communication data. The country's legal framework also addresses international cooperation through the Mutual Legal Assistance in Criminal Matters Act (2001), which provides for mutual legal assistance in criminal matters between Grenada and designated countries.

The CSIRT's incident management service focuses on minimizing the impact of cyber incidents through coordinated detection, triage, analysis, response, and recovery activities. Additionally, the cyber threat intelligence service involves gathering and analyzing information to identify potential cyber threats, recurring patterns, and advise on countermeasures. Through its information sharing service, the CSIRT proactively provides constituents and stakeholders with comprehensive reports and general information on improving cyber resilience. This helps in addressing existing threats, zero-day vulnerabilities, and predicted intelligence sources, further strengthening Grenada's overall cybersecurity posture[159].



CYBERSECURITY POLICY AND STRATEGY

Grenada

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Grenada

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Grenada

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Grenada

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Grenada

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 NA | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Guatemala

Guatemala continues to advance its cybersecurity strategy throughout 2024 and beyond, emphasizing interagency coordination and stakeholder involvement across public and private sectors. The National Cybersecurity Committee (CONCIBER), stablished through Governmental Agreement 200-2021 and managed by the Ministry of Governance, is responsible for evaluating risks, establishing cybersecurity policies, and conducting regular assessments of the country's cyber resilience. This committee also collaborates with international organizations, such as the Organization of American States (OAS), to enhance Guatemala's defensive capabilities through knowledge sharing and training[160].

The 2024-2028 Government Policy highlights the central role of cybersecurity in national development, integrating it with the National Digital Agenda and the National Agenda of Threats and Risks (ANRA, by its acronym in Spanish). These agendas prioritize cybersecurity in areas such as digital transformation, economic growth, and risk management, viewing a robust cybersecurity framework as essential to achieving Guatemala's digitalization and social inclusion goals[161]. One recent example is the Ministry of Finance's initiative to strengthen its cybersecurity, with technical and financial support from the IADB.

Moreover, Guatemala's engagement in the upcoming regional technical cooperation project titled "Strengthening Sectoral Cybersecurity in Latin America and the Caribbean (LAC)" with the Inter-American Development Bank (IADB) will enable the government to assess critical infrastructure vulnerabilities and provide recommendations on best practices for cybersecurity in essential sectors, particularly in finance and energy. This agreement also aims to strengthen the Government CSIRT (CSIRT-GT), which is actively working with ministries to develop real-time threat detection capabilities and establish a unified incident response protocol[162]. Guatemala has also been one of more than 140 countries that have joined ITU-IMPACT[163] and has participated in GLACY+ (Global Action on Cybercrime Extended)[164]. Additionally, Guatemala became member of the Latin American and Caribbean Cyber Competence Centre (LAC4)[165] and is an active member of the EU-LAC Digital Alliance, a bi-regional initiative aimed at fostering digital transformation and innovation[166].

The Ministry of Governance has made cybersecurity education a priority across various sectors, conducting workshops and providing resources to government employees on recognizing phishing attacks, password security, and safe online practices. In partnership with the telecommunications sector, initiatives like "Navega Seguro" offer guidance on secure internet usage, targeting young users and parents to reduce exposure to online risks.

In the financial sector, BanCERT has become an instrumental body in combating cyber fraud by gathering information on cyber threats and sharing it among its networks. Telecommunications companies, recognizing the growing risks, have developed sector-specific incident response teams to prevent disruptions and safeguard consumer data. However, despite these advancements, a nationwide cybersecurity awareness campaign is still lacking. Most citizens remain unaware of best practices for online safety, and digital literacy levels need further improvement to keep pace with technological adoption.

Guatemala has made notable progress in cybersecurity education through coordinated efforts among civil society, academia, and the public sector. Organizations like the Internet Society Guatemala Chapter and Fundación Guatemala Segura raise public awareness by offering workshops and targeted training for vulnerable populations, in partnership with universities such as Universidad del Valle de Guatemala.

Academic institutions including Universidad Galileo, Universidad Mariano Gálvez, and Universidad Internaciones now offer master's programs in cybersecurity management, while the Ministry of Education and INTECAP provide foundational certifications. Meanwhile, the National Institute of Strategic Security Studies (INEES) strengthens public sector capacity with courses in risk management, cyber defense, and incident response, incorporating cybersecurity and digital strategy into its national training agenda. In 2024, Guatemala continues to work towards enacting cybersecurity legislation. A comprehensive Cybersecurity Bill is under consideration, while the Cybercrime Bill, Initiative N° 5.254 de 2017, remains under legislative review, with provisions that address offenses like unauthorized access, digital fraud, and data breaches. The bill also includes measures for protecting minors online, and its passage would align Guatemala's legal framework more closely with international cybercrime standards. Additionally, a separate data protection bill is anticipated, aiming to introduce robust data security requirements for public and private sector databases[167].

Law Enforcement agencies, including the National Police, coordinate with the National Cybersecurity Committee to handle reported cyber incidents. The government is also preparing for Guatemala's potential accession to the Budapest Convention, which would further strengthen its legal structure against cyber threats [168].

In the absence of a unified national cybersecurity standard, the Guatemalan financial sector adheres to technology risk management guidelines established under JM-104-2021, enforced by the Bank of Guatemala. These guidelines require financial institutions to implement risk mitigation strategies, periodic assessments, and cybersecurity training for personnel. Meanwhile, the Ministry of Governance has begun to encourage the adoption of NIST standards within public institutions, aiming to improve security controls across government agencies. Although critical infrastructure sectors are encouraged to adopt best practices, there is no regulatory requirement mandating such practices, resulting in varying degrees of implementation [169].

CYBERSECURITY CULTURE AND SOCIETY

Guatemala

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Guatemala

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Guatemala

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

Guatemala

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 NA | 2020 NA | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Guyana

Guyana has developed a National Cybersecurity Policy Framework to strengthen its digital security posture, especially given its rapid technological growth and expanding oil sector. Launched by the National Data Management Authority (NDMA) in 2024, the framework consists of 43 policies aimed at protecting government information systems, enhancing incident response, and promoting collaboration across agencies. This initiative supports Guyana's goals to modernize public services, safeguard critical infrastructure, and mitigate risks associated with increasing cyber threats[170].

Guyana has also increased its international engagement in cybersecurity by building upon its existing relationships with worldwide organizations. Examples of this include its collaboration with the IDB, whose initiative aims at supporting Guyana's digital transformation and infrastructure development, which can contribute to strengthening cybersecurity measures alongside other aspects of technological modernization in its 2023–2026 Country Strategy. Correspondingly, the OAS has partnered with the U.S. Department of Justice to offer specialized technical assistance, helping Guyana bolster its cybersecurity defenses and providing expertise in tackling cyber threats and managing data security across critical sectors[171] .

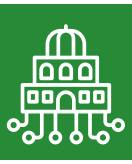
In terms of incident response to a rise in cyberattacks, The Guyana National Computer Incident Response Team (GNCIRT), also known as CIRT.GY, was established in 2013 following a cabinet decision to strengthen the country's cybersecurity posture. Initially operating under the Ministry of Home Affairs, it is now part of the NDMA under the Office of the Prime Minister. CIRT.GY focuses on responding to and managing cybersecurity incidents, providing technical expertise in incident remediation, and raising public awareness about cyber threats. It also collaborates internationally to enhance cybersecurity globally, offering incident response services, alerts, and advisories through its website[172]. Guyana participates in key regional cybersecurity initiatives, including the EU-LAC Digital Alliance, where it benefits from cooperation on digital policy, data protection, and secure public services[173]. It also engages with LAC4 to strengthen national cybersecurity capacities through training in incident response and cyber risk management[174]. As a founding member of CARICOM, Guyana contributes to CARICOM IMPACS initiatives aimed at enhancing regional digital and cybercrime response capabilities[175].

To increase the standards and reduce the vulnerabilities identified in the Critical National Infrastructure (CNI) the government has been increasingly emphasizing the protection of CNI from cyber threats, recognizing cybersecurity as crucial for the nation's digital resilience. As part of its strategy, the government has been working to improve the security framework for CNI sectors, such as energy, transportation, and telecommunications, particularly as the country embraces digital technologies for economic development. Notable initiatives include the National Cyber Risk Assessment (NCRA) workshop, facilitated by the UK, which aims to strengthen cyber resilience in critical infrastructure sectors by providing relevant skills and protection from potential cyberattacks[176].

Throughout 2023 Guyana has worked to close some legislative gaps such as enhancing its digital ecosystem through the ICT Master Plan 2030, which addresses cybersecurity, along with its expanding focus on the use of technology across sectors like healthcare and education. Additionally, local initiatives and regulations, including the Data Protection Bill and efforts to address cybercrime, are central to the country's commitment to secure data management and robust cybersecurity infrastructure[177]. There is a concerted effort by the Guyanese government to update the Cybercrime Act to align with international standards and address these concerns. This effort includes consultations with global experts and participation in the development of a model Cybercrime Bill through the United Nations[178].

Cybersecurity awareness has generally improved in the country. The NDMA possesses training programs that target both IT specialists and general government staff, covering topics such as risk assessment, phishing prevention, and malware detection, to build a foundation of cybersecurity knowledge within public administration. Additionally, the NDMA has been actively promoting safe online practices through its "Cybersecurity Awareness Road Show," which focuses on educating young people in schools across the country. This program reached over 1,100 students from various secondary schools, covering essential topics such as protecting personal information, identifying cyber threats, and managing online privacy risks.

At the Cybersecurity Awareness Month, held on October 2024, the government called for collective responsibility, urging not only government entities but also businesses and the general public to take active steps in securing the nation's digital environment[179]. Likewise, Guyana recently launched the National Defence Institute (NDI) to educate joint services officers and their civilian counterparts through a curriculum focused on defense, security, and development, delivered in a civil-military context. The program aims to better equip participants to assume mid to senior-level operational and strategic roles within their respective organizations[180].



CYBERSECURITY POLICY AND STRATEGY

Guyana

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Guyana

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Guyana

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Guyana

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Guyana

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Haiti

Haiti's cybersecurity policy and strategy development is in its early stages, with considerable room for improvement. The country lacks a comprehensive national cybersecurity strategy, which has hindered its ability to effectively address digital security challenges. However, Haiti has demonstrated commitment to address public sector management and digital government challenges. The country has received support to strengthen its digital transformation efforts, including cybersecurity initiatives, from the international community. Through the Program to Strengthen the Foundations of Digital Transformation of Public Management to Improve Government Effectiveness[xxxviii], supported by the IDB, Haiti will enhance its capacity to monitor and manage public sector cybersecurity, developing governance structures and the ability to protect, monitor, detect, respond to, and recover from cybersecurity incidents. Haiti actively engages in regional cybersecurity cooperation through Latin America and Caribbean Cyber Competence Centre (LAC4), and CARICOM IMPACS. As part of LAC4, Haiti benefits from training and support in areas such as incident response and cybersecurity strategy development[181]. As a CARICOM member, Haiti also takes part in CARICOM IMPACS programs; for example, it joined Regional In-Country Cyber Awareness and Cybersecurity Sensitization and Training[182].

Haiti faces significant challenges in fostering a responsible cybersecurity culture. The country misses comprehensive public awareness campaigns and educational initiatives focused on promoting cybersecurity hygiene and literacy among the general population. However, the Digital Observatory[xxxix] supports the local ecosystem and decision-making processes to prepare society for digital revolutions. Its educational materials, practical guides, and newsletters on cybersecurity are noteworthy contributions to raising awareness.

In a similar manner, the legal and regulatory landscape for cybersecurity in Haiti is currently underdeveloped. The country lacks comprehensive laws and policies related to data protection, digital rights, cybercrime, and critical infrastructure security. This legislative gap leaves Haiti vulnerable to cyber threats and ill-equipped to address cybercrime effectively. The absence of a robust legal framework also hinders the country's ability to participate fully in international cybersecurity cooperation efforts. This regulatory vacuum poses significant challenges for Haiti in establishing a secure and resilient digital environment.

Haiti's approach to controlling cybersecurity risks through standards and technologies can also be considered embryonic. The country has a notable lack of national standards for cybersecurity to guide organizations in risk assessment, incident response, and data protection. This absence of standardized practice leaves critical sectors vulnerable to cyberattacks and hinders the development of a cohesive national cybersecurity posture. Haiti does not yet have a public sector Cybersecurity Incident Response Team (CSIRT) established to protect, monitor, detect, respond to, and recover from cybersecurity incidents, however, one will be established under the abovementioned IDB project. In this same regard, an initiative[xl] in conjunction with the International Telecommunication Union (ITU) to assess the resilience of telecommunications networks and infrastructure in the country is another noteworthy step[183].

CYBERSECURITY POLICY AND STRATEGY

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | 2025
Content
2016 | 2020 | 2025
Implementation and Review
2016 NA | 2020 NA | 2025
International Engagement
2016 NA | 2020 NA | 2025
Organization
2016 | 2020 | 2025 NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | 2025
Organization
2016 | 2020 | 2025
Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | 2025
Coordination
2016 | 2020 | 2025 NA
Mode of Operation
2016 NA | 2020 | 2025 NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | 2025
Regulatory Requirements
2016 NA | 2020 NA | 2025
Operational Practice
2016 NA | 2020 NA | 2025
Organization
2016 | 2020 | 2025 NA
Risk Management and Response
2016 | 2020 | 2025 NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | 2025
Defense Force Cyber Capability
2016 NA | 2020 NA | 2025
Civil-Defense Coordination
2016 NA | 2020 NA | 2025
Organization
2016 NA | 2020 NA | 2025 NA
Coordination
2016 NA | 2020 NA | 2025 NA

CYBERSECURITY CULTURE AND SOCIETY

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025
Priority of Security
2016 NA | 2020 NA | 2025
Practices
2016 NA | 2020 NA | 2025
Government
2016 | 2020 | 2025 NA
Private Sector
2016 | 2020 | 2025 NA
Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025
User Trust and Confidence in Online Search and Information
2016 | 2020 | 2025
Disinformation
2016 NA | 2020 NA | 2025
User Trust in E-Government Services
2016 | 2020 | 2025
User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Haiti

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Haiti

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 NA | 2020 NA | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025**

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025**

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Honduras

Honduras is in the development process of its national cybersecurity strategy, that is expected for 2025. The recently introduced National Digital Government Plan 2023-2026[xli] aims to bridge the digital divide and kickstart a growing creative economy. This plan outlines several cybersecurity initiatives to be implemented during its tenure, including issuing a National Cybersecurity Strategy, formulating and approving data protection legislation and regulations, drafting and passing a cybersecurity law, and establishing and operationalizing a cybersecurity expert team.

Honduras actively engages in regional cybersecurity initiatives through its participation in the EU-LAC Digital Alliance and as a member of the LAC4 network. Within the EU-LAC Digital Alliance, the country contributes to bi-regional efforts aimed at promoting secure digital transformation, data protection, and resilient public services[184]. Precisely under the support of LAC4, Honduras has received technical assistance for the development of its first National Cybersecurity Strategy, adopting a multi-stakeholder approach through a dedicated workshop focused on international best practices and governance frameworks[185].

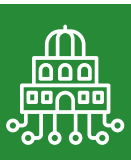
One of the main challenges Honduras faces is fostering a cybersecurity-aware culture, largely due to low digital literacy rates. The country has acknowledged the need to raise awareness about the risks associated with information technology use. To address this, the National Digital Government Plan 2023-2026 includes initiatives for digital inclusion and skills development.

These initiatives, led by the Results-Based Management Directorate (DIGER) of the Presidency of the Republic, are accompanied, among other initiatives, by the investment program with the IDB "Digital Transformation for Greater Competitiveness[186]" for a total of USD 49 million. There have been advances in specific sectors, such as the financial sector, thanks to regulations issued by the National Banking and Insurance Commission (CNBS) regarding information technology management and cybersecurity for this sector[187].

In the private sector, the Honduran Association of Banking Institutions (AHIBA) has launched several cybersecurity awareness campaigns. CONATEL has also contributed by organizing a cybersecurity course for the Mesoamerica Project region[xliii].

Honduras is still in the early stages of building cybersecurity expertise. However, several educational institutions have begun offering online courses and diplomas in this field: Universidad Politécnica Innovación provides a Diploma in Cybersecurity for IT professionals, system administrators, and individuals interested in enhancing their information protection knowledge[xliv]. Universidad Nacional Autónoma de Honduras offers a Cybersecurity for SMEs course, targeting young business owners, managers, and decision-makers[xlv]. Universidad de Defensa de Honduras has a Diploma in Cyberdefense and Cybersecurity for both civilian and military professionals[xlvi]. Universidad Tecnológica de Honduras runs a Cybercrime in Financial Institutions Course, designed for IT professionals in banking and others looking to update their knowledge in this area[xlvii].

On the legal front, Honduras has made some progress. Decree 130-2017, which contains the Penal Code (Title XXII: "Security of Networks and Computer Systems")[xlviii], defines various technology-related crimes. These include computer fraud, child pornography (including grooming and sexting), rape, and disclosure of secrets. The country's criminal procedure code[xlix] establishes procedures and measures for investigating all crimes, including cybercrimes. However, Honduras still lacks specific provisions for handling electronic evidence in its Criminal Procedure Code. This gap suggests that while the country has made strides in criminalizing cyber offenses, effectively prosecuting these crimes may prove challenging due to procedural limitations[188].



CYBERSECURITY
POLICY AND STRATEGY

Honduras

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | **2025**
Content
2016 | 2020 | **2025**
Implementation and Review
2016 NA | 2020 NA | **2025**
International Engagement
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | **2025**
Organization
2016 | 2020 | **2025**
Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | **2025**
Coordination
2016 | 2020 | **2025** NA
Mode of Operation
2016 | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | **2025**
Regulatory Requirements
2016 NA | 2020 NA | **2025**
Operational Practice
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA
Risk Management and Response
2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | **2025**
Defense Force Cyber Capability
2016 NA | 2020 NA | **2025**
Civil-Defense Coordination
2016 NA | 2020 NA | **2025**
Organization
2016 | 2020 | **2025** NA
Coordination
2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Honduras

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Honduras

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Jamaica

Jamaica published its first comprehensive National Cybersecurity Strategy in 2015, aiming to fortify cybersecurity by improving public and private sector protections, expanding public awareness, and establishing a resilient cyberspace for Jamaica's citizens and businesses. Key goals included enhancing cyber infrastructure, developing cybersecurity legislation, and fostering collaboration across government, academia, and private sectors. The strategy also prioritized setting up a Cyber Incident Response Team (JaCIRT), which began monitoring cyber threats and guiding responses to incidents, especially in critical infrastructure. JaCIRT operates under the Ministry of Science, Energy, Telecommunications, and Transport, providing technical cybersecurity responses.

Although a new cybersecurity strategy has not yet been published, the Jamaican government is actively implementing initiatives to strengthen its cybersecurity framework. In August 2022, the National Security Council received an update on the technical and operational implementation of a new Cybersecurity Strategy, indicating ongoing efforts to address cybersecurity challenges and leverage opportunities in cyberspace[189].

In 2023, additionally, the government proposed an additional National Cybersecurity Authority to integrate policy, compliance, and incident management functions, supported by funding from the U.S. government and the Inter-American Development Bank[190]. This entity, expected within 2–4 years, would bring JaCIRT under its oversight, aiming to unify cyber governance, develop training programs, and enhance Jamaica's overall cybersecurity capacity[191].

Jamaica participates in key regional cybersecurity initiatives, including the EU-LAC Digital Alliance[192], benefits from LAC4's cyber capacity-building programs[193] and contributes to CARICOM IMPACS efforts to strengthen national cybersecurity infrastructure[194].

Budget allocations for cybersecurity capacity building have been substantial, with initiatives like the Cybersecurity Strengthening Project, developed with the IDB, enhancing technical capacity and workforce training for handling cyber threats. This includes collaborations with regional partners, such as CARICOM IMPACTS, to access international training and intelligence-sharing resources[195].

In terms of legislative updates, Jamaica, instituted in 2015 a Cybercrimes Act[196], which revised initial 2010 Cybercrime legislation, laid the groundwork for prosecuting cybercrimes, including unauthorized computer access, cyber fraud, and data theft. The Act has been updated to address evolving threats, with amendments in 2021 and 2023 adding new offenses, such as cyberbullying, and increasing penalties to deter malicious communications[197,198].

Recent proposals, influenced by the Ministry of National Security and other stakeholders, emphasize stricter penalties for crimes impacting minors and broader protection for individuals facing reputational harm online. These proposals build upon the 2020 Data Protection Act[199,200]. The amendments reflect Jamaica's commitment to evolving its cybersecurity laws in response to digital advances and growing cyber threat[201].

There have been advances in specific sectors, such as the financial sector. In Jamaica, the Financial System Stability Committee (FSSC) established 10 Cyber Resilience Principles for the financial sector. These principles aim to enhance board-level oversight of cyber risks, strengthen cybersecurity preparedness, and promote collaboration among regulated entities to ensure the stability of the financial system[202].

In recent years, Jamaica has prioritized developing its E-Government services in an aim to modernize public administration by providing accessible, efficient, and transparent digital platforms for citizens and businesses. Core systems include the Gov.jm portal, a centralized hub for government services, and the Tax Administration Jamaica (TAJ) platform[203], which simplifies tax filing and payments. Other key platforms, such as the National Land Agency's eLandJamaica[204], streamline trade processes and property-related services. Significant advancements in education, health, and justice sectors include e-learning resources, digital health records, and electronic case management systems[205]. Major initiatives like the National Identification System (NIDS, supported by the IDB[206]) aim to create a unified ID framework for seamless access to government services[207]. However, challenges such as rural digital infrastructure gaps, cybersecurity threats, and digital literacy disparities remain barriers to full adoption. These efforts reflect Jamaica's commitment to fostering an inclusive, tech-driven governance model.

To enhance cybersecurity training and awareness, the Jamaican government has benefited from training and skills development through partnerships with organizations such as the Organization of American States (OAS) and the E-Governance Academy of Estonia[208]. Other initiatives, such as those led by the Jamaica Technology & Digital Alliance (JTDA) launched the "Jamaica Cyber Skills Initiative" with the goal of providing cybersecurity training to individuals, enhancing the country's cyber resilience and contributing to economic growth in the digital era[209].

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Jamaica

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Jamaica

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025**

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Mexico

On September 6, 2021, Mexico introduced a National Digital Strategy as part of the broader objectives of the 2019-2024 National Development Plan, building upon the foundations laid in the 2013–2018 plan. This strategy prioritizes "increasing the digitalization of Mexico" by promoting the deployment and expansion of telecommunications infrastructure and fostering the adoption and use of information and communication technologies (ICTs) to benefit society. A key aspect is transforming the relationship between citizens and government, emphasizing user-centric public services enabled through ICTs. Beyond enhancing connectivity, the strategy addresses specific cybersecurity risks and integrates efforts from government, the private sector, and civil society to promote responsible ICT use, innovation, and technological development. This aligns with Mexico's National Cybersecurity Strategy (NCS) introduced in 2017, showcasing a commitment to building a safer, more inclusive digital ecosystem that supports economic growth, social inclusion, and resilience against emerging cyber threats.

Mexico is a participating country in the EU-LAC Digital Alliance, a bi-regional initiative aimed at fostering inclusive and human-centric digital transformation. The alliance promotes cooperation on digital policy, data protection, and secure public services[210].

In early 2025, the Digital Transformation and Telecommunications Agency (ATDT, by its acronym in Spanish) was established, assuming several responsibilities for Mexican cybersecurity policies. The national Inter-Ministerial Commission on Information and Communication Technologies and Information Security (CITICSI, by its acronym in Spanish)[211] established in 2023, coordinates the implementation of federal cybersecurity policies across public administration. Mexico also boasts the CERT-MX (National Cyber Incident Response Center)[212], managed by the National Guard, which acts as the primary point of contact for national and international cybersecurity incident coordination.

The government actively promotes cybersecurity awareness through nationwide campaigns such as the National Cybersecurity Week, which includes workshops on incident management based on the Standardized National Protocol for Cyber Incident Management[213]. Mexico has also participated in the FIRST initiative, aligning itself with the regional trend of improving and coordinating its capabilities.

Awareness is also extended to children and families, with resources such as Parental Guides[214] and recommendations for safe internet use, promoted through events and campaigns organized by entities such as the National Guard and the Secretariat of Security and Citizen Protection (SSPC, by its acronym in Spanish). Notable initiatives include the annual National Cybersecurity Campaign "Safe Internet for All" and the aforementioned National Cybersecurity Weeks, which in their most recent editions have promoted sound cybersecurity practices with nationwide reach and high impact[215]. Reports from the Federal Telecommunications Institute (IFT, by its acronym in Spanish) offer insights into public perceptions of cybersecurity risks[216] Moreover, the Private Sector also contributes with initiatives like the Cybersecurity Tips and Guidelines[217] published by CERT-MX, which target both citizens, organizations and business.

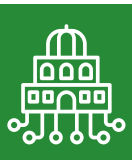
Mexico has invested in public-private partnerships to bolster cybersecurity skills. The IFT's 2023 report highlights the participation of SMEs in cybersecurity training programs and emphasizes the need for advanced ICT knowledge[218]. Several higher education institutions now offer accredited cybersecurity programs, although efforts to expand access and resources for specialized training remain ongoing. Additionally, initiatives such as the Mexico CyberSecure Alliance (AMCS, by its acronym in Spanish) have emerged to strengthen collaboration among stakeholders from various sectors and disciplines. This collaborative effort aims to contribute to the improvement of cybersecurity through a collective approach[219].

Mexico is making progress in strengthening its legal and institutional framework for addressing cybercrime and protecting online rights. As of 2024, the Mexican Congress had been debating comprehensive cybersecurity legislation proposals, and efforts are underway to adapt general criminal procedural laws to meet the specific needs of cybercrime investigations. Data protection is a priority, supported by stakeholder consultations, with key frameworks such as the Federal Law on the Protection of Personal Data Held by Individuals (LFPDPPP, by its acronym in Spanish) and the General Law on the Protection of Personal Data in Possession of Obliged Subjects (LGPDPPSO, by its acronym in Spanish) providing a foundation for broader implementation. Important strides are also being made to address specific online risks, such as the adaptation of the General Law on the Rights of Children and Adolescents (LGDNNA, by its acronym in Spanish) to better protect children in digital environments and the enforcement of intellectual property rights under the Federal Law on the Protection of Industrial Property (LFPPI, by its acronym in Spanish).

Institutionally, Mexico has significant opportunities to build on its existing capabilities. While digital forensic resources like the CIBERCOM-AM Digital Forensics Laboratory demonstrate technical capacity, greater standardization and institutionalization are needed to ensure consistent results. Training for Law Enforcement and judiciary personnel on digital evidence and cybercrime remains ad hoc, but these gaps highlight the potential for more structured programs. Internationally, while Mexico's participation in global networks like the G8 24/7 or Global Prosecutors E-Crime Network (GPEN) GPEN is limited, its ongoing consultations with stakeholders to develop cross-sectoral cybersecurity regulation signal a promising direction. Similarly, Mexico holds the forenamed National Cybersecurity Week, featuring workshops and drills for incident response processes, where different sectors of society coordinate their efforts.

Mexico has made strides in adopting international cybersecurity standards, such as the NIST Cybersecurity Framework[220] and ISO/IEC 27001[221], with a voluntary implementation. Mexico has further guidance in this topic in documents like the Federal Telecommunications Institute´s "Code of Best Practices for Cybesecurity of IoT Devices"[222].

Mexico shows its efforts to digitize10 the government services11 providing identification, health, and visa services, among others. These digitalization efforts will be driven by the ATDT, which aims to digitalize 80% of administrative procedures and reduce waiting times by 50%, supported by a constitutional reform[223]. Mexico has also embraced cyber incident simulation exercises, led by CERT-MX, to enhance the resilience of its critical infrastructure, which are the type of activities that align with international best practices and ensure preparedness for emerging threats.



CYBERSECURITY POLICY AND STRATEGY

Mexico

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Mexico

D2

2-1 Cybersecurity Mind-Set

- Awareness of Risks — 2016 NA | 2020 NA | **2025**
- Priority of Security — 2016 NA | 2020 NA | **2025**
- Practices — 2016 NA | 2020 NA | **2025**
- Government — 2016 | 2020 | **2025** NA
- Private Sector — 2016 | 2020 | **2025** NA
- Users — 2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

- Digital Literacy and Skills — 2016 NA | 2020 NA | **2025**
- User Trust and Confidence in Online Search and Information- — 2016 | 2020 | **2025**
- Disinformation — 2016 NA | 2020 NA | **2025**
- User Trust in E-Government Services — 2016 | 2020 | **2025**
- User Trust in E-commerce Services — 2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

- Personal Information Protection Online — 2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

- Reporting Mechanisms — 2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

- Media and Social Media — 2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025 NA

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

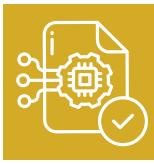
Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA



STANDARDS AND TECHNOLOGIES

Mexico

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Panama

Resolution No. 17, issued on September 10, 2021, by Panama's National Authority for Government Innovation (AIG, by its acronym in Spanish), introduced the country's updated National Cybersecurity Strategy for the 2021–2024 period, following it's first strategy published in 2013. This document formally replaced the previous cybersecurity and critical infrastructure protection strategy established in 2013. The new strategy focuses on strengthening Panama's cybersecurity landscape by addressing emerging cyber threats, enhancing public awareness, building stronger digital defenses, and promoting collaborations with both national and international partners to protect critical information infrastructure[224]. The strategy is built around four main pillars: safeguarding the privacy and fundamental rights of citizens in cyberspace; deterring and prosecuting cybercrime; strengthening the security and resilience of the nation's critical infrastructure; and promoting a national culture of cybersecurity[225].

Panama established a CSIRT in 2011[226], which functions as the country's main response team for cybersecurity incidents affecting government systems and works to mitigate risks for national infrastructure. Following the enactment of Panama's Resolution No. 17, CSIRT Panama was designated with an expanded and formalized role in bolstering the nation's cybersecurity. CSIRT Panama, under the oversight of the AIG, is tasked with addressing cybersecurity incidents, improving cybersecurity awareness, and implementing protocols to safeguard Panama's critical infrastructure[227]; while AIG protects and monitors governmental systems. These efforts are technically and financially supported by IDB's Digital Panama project[228], through which over USD 20 million were made available for national cybersecurity initiatives over several years.

Panama has made notable progress in its E-Government initiatives, aiming to improve the delivery of public services, increase accessibility, and enhance transparency. The government, through the AIG, has implemented a Digital Government Strategy that promotes Online Services such as tax payments, health records, and permits. Panama City has also embraced smart city technologies, such as smart traffic management systems and platforms for citizens to report infrastructure issues. Additionally, Panama is working on a national digital identity system to streamline access to various government services securely. Surveys suggest that trust in digital platforms is growing, but access and digital inclusion remain a key focus. The government continues to work on overcoming these barriers, emphasizing cybersecurity and enhancing digital skills to ensure a more inclusive and secure digital environment[229].

Forensic analysis, making it ideal for those seeking specialized knowledge in combating cybercrime.

Panama has promoted cybersecurity awareness through public-private partnerships and digital campaigns, such as those led by the AIG to foster digital literacy and safe online behavior. These efforts support the country's broader ICT and Digital Agenda goals. The Panamá Cibersegura initiative, launched in 2023, has drawn 13,000 visitors to its website and features content on legislation, internet safety, and digital protection for youth. In 2024, a Cybersecurity Club was launched in schools, training 20 student ambassadors across two schools. Panama has also expanded cybersecurity education through programs at Universidad Tecnológica de Panamá and Universidad de Panamá, offering degrees and technical training in cybersecurity and digital forensics.

In terms of Panama's cybersecurity legislation, it is primarily outlined in the Penal Code (Law 14, 2007), which addresses cybercrime, including unauthorized access to data, systems, and networks. Articles 289 to 292 criminalize activities such as data manipulation, interference, and unlawful interception, with penalties that increase under aggravating circumstances. Additionally, Panama has enacted Law 81 (2019) on personal data protection, which governs how personal data should be processed, stored, and shared. This law mandates consent from individuals for data processing, ensures privacy rights like access and deletion of personal data, and is overseen by the National Authority for Transparency and Access to Information (ANTAI, by its acronym in Spanish)[230]. Additionally, in 2024, Panama's Congress debated an Artificial Intelligence Law, which included cybersecurity aspects.

Panama actively engages in regional cybersecurity efforts through its participation in the EU-LAC Digital Alliance, contributing to bi-regional initiatives aimed at promoting secure digital transformation and data protection frameworks across Latin America and the Caribbean[231]. As a full member of the Latin America and Caribbean Cyber Competence Centre (LAC4), Panama benefits from capacity-building programs that strengthen its cybersecurity capabilities through training in areas such as incident response and strategy implementation[232]. Panama also participates in international partnerships aimed at strengthening cybersecurity, such as Memoranda of Understanding (MoUs) with countries like the United States, Israel, and regional neighbors including Costa Rica, Honduras, and the Dominican Republic. These agreements focus on knowledge exchange, technical assistance, and strengthening national and regional cyber defenses. Furthermore, Panama's participation in global frameworks, such as the 2024 UN Convention against Cybercrime, reinforces its commitment to addressing cyber threats, including child protection and online exploitation.Panama has also been a signatory of the Budapest Convention on Cybercrime since 2013, which supports international cooperation in addressing cybercrimes like data breaches, intellectual property violations, and unauthorized system access.

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | 2025
- Content — 2016 | 2020 | 2025
- Implementation and Review — 2016 NA | 2020 NA | 2025
- International Engagement — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | 2025
- Organization — 2016 | 2020 | 2025
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | 2025
- Coordination — 2016 | 2020 | 2025 NA
- Mode of Operation — 2016 NA | 2020 | 2025 NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | 2025
- Regulatory Requirements — 2016 NA | 2020 NA | 2025
- Operational Practice — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA
- Risk Management and Response — 2016 | 2020 | 2025 NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | 2025
- Defense Force Cyber Capability — 2016 NA | 2020 NA | 2025
- Civil-Defense Coordination — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA
- Coordination — 2016 | 2020 | 2025 NA

CYBERSECURITY CULTURE AND SOCIETY

Panama

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Panama

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Panama

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Panama

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Paraguay

Since 2024, Paraguay is developing an updated National Cybersecurity Strategy for 2024-2028[l] using a multi-stakeholder approach aligned with current public policy instruments and national planning. This new strategy builds on the achievements, objectives, and criteria of the National Cybersecurity Plan 2017-2021[li], which made progress in incident response capacity, training and awareness, protection of critical infrastructure, security in public administration, capacity for investigation and prosecution of cybercrime, and national coordination. The draft of the new strategy articulates a forward-looking vision: by 2028, Paraguay aims to be a country with a safe, resilient and sustainable digital ecosystem, with clear and robust norms, technical capabilities to prevent, detect and respond to cyber threats, and a skilled workforce across public and private sectors. It also aims to reinforce international cooperation, foster digital trust, and promote a culture of shared responsibility among all actors in the ecosystem[233].

The Ministry of Information and Communication Technologies of Paraguay (MITIC) has an investment project financed by the IADB to support the development of the country's Digital[234] which includes the revision of the regulatory framework and the creation of a SOC. Through that project MITIC, is improving its monitoring capabilities with three organizations already integrated into this program. This initiative marks the beginning of a significant expansion, as allocated budget resources will enable the incorporation of enhanced detection tools and the development of a national-level Security Operations Center (SOC), thereby strengthening Paraguay's overall cybersecurity posture.

Likewise, Paraguay has established a comprehensive framework to address cybersecurity challenges, led by the M MITIC. This framework includes a National Cybersecurity Commission[lii] comprising representatives from 32 State Agencies and Entities (OEE), Specialized Subcommittees, Working Groups, a National Cybersecurity Coordinator[liii], and the Cyber Incident Response Center (CERT-PY)[liv]. CERT-PY provides cybersecurity services to prevent, detect, mitigate, and respond to cyber incidents and conducts cyber-attack drills[lv]. The Public Ministry has a Specialized Unit for Computer Crimes to combat technology-related offenses. Additionally, the country has implemented an Information Security Governance Model[lvi], creating information security areas and appointing security officers in all OEEs with well-defined objectives, roles, competencies, and responsibilities.

In a collaborative effort to strengthen national cybersecurity, Paraguay has formalized a Specific Cooperation Agreement between the General Directorate of Information and Communication Technologies of the Armed Forces (DIGETIC/FFAA) and the Ministry of Information and Communication Technologies (MITIC). This agreement aims to enhance cybersecurity capabilities through technical and operational cooperation, focusing on information security and protection, as well as streamlined communication and coordination. Notably, this partnership does not entail any financial commitments between the participating entities. This initiative aligns with Paraguay's broader strategy to fortify its digital infrastructure, complementarily to its ongoing efforts in citizen training, regulatory framework development, and international collaborations, as evidenced by its adherence to the Budapest Convention and its Additional Protocols. Such inter-institutional cooperation underscores Paraguay's commitment to a robust and resilient cybersecurity ecosystem, safeguarding its digital assets against evolving cyber threats."

In terms of its broader international engagements, Paraguay actively participates in the EU-LAC Digital Alliance, contributing to bi-regional initiatives aimed at promoting secure digital transformation and data protection frameworks across Latin America and the Caribbean[235]. Additionally, the country collaborates with the Latin America and Caribbean Cyber Competence Centre (LAC4) to enhance its cybersecurity capabilities through training programs, incident response planning, and policy support[236]. Beyond regional platforms, Paraguay also works closely with international organizations such as the United Nations, the Organization of American States (OAS), and MERCOSUR, and receives technical and financial assistance from multilateral development banks like the Inter-American Development Bank (IDB) to implement its national Digital Agenda. Paraguay also maintains bilateral cooperation on cybersecurity with countries such as the United States[237], Taiwan[238], and the United Arab Emirates[239].

Paraguay is aslo making strides in citizen training and awareness through campaigns like CONECTATE SEGURO PY[lvii], which aims to educate children, youth, and adults about internet dangers and prevent cyberbullying, grooming, sexting, and other crimes. The country is also addressing disinformation challenges[lviii]. Private sector actors, especially in finance and telecommunications, are consistently educating their users on safe and responsible internet use and cybersecurity risk management.

Additionally, in August 2024, the Ministry of Information and Communication Technologies (MITIC) updated the national E-Government guidelines, establishing new standards to optimize processes and procedures across public institutions. The revised guidelines address key areas such as electronic identity, online payments, document management, and digital citizen participation, aiming to enhance efficiency and transparency in public administration.

The country has established foundations for preventing and managing cybersecurity risks and responding to incidents through international agreements and specific laws, decrees, resolutions, regulations, guidelines, and standards. While there are legal norms regulating essential aspects of privacy protection and some personal data, Paraguay lacks a comprehensive regulatory framework for data protection.

Regarding cybercrime legislation, Law No. 4439 defines various criminal behaviors related to information and communication technologies. Paraguay acceded to the Convention on Cybercrime (Budapest Convention) and its Additional Protocol on July 30, 2018, which came into force on November 1, 2018. On September 24, 2024, Paraguay also signed the Second Additional Protocol to the Budapest Convention, aimed at improving cooperation and disclosure of electronic evidence.

Paraguay has developed a technical regulatory framework for cybersecurity risk management, including guidelines for managing official social media accounts, mandatory reporting of cyber incidents by OEEs[lix], a Critical Cybersecurity Controls Guide, and cybersecurity directives for state media. Under the Digital Transformation Strategy Action Plan, the country has enhanced its cyber incident management capacity through CERT-PY and improved cybersecurity information exchange. Services include monitoring and preparing informative bulletins and cybersecurity alerts, conducting security audits for public institutions, providing technical assistance, and analyzing software system vulnerabilities[240].

CYBERSECURITY POLICY AND STRATEGY

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | 2025
- Content — 2016 | 2020 | 2025
- Implementation and Review — 2016 NA | 2020 NA | 2025
- International Engagement — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | 2025
- Organization — 2016 | 2020 | 2025
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | 2025
- Coordination — 2016 | 2020 | 2025 NA
- Mode of Operation — 2016 | 2020 | 2025 NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | 2025
- Regulatory Requirements — 2016 NA | 2020 NA | 2025
- Operational Practice — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA
- Risk Management and Response — 2016 | 2020 | 2025 NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | 2025
- Defense Force Cyber Capability — 2016 NA | 2020 NA | 2025
- Civil-Defense Coordination — 2016 NA | 2020 NA | 2025
- Organization — 2016 | 2020 | 2025 NA
- Coordination — 2016 | 2020 | 2025 NA

CYBERSECURITY CULTURE AND SOCIETY

D2

2-1 Cybersecurity Mind-Set

- Awareness of Risks — 2016 NA | 2020 NA | 2025
- Priority of Security — 2016 NA | 2020 NA | 2025
- Practices — 2016 NA | 2020 NA | 2025
- Government — 2016 | 2020 | 2025 NA
- Private Sector — 2016 | 2020 | 2025 NA
- Users — 2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

- Digital Literacy and Skills — 2016 NA | 2020 NA | 2025
- User Trust and Confidence in Online Search and Information- — 2016 | 2020 | 2025
- Disinformation — 2016 NA | 2020 NA | 2025
- User Trust in E-Government Services — 2016 | 2020 | 2025
- User Trust in E-commerce Services — 2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

- Personal Information Protection Online — 2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

- Reporting Mechanisms — 2016 NA | 2020 | 2025

2-5 Media and Online Platforms

- Media and Social Media — 2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Paraguay

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Paraguay

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Peru

Although Peru does not currently have an independent national cybersecurity strategy document, it is guided by the National Digital Transformation Policy, issued in 2023[241], with digital security as one of its priority objectives.

In 2020, The National Center for Digital Security (CNSD) in Peru was created by the Urgent Decree No. 007-2020, as part of a national strategy to enhance digital security and trust. Functioning under the supervision of the Council of Minister Presidency (PCM), it coordinates, promotes, and oversees the nation's digital security infrastructure, including incident response and national-international collaboration with similar entities. Its creation marked a formal step in strengthening Peru's capacity to address cybersecurity threats comprehensively across public and private sectors, also aligning with international initiatives like CSIRT Américas[242]. Additionally, several public entities have developed their own plans aligned with the national policy, such as the Digital Government Plan of the Central Reserve Bank of Peru (BCRP) for the 2024–2026 period[243]. These plans aim to modernize public administration through the digitalization of processes and services, while strengthening cybersecurity and promoting technological innovation. Law No. 30618, passed in 2017, focused on enhancing the country's intelligence system by strengthening the National Intelligence System (SINA) and modernizing the National Intelligence Directorate (DINI). The law aims to consolidate the country's intelligence capacity, through these two organizations, especially regarding national security, through better inter-agency coordination, advanced digital and cybersecurity protocols, and international intelligence partnerships. It also mandates updates to existing intelligence regulations to improve security operations and protect intelligence personnel's identity in the digital space. Peru has achieved a level of awareness that recognizes the importance of incorporating cybersecurity in its digital initiatives, which can be seen in the PCM's Digital Transformation with Equity projects, the "Digital Transformation of Banco Nación" project, and the Program to Strengthen the Pension Normalization Office (ONP), which include investments of more than USD 30 million for cybersecurity[244].

In collaboration with the IADB, Peru launched the Digital Infrastructure Strengthening Program in 2024, aiming to enhance the IT infrastructure of the public sector, ensure data security, and improve the efficiency of public service delivery. This project includes the establishment of a robust data center to protect the sovereignty and availability of government data[245]. Additionally, IDB collaborates with the Organization of American States (OAS) to address regional cybersecurity challenges by enhancing public institutions' ability to protect critical infrastructure and to combat cyber threats more effectively, a priority identified in the 2020 IADB-OAS Cybersecurity Report[246].

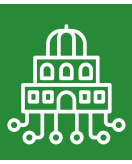
Peru actively participates in the EU-LAC Digital Alliance, contributing to bi-regional initiatives aimed at promoting secure digital transformation and data protection frameworks across Latin America and the Caribbean[247]. Additionally, Peru collaborates with the Latin America and Caribbean Cyber Competence Centre (LAC4) to enhance its cybersecurity capabilities through training, consultations, and technical support on incident response and national risk assessments[248].

In Peru, the approach to Incident Response and Crisis Management for cybersecurity includes the establishment of the National Center for Digital Security, which is part of the broader Digital Government and Transformation Secretariat (SGTD) under the Presidency of the Council of Ministers . This center manages the National Registry of Digital Security Incidents, where incidents are reported by digital service providers to coordinate responses and mitigate threats. One of the central entities that coordinates incident response in the country is the national CSIRT, PeCERT, created in 2009. PeCERT serves as the country's primary organization for managing cybersecurity incidents, promoting coordination among national public administration entities, and setting standards to safeguard public sector IT resources. PeCERT's responsibilities include preventing, detecting, and managing cyber threats, as well as gathering information to address and develop solutions for security challenges. Additionally, PeCERT collaborates with the private sector, particularly Internet Service Providers and banks, to strengthen national cybersecurity efforts and is a member of the CSIRT Americas network[249]. Moreover, the country has introduced laws such as Supreme Decree No. 004-2018-IN, which mandates the protection of national critical assets and implements specific cybersecurity measures for essential sectors such as finance, healthcare, and energy. This framework is designed to integrate private and public resources to safeguard critical systems against cyber threats, aligning with global standards such as the Budapest Convention, which Peru ratified in 2019 to strengthen its legal framework against cybercrime and cyberattacks[250]. Additionally, PeCERT, the national Computer Emergency Response Team, conducts public awareness campaigns and technical training for handling cyber incidents, especially aimed at professionals in critical sectors.

In the private sector, organizations such as ISACA's Lima Chapter and APEPCIT (Peruvian Association of Professionals in Cybersecurity) host regular workshops, certifications, and events like CyberSecPeru, where professionals can further their cybersecurity skills. Various Peruvian companies in finance and telecom, including Banco de Crédito del Perú and Telefónica, also invest heavily in cybersecurity training for their staff to protect sensitive data and networks, contributing to the growing pool of cybersecurity professionals in the country[251,252].

E-Government continues to be an important component of Peru's digital policy. Besides the legislative achievement in this sector with its E-Government Law in 2018[253] one key area of progress is the recent launch of the Gobierno Digital platform, which facilitates online public service access and has led to a significant boost in e-services. Between 2020 and 2023, Peru saw a 30% increase in online interactions with government services, reflecting increased digital literacy and accessibility across the nation. In addition, efforts in open data and transparency have been expanded, allowing Peru to improve its global digital government rankings and ensure more inclusive and streamlined access for citizens and businesses alike. According to the latest 2024 UN E-Government Development Index, Peru has a score of 0.807, ranking 58th globally and placing it within the "very high performance" group among Latin American countries[254].

Regarding legislation, Peru has Law No. 30096 on computer crimes that delivers substantive provisions on computer crime. This law specifically criminalizes online grooming, with penalties for anyone attempting to solicit or exploit minors via digital means. Additionally, the Code of Children and Adolescents mandates that school directors report any cases of abuse, including online exploitation and Law No. 27309 that incorporated computer crime into the country's criminal code. In addition, Peru has Law No. 29733 on the protection of personal data, which applies to both public and private databases.



CYBERSECURITY POLICY AND STRATEGY

Peru

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 | 2020 | **2025**
- International Engagement — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 | 2020 | **2025**
- Coordination — 2016 | 2020 | **2025**
- Mode of Operation — 2016 | 2020 | **2025**

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 | 2020 | **2025**
- Operational Practice — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Risk Management and Response — 2016 | 2020 | **2025**

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 | 2020 | **2025**
- Civil-Defense Coordination — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Coordination — 2016 | 2020 | **2025**

CYBERSECURITY CULTURE AND SOCIETY

Peru

D2

2-1 Cybersecurity Mind-Set

- Awareness of Risks — 2016 NA | 2020 NA | **2025**
- Priority of Security — 2016 NA | 2020 NA | **2025**
- Practices — 2016 NA | 2020 NA | **2025**
- Government — 2016 | 2020 | **2025** NA
- Private Sector — 2016 | 2020 | **2025** NA
- Users — 2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

- Digital Literacy and Skills — 2016 NA | 2020 NA | **2025**
- User Trust and Confidence in Online Search and Information- — 2016 | 2020 | **2025**
- Disinformation — 2016 NA | 2020 NA | **2025**
- User Trust in E-Government Services — 2016 | 2020 | **2025**
- User Trust in E-commerce Services — 2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

- Personal Information Protection Online — 2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

- Reporting Mechanisms — 2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

- Media and Social Media — 2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

Peru

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 NA | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025**

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Saint Kitts and Nevis

Under its National ICT Strategic Plan, Saint Kitts and Nevis has prioritized building a secure digital infrastructure. The plan focuses on five axes, including developing ICT human resources, creating an enabling policy and legal environment, and modernizing government services through electronic delivery. This framework also aims to stimulate economic and social development through public-private partnerships[255].

In terms of cybersecurity, Saint Kitts and Nevis has recently engaged in several regional initiatives. Notably, the country participated in "CyberCrabs 2022," a cybersecurity exercise organized by EU CyberNet and LAC4 in partnership with CARICOM and the OAS, designed to test crisis management protocols across the Caribbean[256]. Additionally, Saint Kitts and Nevis joined the CARICOM Cyber Resilience Strategy 2030, an initiative supported by the U.S. Goverment to strengthen cybersecurity across CARICOM nations, with a focus on building resilience, protecting critical infrastructure, and cultivating a skilled workforce[257]. Recently, the nation has launched the "Cyber Nations Program 2025" in collaboration with Canadian firm Protexxa, focusing on developing a skilled cybersecurity workforce through training and internationally recognized certifications[258].

The government has also made strides toward establishing a National CIRT (Computer Incident Response Team). A National CIRT Assessment is underway, evaluating the country's cybersecurity status and readiness to set up a CIRT through stakeholder engagement, public resources, and the ITU Global Cybersecurity Index.

Saint Kitts and Nevis has taken steps to improve cybersecurity awareness through initiatives like the "Get Safe Online" campaign, funded by the UK Government. This campaign provides free, impartial advice to citizens on protecting themselves from cyber threats, including identity theft and online fraud. It aims to foster a safer online environment by empowering citizens to make informed decisions regarding online activities[259].

In collaboration with the Commonwealth Secretariat, the country is also involved in a five-year Caribbean Electronic Evidence Training project. This program strengthens the legal and institutional framework for combating cybercrime by enhancing the digital evidence capabilities of Law Enforcement officials, prosecutors, and judiciary members across the Commonwealth Caribbean[260].

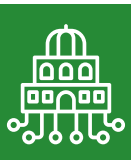
It also participated in the international military cybersecurity exercises, at the Tradewinds 2024 (TW24)[261].

Saint Kitts and Nevis has continued to build cybersecurity knowledge and capabilities with a focus on public and private sector engagement. While in 2020 the country's cybersecurity training initiatives were primarily limited to ISO 31000 risk training for public officials, recent efforts have expanded to include broader capacity-building and skill development.

Saint Kitts and Nevis has enacted robust legislation to address cybercrime. The Electronic Crimes Act No. 27 covers a wide range of offenses, including illegal access, data interference, unauthorized access to restricted systems, and unlawful communications. Additionally, Article 13 addresses child pornography, showing a commitment to safeguarding vulnerable populations.

The nation has also advanced its Data Protection Bill, based on the model from the Organization of Eastern Caribbean States (OECS). This bill ensures that personal information collected by public and private entities remains confidential and used solely for its intended purpose, aligning Saint Kitts and Nevis with international standards for data privacy and protection.

Saint Kitts and Nevis continues to modernize government services under its ICT Strategic Plan, with goals of digitizing administrative processes and delivering services electronically. Through public-private partnerships, the nation is gradually adopting technologies that improve efficiency, security, and accessibility in public services, fostering a more connected and responsive government.



CYBERSECURITY
POLICY AND STRATEGY

Saint Kitts and Nevis

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Saint Kitts and Nevis

D4

4-1 Legal and Regulatory Provisions[15,16]

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security[18]
2016 | 2020 | **2025**

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation[23]
2016 NA | 2020 | **2025**

Child Protection Online[24]
2016 NA | 2020 | **2025**

Consumer Protection Legislation[25]
2016 NA | 2020 | **2025**

Intellectual Property Legislation[26]
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity[27]

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Saint Kitts and Nevis

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Saint Lucia

Saint Lucia's cybersecurity policy landscape includes several foundational laws but lacks a comprehensive national cybersecurity strategy. Key legislation includes the 2018 Computer Misuse Act. This piece of legislation aimed at safeguarding computer systems and data by criminalizing specific cyber activities. Key provisions include penalties for unauthorized access to computer data, interception of computer services, unauthorized modification of data, and computer-related fraud. The Act also covers offenses like unauthorized disclosure of passwords, electronic fraud, and actions that damage or disrupt computer systems[262]. This law builds upon Article 267 of Saint Lucia's Criminal Code (2003), which also targets offenses involving computer fraud and related cybercrimes, further enhancing the legal framework against digital threats. Additionally, Article 330 criminalizes the production and distribution of child pornography, addressing specific digital threats to children[263].

Saint Lucia has not yet established a dedicated website or hotline specifically for reporting cases of child online protection or cyber abuse. However, the country has implemented various child protection measures, such as partnerships and campaigns with UNICEF and CARICOM. Notably, Saint Lucia's "Break the Silence" campaign, initiated by the Division of Human Services, promotes public awareness and reporting of child abuse cases, including online risks to children. These efforts fall under broader child protection strategies rather than a targeted platform for online-specific concerns.

Saint Lucia is working to establish a national Computer Emergency Response Team (CERT) but currently does not have an operational team. The nation has collaborated with international organizations like the International Telecommunication Union (ITU) IMPACT, which aids in aligning cybersecurity policies with international standards and facilitates access to cybersecurity resources and training for public officials[264].

Saint Lucia offers E-Government services through its digital platform, DigiGov. Launched in 2020, DigiGov is a centralized portal that provides citizens, residents, and businesses with access to various public services online, allowing them to apply, pay, and track services. It currently includes services like driver's license renewals, birth and death certificates, business registration, tax registration, passport applications, and more, with plans to expand to 154 services across nine ministries in the future. DigiGov aims to streamline government interactions and improve accessibility for Saint Lucian citizens and residents by offering secure online payments and a user-friendly experience for accessing government services.[265]

National Cybersecurity awareness-raising campaign for society at large, and educational opportunities for Cybersecurity in the country are limited. However, some initiatives involving international partners have been quite impactful. One key initiative is its participation in the Caribbean region's collaborative efforts to combat cybercrime, often through the Organization of American States (OAS)[266] and the Commonwealth. These partnerships enable knowledge sharing, cybersecurity capacity building, and the creation of frameworks for tackling cybercrime collectively across the Caribbean[267]. Another notable projects are the training and capacity-building initiatives with the Council of Europe's Octopus Project, which aims to improve cybersecurity skills and knowledge in judicial and Law Enforcement personnel across the Caribbean. Through this program, Caribbean magistrates and prosecutors, including those from Saint Lucia, receive training in cybercrime legislation, handling electronic evidence, and international cooperation to align with the standards of the Budapest Convention on Cybercrime[268].

Saint Lucia actively engages in regional cybersecurity efforts through its membership in CARICOM IMPACS, participating in initiatives such as the 2023 national cyber awareness and sensitization training sessions aimed at strengthening cyber resilience[269]. Additionally, the country collaborates with the Latin America and Caribbean Cyber Competence Centre (LAC4), taking part in advanced training programs focused on cyber incident response, threat hunting, and endpoint security[270].

CYBERSECURITY CULTURE AND SOCIETY

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 | 2020 | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

Saint Lucia

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Saint Lucia

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025**

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Saint Lucia

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Saint Vincent and the Grenadines

Saint Vincent and the Grenadines currently lacks a formal national cybersecurity strategy, despite increased cyber incidents that highlight the island's vulnerability to cybercrime and cyberattacks. An example includes the 2015 hacking incident by a group claiming affiliation with ISIS, which targeted the government's website, demonstrating the nation's exposure to international cyber threats. Though the government has introduced some legislation to address cybercrime, and expressed commitment to regional cybersecurity efforts, there remains no designated Computer Security Incident Response Team (CSIRT) or national cybersecurity framework to systematically handle cyber incidents, manage critical infrastructure protection, or promote widespread cybersecurity awareness and resilience in the region.
Following the 2015 attacks, The Cybercrime Act of Saint Vincent and the Grenadines was passed in August 2016[271,272]. This Act is designed to criminalize a variety of cyber offenses and enhance the legal framework around cybersecurity in the country. This legislation addresses illegal access to computer systems, unauthorized data interception, data interference, system interference, and cyber-enabled offenses like identity theft, computer-related fraud, and online harassment[273].

Although there are some legislative and technical gaps in the country's current cyber framework[274], its regional and international level of engagement is crucial for in building a resilient cybersecurity framework and has shown some improvement in this area[275]. One important effort is the Caribbean Digital Transformation Project (CARDTP), from 2020. This is a World Bank-funded initiative aimed at enhancing digital services, connectivity, and economic opportunities across several Eastern Caribbean countries, including Saint Vincent and the Grenadines. Its main objectives include developing a "Digital Enabling Environment" to foster a secure, competitive, and innovative digital economy, building digital infrastructure for public services, and improving digital skills among citizens to drive economic growth. The project supports digital public services and technology-enabled businesses, aiming to make the region more resilient, create jobs, and boost digital service adoption by improving trust, transparency, and affordability in digital transactions[276]. Additionally, through partnerships with organizations like the Organization of Eastern Caribbean States (OECS) and the Caribbean Community (CARICOM), Saint Vincent and the Grenadines can access resources, shared expertise, and cybersecurity policies that help smaller nations enhance their security measures collectively[277].

Saint Vincent and the Grenadines has benefited from regional cybersecurity initiatives through its participation in CARICOM IMPACS initiatives, such as the 2025 workshop to develop a national Computer Incident Response Team (CIRT) Establishment Plan, held under the OECS-led Caribbean Digital Transformation Project[278]. Additionally, t the country participates in activities organized by the Latin America and Caribbean Cyber Competence Centre (LAC4) including advanced cybersecurity training programs focused on cyber incident response, threat hunting, and endpoint security[279].

In Terms of awareness raising, the Internet Society (ISOC) Saint Vincent and the Grenadines chapter has been actively involved in raising cybersecurity awareness through various initiatives. One major effort was the hosting of the 1st ISOC SVG Cyber-Security Symposium, in 2017, which aimed to engage stakeholders from the government, business, and civil society to discuss pressing issues in cybersecurity. Additionally, ISOC is part of a broader international effort to promote cybersecurity awareness through training and public policy discussions, especially for IT professionals and government bodies[280].

Another area of improvement Caribbean Digital Transformation Project, the government has implemented systems like GOVPAY, which allows citizens to pay for services using credit and debit cards across agencies such as Customs, Inland Revenue, and the Commerce and Intellectual Property Office. Additionally, the government has advanced projects in network services, cybersecurity, and e-tax services, focusing on a digital ID and single-window platforms for trade and property transactions to further improve accessibility and streamline services across government departments[281].

Saint Vincent and the Grenadines

CYBERSECURITY POLICY AND STRATEGY

D1

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

Saint Vincent and the Grenadines

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

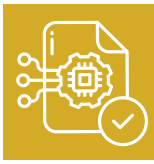
Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA



STANDARDS AND TECHNOLOGIES

Saint Vincent and the Grenadines

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025**

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Suriname

Suriname has taken concrete steps towards formalizing its cybersecurity strategy after it was commissioned to the Directorate of National Security[282]. A draft National Cybersecurity Strategy is currently under development, led by the Directorate of National Security. This strategy outlines a framework to address cyber threats, focusing on collaboration among public, private, and international stakeholders, as well as civil society[283]. However, Suriname has designed a National Digital Strategy 2023-2030, in which one of its 5 pillars is to improve cybersecurity and data protection "ensuring a safe and secure online environment". The establishment of SURCSIRT, Suriname's Computer Security Incident Response Team, plays a central role in national cyber defense. Although coordination remains ad hoc, SURCSIRT is the designated body responsible for incident response, development of cyberecurity protocols and maintaining the registry, under the Directorate's supervision[284]. Moreover, The Central Intelligence and Security Agency (CIVD) is the agency responsible for cybersecurity in Suriname[285], while a Cyber Crime Unit is being created within the national police.

Suriname is actively participating in the CARICOM Cyber Resilience Strategy 2030 Project, a regional initiative developed by the CARICOM Secretariat in partnership with USAID. This project is designed to enhance cybersecurity capabilities across CARICOM states, supporting collaboration and resilience at both the national and regional levels. Guided by a Steering Committee comprising CARICOM and regional experts, the strategy will establish a framework to improve information sharing, address regulatory gaps, and strengthen the cybersecurity workforce to protect critical infrastructure and digital resources throughout the Caribbean[286]. In February 2023, Suriname hosted the inaugural session of the Regional In-Country Cyber Awareness and Cybersecurity Sensitization and Training series, organized by CARICOM IMPACS (Caribbean Community Implementation Agency for Crime and Security). to reduce the risk of cybercrimes and implement mechanisms to enhance Cybersecurity in Member States[287].

Suriname also participated in the GLACY+ (Global Action on Cybercrime Extended). This initiative is a collaborative effort between the European Union and the Council of Europe, funded through the Instrument Contributing to Peace and Stability. Led by the Council of Europe, the project aims to build the capacity of countries around the world to enforce laws related to cybercrime and electronic evidence, while also improving their capabilities for effective international cooperation in these areas[288].

Efforts to raise public awareness around cybersecurity remain limited in Suriname, with information being disseminated mainly through social media, television, and radio segments. These efforts focus on basic cyber hygiene, such as recognizing phishing attempts and securing personal information online. They have focused on showing an international image to raise awareness, participating in both the ITU-IMPACT and the GFCE (Global Forum on Cyberexpertise), "a platform for international cooperation on strengthening cyber capacity and expertise globally"[289]. It also participated in the international military cybersecurity exercises, at the Tradewinds 2024 (TW24)[290].

There are no accredited university-level courses dedicated solely to cybersecurity, but the government has started offering introductory cybersecurity training sessions for public officials, supported by technical assistance from the OAS.

It is relevant to mention the introductory training courses provided by the government online through its Cisco Networking Academy initiative, which provides official certifications in courses such as "Introduction to Cybersecurity" and "Cybersecurity Essentials"[291]. Similarly, government ICT employees receive Cisco Certified Support Technician (CCST) training with the aim of expanding their skills and knowledge[292].

In recent years, Suriname has made strides in establishing a legal framework for cybersecurity, though substantial gaps remain. The government has begun drafting legislation to address cybercrime and data privacy; however, this is still under review and not yet formalized. Suriname's Directorate of National Security manages an annual audit of critical infrastructure, focusing on sectors like energy, water, and telecommunications to ensure resilience against cyber threats. A registry of incidents, managed by SURCSIRT, captures significant national incidents, though the response framework is still evolving[293]. Cybercrimes are defined in their legislation, as it appears in the Criminal Code of 2025[294], while it has a police force with a Digital Investigation Department[295].

Some industry best practices are followed on an ad hoc basis, particularly in critical infrastructure sectors, where operators are encouraged to conduct regular risk assessments and implement basic security controls. These controls include cryptographic measures like TLS for securing communications, although adoption is inconsistent across sectors. The financial sector has also begun exploring cybersecurity insurance options, though no formal cyber insurance market has been established[296].

As for digital government, Suriname provides a digital identity[297] with which to access certain services, such as digital signature[298]. In addition, this identity has an Authenticator, "a convenient security identification and encryption solution necessary to execute transactions and securely access online services"[299].

1-1 National Cybersecurity Strategy

- Strategy Development — 2016 | 2020 | **2025**
- Content — 2016 | 2020 | **2025**
- Implementation and Review — 2016 NA | 2020 NA | **2025**
- International Engagement — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025**

1-2 Incident Response and Crisis Management

- Identification and Categorization of Incidents — 2016 | 2020 | **2025**
- Organization — 2016 | 2020 | **2025**
- Integration of Cyber into National Crisis Management — 2016 NA | 2020 NA | **2025**
- Coordination — 2016 | 2020 | **2025** NA
- Mode of Operation — 2016 NA | 2020 | **2025** NA

1-3 Critical Infrastructure (CI) Protection

- Identification — 2016 | 2020 | **2025**
- Regulatory Requirements — 2016 NA | 2020 NA | **2025**
- Operational Practice — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Risk Management and Response — 2016 | 2020 | **2025** NA

1-4 Cybersecurity in Defense and National Security

- Defense Force Cybersecurity Strategy — 2016 | 2020 | **2025**
- Defense Force Cyber Capability — 2016 NA | 2020 NA | **2025**
- Civil-Defense Coordination — 2016 NA | 2020 NA | **2025**
- Organization — 2016 | 2020 | **2025** NA
- Coordination — 2016 | 2020 | **2025** NA

CYBERSECURITY CULTURE AND SOCIETY

Suriname

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information-
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Suriname

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025 NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Suriname

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | **2025**

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | **2025**

Procedural Cybercrime Legislation
2016 | 2020 | **2025**

Human Rights Impact Assessment
2016 NA | 2020 NA | **2025**

Legislative frameworks for ICT Security
2016 | 2020 | **2025** NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | **2025** NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | **2025**

Child Protection Online
2016 NA | 2020 | **2025**

Consumer Protection Legislation
2016 NA | 2020 | **2025**

Intellectual Property Legislation
2016 NA | 2020 | **2025**

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | **2025**

Prosecution
2016 | 2020 | **2025**

Courts
2016 | 2020 | **2025**

Regulatory Bodies
2016 NA | 2020 NA | **2025**

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | **2025**

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | **2025**

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | **2025**

Formal Cooperation
2016 NA | 2020 | **2025** NA

Informal Cooperation
2016 NA | 2020 | **2025** NA

STANDARDS AND TECHNOLOGIES

Suriname

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | **2025**

Standards in Procurement
2016 | 2020 | **2025**

Standards for Provision of Products and Services
2016 | 2020 | **2025**

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | **2025**

Cryptographic Controls
2016 NA | 2020 | **2025**

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | **2025**

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | **2025**

Monitoring and Response
2016 NA | 2020 NA | **2025**

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | **2025**

Cybersecurity Services and Expertise
2016 NA | 2020 NA | **2025**

Security Implications of Outsourcing
2016 NA | 2020 NA | **2025**

Cyber Insurance
2016 NA | 2020 NA | **2025**

Cybercrime Insurance
2016 | 2020 | **2025** NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | **2025**

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | **2025**

Trinidad and Tobago

Trinidad and Tobago's National Cybersecurity Strategy was first implemented in 2012. This initial strategy laid out critical policies aimed at creating a secure digital environment, establishing governance for cybersecurity, and implementing mechanisms to protect physical, virtual, and intellectual assets from cyber threats. Key elements included awareness campaigns, protection of critical infrastructure, cyber incident response measures, and a legal framework to combat cybercrime[300]. Trinidad and Tobago's National Digital Transformation Strategy (2024-2027) renews and updates these commitments, listing the National Cybersecurity Framework as one of the key drivers for digital transformation[301]. Likewise, the document "Vision 2030: The National Development Strategy of Trinidad and Tobago 2016–2030" explicitly recognizes cybersecurity as a key component of national development. The strategy emphasizes the need to align with and facilitate regional and international agreements on cybersecurity —such as the CARICOM Caribbean Cybersecurity and Cybercrime Action Plan (CCSCAP)— and prioritizes the strengthening of strategic global partnerships to effectively combat cybercrime[302].

The Ministry of Digital Transformation (MDT), established in 2021, is spearheading the national digital agenda. Its goals include enhancing digital access, creating a secure online government infrastructure with electronic identification (e-ID), and expanding the digital economy, particularly in software development and e-commerce. MDT benefits from IDB's technical and financial support through the Programto Accelerate the Digital Transformation Agenda, which channels over USD 11 million to implement a variety of cybersecurity initiatives through a dedicated component[303]. As part of this broader push toward modernization and transformation, the Development Bank of Latin America and the Caribbean (CAF) approved USD 120 million to support the country's digital transformation, including cybersecurity initiatives and the modernization of digital infrastructure[304].

In addition, international organizations like the UNDP are collaborating on projects to improve government service delivery and accessibility through digital tools. The Trinidad and Tobago Digital Transformation Project, led by the MDT and supported by partners such as iGovTT, is focused on enhancing the efficiency and inclusiveness of government services, especially for underserved communities. Likewise, the International Monetary Fund (IMF) has highlighted efforts to modernize the financial system, embrace Fintech, and enhance cybersecurity frameworks to support a digital economy. The private sector is also involved, with initiatives like SmartTerm helping drive digital innovation[305].

These efforts collectively aim to boost Trinidad and Tobago's digital infrastructure, ensuring wider access to services and fostering economic growth, while simultaneously addressing the challenges of cybersecurity and digital inclusion.

Trinidad and Tobago's Cybersecurity Incident Response Team (TT-CSIRT) was established in 2015, as the primary entity responsible for national cybersecurity incident management and collaboration with various stakeholders to enhance national cyber resilience[306]. It is supported by international cybersecurity organizations such as the IDB through the abovementioned Programme to Accelerate the Digital Transformation Agenda, the Organization of American States (OAS), through the CSIRTAmericas Network, and the International Telecommunication Union (ITU). Through these partnerships, TT-CSIRT aligns its practices with global cybersecurity standards, exchanges information on emerging cyber threats, and participates in joint response activities for cross-border incidents. These alliances enhance Trinidad and Tobago's capacity to respond to sophisticated cyber threats, particularly those that may impact multiple countries simultaneously. TT-CSIRT also plays a key role in safeguarding the nation's critical infrastructure by developing frameworks for risk assessment, continuity planning, and incident recovery. It assesses and mitigates risks to sectors crucial for national security, such as power grids, transportation, and finance.

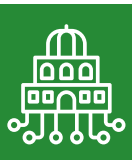
Although there has been no major overhaul of the 2012 strategy, Trinidad and Tobago's government has initiated legislative reforms to address gaps in cybersecurity law. This includes introducing updated cybercrime legislation to address emerging threats, such as ransomware and data breaches, and incorporating provisions for international collaboration to strengthen cross-border cyber defenses. Additionally, the Ministry of National Security's Strategic Plan for 2018-2023 highlights enhanced stakeholder collaboration and resilience to cyber threats, reflecting the government's increased attention to cybersecurity issues despite the lack of a comprehensive revision to the original strategy[307].

One such key legislative reform is the Cybercrime Bill of 2017, currently under consideration, which seeks to replace the outdated Computer Misuse Act of 2000. This bill introduces specific provisions to address various types of cybercrimes, such as unauthorized access to computer systems, identity theft, phishing, and cyberstalking. The bill is also designed to support investigations and evidence gathering in digital environments, making it easier for authorities to prosecute online offenses effectively[308]. In addition to this prosed Bill, the Data Protection Act of 2011 provides guidelines for handling personal information, ensuring individuals' data privacy and security, and mandating that entities securely manage and use personal data responsibly[309].

The private sector has had a growing role in collaborating with its public counterparts in raising cybersecurity awareness. Local companies, often in collaboration with cybersecurity consultancies like G5 Cybersecurity, work to enhance awareness within the business community, offering services like vulnerability assessments and employee cybersecurity training. These services help companies comply with cybersecurity best practices, safeguard customer data, and reduce vulnerabilities to cyber attacks.

Trinidad and Tobago have also partnered with international organizations to boost cybersecurity awareness. Notable collaborations include the "Get Safe Online Trinidad and Tobago" initiative, which provides online resources for individuals and businesses, advising them on safer online practices. Additionally, Trinidad and Tobago benefits from partnerships with the OAS, particularly through the STOP. THINK. CONNECT.™ campaign, which seeks to promote responsible online behavior and reduce cyber risks through public engagement[310].

Trinidad and Tobago benefits from regional cybersecurity initiatives through its participation in CARICOM IMPACS programs, such as the 2024 Regional Cyber Crisis Management Training aimed at enhancing national cyber resilience[311]. Additionally, the country has participated in advanced cybersecurity training programs organized by the Latin America and Caribbean Cyber Competence Centre (LAC4), focusing on incident response, threat hunting, and endpoint security[312]. As a signatory to the EU–LAC Digital Alliance, Trinidad and Tobago contributes to bi-regional initiatives promoting secure digital transformation and data protection frameworks across Latin America and the Caribbean[313,314].



CYBERSECURITY POLICY AND STRATEGY

Trinidad and Tobago

D1

1-1 National Cybersecurity Strategy

Strategy Development
2016 | 2020 | 2025

Content
2016 | 2020 | 2025

Implementation and Review
2016 NA | 2020 NA | 2025

International Engagement
2016 NA | 2020 NA | 2025

Organization
2016 | 2020 | 2025 NA

1-2 Incident Response and Crisis Management

Identification and Categorization of Incidents
2016 | 2020 | 2025

Organization
2016 | 2020 | 2025

Integration of Cyber into National Crisis Management
2016 NA | 2020 NA | 2025

Coordination
2016 | 2020 | 2025 NA

Mode of Operation
2016 NA | 2020 | 2025 NA

1-3 Critical Infrastructure (CI) Protection

Identification
2016 | 2020 | 2025

Regulatory Requirements
2016 NA | 2020 NA | 2025

Operational Practice
2016 NA | 2020 NA | 2025

Organization
2016 | 2020 | 2025 NA

Risk Management and Response
2016 | 2020 | 2025 NA

1-4 Cybersecurity in Defense and National Security

Defense Force Cybersecurity Strategy
2016 | 2020 | 2025

Defense Force Cyber Capability
2016 NA | 2020 NA | 2025

Civil-Defense Coordination
2016 NA | 2020 NA | 2025

Organization
2016 | 2020 | 2025 NA

Coordination
2016 | 2020 | 2025 NA

CYBERSECURITY CULTURE AND SOCIETY

Trinidad and Tobago

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | 2025

Priority of Security
2016 NA | 2020 NA | 2025

Practices
2016 NA | 2020 NA | 2025

Government
2016 | 2020 | 2025 NA

Private Sector
2016 | 2020 | 2025 NA

Users
2016 | 2020 | 2025 NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | 2025

User Trust and Confidence in Online Search and Information
2016 | 2020 | 2025

Disinformation
2016 NA | 2020 NA | 2025

User Trust in E-Government Services
2016 | 2020 | 2025

User Trust in E-commerce Services
2016 | 2020 | 2025

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | 2025

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | 2025

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | 2025

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Trinidad and Tobago

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | 2025

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | 2025

Executive Awareness Raising
2016 | 2020 | 2025

Awareness Raising Programmes
2016 | 2020 | 2025

3-2 Cybersecurity Education

Provision
2016 | 2020 | 2025

Administration
2016 | 2020 | 2025

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | 2025

Uptake
2016 | 2020 | 2025

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | 2025

LEGAL AND REGULATORY FRAMEWORKS

Trinidad and Tobago

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government-Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

Uruguay

Over the past decade, Uruguay has made significant strides in promoting cybersecurity at the state level through various digital policy instruments and legal and regulatory frameworks, contributing to a more cyber-secure environment for the country. The Uruguay Digital Agenda 2025[lx] and the IDB-supported "Strengthening Cybersecurity in Uruguay" USD 10 million program[lxi] have laid the groundwork for establishing a clear stance on cybersecurity. Additionally, the enactment of Law No. 20.212[lxii] has introduced a new institutional framework, created new competencies, and legally mandated the development of an ecosystem and mechanisms to bolster national cybersecurity capabilities. Looking forward, Uruguay has approved the National Cybersecurity Strategy 2024-2030[315], which takes a modern, holistic approach crafted through inclusive consultations involving all sectors. The "Digital Transformation for a Smart Nation I" project financed by the IDB was approved in 2024, including a specific US$6 million component for additional national cybersecurity initiatives.

The regulatory framework in Uruguay empowers key institutions to play crucial roles in securing digital environments The Agency for the Development of Electronic Government and the Information and Knowledge Society (AGESIC)[lxiii], under the Presidency of the Republic, and the National Computer Security Incident Response Center (CERTuy)[lxiv] have been instrumental in building an ecosystem that prioritizes information security in digital environments. The Ministry of National Defense is responsible for coordinating critical infrastructures, while AGESIC oversees critical information infrastructures. The creation of bodies like the Honorary Advisory Council on Information Security (CAHSI), the National Cybersecurity Strategy Management Committee and the Strategic Management Council (CGE) further demonstrates Uruguay's commitment to a structured and collaborative approach to cybersecurity governance. In 2024, AGESIC, along with CAHSI and CGE, are spearheading a collaborative process to develop a National Cybersecurity Strategy[lxv]. Uruguay actively participates in key international cybersecurity forums, including the OAS, UN, DIGITAL NATION, FIRST, GFCE, MERCOSUR, REDGEALC, EU LAC4, CRI, ALADI, ITU, and OECD, among others.

Uruguay demonstrates maturity in education, training, and capacity building for multiple stakeholders in the cybersecurity field. A wide range of cybersecurity courses are available to all citizens[lxvi] highlighting courses supported by the OAS aimed at girls and adolescent women[lxvii]. The country has integrated cybersecurity and digital citizenship training into its Integrated Basic Education Programs (EBI)[lxviii], which represent the most comprehensive curricular documents in the territory. Various awareness initiatives have been launched, including campaigns promoting responsible internet use across different sectors of society, such as education and SMEs. Notable examples include the "Seguro Te Conectás" program[lxix] and the AGESIC platform[lxx]. Furthermore, the SINAE Virtual Educational Platform offers awareness and training strategies aimed at fostering a more prepared and resilient community.

Uruguay has also conducted formal analyses of the cybersecurity labor market[lxxi], with a comprehensive understanding of the potential demand for cybersecurity training and employment[lxxii] in Uruguay. The

educational landscape includes a variety of postgraduate and specialized cybersecurity courses[lxxiv], including state-organized programs for public sector employees[lxxv]. The Study Plan for the Technical Analyst in Cybersecurity Degree[lxxvi] promoted by AGESIC and developed with the Faculty of Engineering (Computing Institute) through the Julio Ricaldoni Foundation, with the support of the IDB, allows interested people who have completed the second year of secondary education in the Uruguayan educational system to train or retrain technically in Cybersecurity.

Uruguay has established a comprehensive legal and regulatory framework to address cybersecurity challenges and protect digital rights. The cornerstone of this framework is Law No. 18.331 on the Protection of Personal Data and Habeas Data Action. Also highlighted are Law No. 9739 on Copyright, Law No. 17.616 on the Protection of Intellectual Property, Law No. 17,815 on Sexual Violence against Children, Adolescents or Incapacitated Persons by any means, Law No. 18383 on attacks against the regularity of Telecommunications, Law No. 18561 on the prevention and punishment of sexual harassment in the workplace and in teacher-student relations, and Law No. 19580 on gender-based violence against women. In 2024, the Uruguayan Parliament approved Law No. 20.327 September 25, 2024 on cybercrim[lxxvii], providing tools to prevent and punish illegal digital activities. This law defines and penalizes various cybercrimes, including cyberbullying, computer fraud, unlawful access to computer data, and identity theft. It also establishes prevention and education measures, creates a cybercriminal registry, and empowers financial institutions to act against non-consensual transactions.

The country has consolidated risk control through standards and technologies. Both the public and private sectors, particularly entities linked to critical services, utilize the National Cybersecurity Framework[lxxviii], which is based on the NIST Cybersecurity Framework. The country is also working to incorporate security-by-design requirements into public procurement specifications[lxxix]. Uruguay has established a National Cybersecurity Incident Registry[lxxx], requiring all critical services to report cybersecurity incidents to CERTuy through various communication channels, including telephone, email, monitoring probes, and web form[316] .

CYBERSECURITY CULTURE AND SOCIETY

Uruguay

D2

2-1 Cybersecurity Mind-Set

Awareness of Risks
2016 NA | 2020 NA | **2025**

Priority of Security
2016 NA | 2020 NA | **2025**

Practices
2016 NA | 2020 NA | **2025**

Government
2016 | 2020 | **2025** NA

Private Sector
2016 | 2020 | **2025** NA

Users
2016 | 2020 | **2025** NA

2-2 Trust and Confidence in Online Services

Digital Literacy and Skills
2016 NA | 2020 NA | **2025**

User Trust and Confidence in Online Search and Information-
2016 | 2020 | **2025**

Disinformation
2016 NA | 2020 NA | **2025**

User Trust in E-Government Services
2016 | 2020 | **2025**

User Trust in E-commerce Services
2016 | 2020 | **2025**

2-3 User Understanding of Personal Information Protection Online

Personal Information Protection Online
2016 NA | 2020 | **2025**

2-4 Reporting Mechanisms

Reporting Mechanisms
2016 NA | 2020 | **2025**

2-5 Media and Online Platforms

Media and Social Media
2016 NA | 2020 | **2025**

BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

Uruguay

D3

3-1 Building Cybersecurity Awareness

Awareness-raising initiatives by Government
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Private Sector
2016 NA | 2020 NA | **2025**

Awareness-raising initiatives by Civil Society
2016 NA | 2020 NA | **2025**

Executive Awareness Raising
2016 | 2020 | **2025**

Awareness Raising Programmes
2016 | 2020 | **2025** NA

3-2 Cybersecurity Education

Provision
2016 | 2020 | **2025**

Administration
2016 | 2020 | **2025**

3-3 Cybersecurity Professional Training

Provision
2016 | 2020 | **2025**

Uptake
2016 | 2020 | **2025**

3-4 Cybersecurity Research and Innovation

Cybersecurity Research and Development
2016 NA | 2020 NA | **2025**

LEGAL AND REGULATORY FRAMEWORKS

D4

4-1 Legal and Regulatory Provisions

Substantive Cybercrime Legislation
2016 | 2020 | 2025

Legal and Regulatory Requirements for Cybersecurity
2016 NA | 2020 NA | 2025

Procedural Cybercrime Legislation
2016 | 2020 | 2025

Human Rights Impact Assessment
2016 NA | 2020 NA | 2025

Legislative frameworks for ICT Security
2016 | 2020 | 2025 NA

Privacy, Freedom of Speech and other Human Rights Online
2016 | 2020 | 2025 NA

4-2 Related Legislative Frameworks

Data Protection Legislation
2016 NA | 2020 | 2025

Child Protection Online
2016 NA | 2020 | 2025

Consumer Protection Legislation
2016 NA | 2020 | 2025

Intellectual Property Legislation
2016 NA | 2020 | 2025

4-3 Legal and Regulatory Capability and Capacity

Law Enforcement
2016 | 2020 | 2025

Prosecution
2016 | 2020 | 2025

Courts
2016 | 2020 | 2025

Regulatory Bodies
2016 NA | 2020 NA | 2025

4-4 Formal and Informal Cooperation Frameworks to Combat Cybercrime

Law Enforcement with Private Sector
2016 NA | 2020 NA | 2025

Cooperation with Foreign Law Enforcement Counterparts
2016 NA | 2020 NA | 2025

Government–Criminal Justice Sector Collaboration
2016 NA | 2020 NA | 2025

Formal Cooperation
2016 NA | 2020 | 2025 NA

Informal Cooperation
2016 NA | 2020 | 2025 NA

STANDARDS AND TECHNOLOGIES

D5

5-1 Adherence to Standards

ICT Security Standards
2016 | 2020 | 2025

Standards in Procurement
2016 | 2020 | 2025

Standards for Provision of Products and Services
2016 | 2020 | 2025

5-2 Security Controls

Technological Security Controls
2016 NA | 2020 NA | 2025

Cryptographic Controls
2016 NA | 2020 | 2025

5-3 Software Quality

Software Quality and Assurance
2016 NA | 2020 | 2025

5-4 Cybersecurity Professional Training

Internet Infrastructure Reliability
2016 NA | 2020 NA | 2025

Monitoring and Response
2016 NA | 2020 NA | 2025

5-5 Cybersecurity Marketplace

Cybersecurity Technologies
2016 | 2020 | 2025

Cybersecurity Services and Expertise
2016 NA | 2020 NA | 2025

Security Implications of Outsourcing
2016 NA | 2020 NA | 2025

Cyber Insurance
2016 NA | 2020 NA | 2025

Cybercrime Insurance
2016 | 2020 | 2025 NA

5-6 Responsible Disclosure

Sharing Vulnerability Information
2016 NA | 2020 NA | 2025

Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
2016 NA | 2020 NA | 2025

FOOTNOTES

34 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Status_ITU_IMPACT.pdf

35 https://www.southcom.mil/Media/Special-Coverage/Tradewinds-2022/

36 https://www.lac4.eu/es/antigua-y-barbuda-se-une-a-lac4/

37 https://caricom.org/caricom-usaid-partner-on-cyber-resilience-strategy-2030-project/

38 https://www.indianewsnetwork.com/es/20230914/india-inks-pacts-to-foster-digital-transformation-with-armenia-antigua-barbuda-and-sierra-leone

39 https://dig.watch/updates/india-and-antigua-barbuda-sign-mou-for-digital-transformation-cooperation

40 https://iica.int/es/prensa/noticias/ministras-de-antigua-y-barbuda-y-de-costa-rica-destacan-el-potencial-de-las

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

42 http://laws.gov.ag/wp-content/uploads/2021/02/No.-12-Electronic-Crimes-Amendment-Act-2020.pdf?

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

44 http://laws.gov.ag/wp-content/uploads/2019/04/Electronic-Transactions-Act-2013.pdf

45 https://www.caf.com/es/actualidad/noticias/2024/07/caf-aprueba-la-incorporacion-de-antigua-y-barbuda-como-miembro/

46 https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

47 https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1-2023-377806/texto

48 https://www.argentina.gob.ar/sites/default/files/2023/06/consulta_publica_segunda_estrategia.pdf

49 https://www.boletinoficial.gob.ar/pdf/aviso/primera/195154/20240619

50https://www.argentina.gob.ar/jefatura/innovacion-publica/innovacion-administrativa/firma-digital/normativa-de-firma-digital

51 https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-7

52 https://www.first.org/tlp/

53 https://www.argentina.gob.ar/sites/default/files/infoleg/disp3-386227.pdf

54 https://disarmament.unoda.org/open-ended-working-group/

55 https://ec.europa.eu/commission/presscorner/detail/en/statement_23_3892

56 https://eceur.cancilleria.gob.ar/es/argentina-promueve-la-agenda-digital-en-el-mercosur

57 https://buenosaires.gob.ar/jefaturadegabinete/centro-de-ciberseguridad/quienes-somos-y-que-hacemos

58 https://ccatlat.org/mplace/shop/

59 https://fundacionsadosky.org.ar/ctf-junior/

60 https://www.palermo.edu/ingenieria/h4ck3d/

61 https://www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales

62 https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

63 https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798

64 https://www.boletinoficial.gob.ar/detalleAviso/primera/238576/20201216

65 https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-641-2021-351345

66 https://acrobat.adobe.com/id/urn:aaid:sc:VA6C2:db83ed97-0946-4c03-b400-24bfc04b37b6?viewer%21megaVerb=group-discover

67 https://www.bahamas.gov.bs/wps/portal/public/gov/government/news/cybersecurity%20plays%20pivotal%20role%20in%20the%20bahamas%20national%20strategy/

68 https://www.first.org/members/teams/cirt-bs

69 https://www.iadb.org/en/project/BH-L1045

70 https://www.lac4.eu/es/event/caribbean-regional-cybersecurity-exercise-cybercrabs-2022/

71 https://caricom.org/caricom-usaid-partner-on-cyber-resilience-strategy-2030-project/

72 https://www.southcom.mil/Media/Special-Coverage/Tradewinds-2024/

73 https://www.getsafeonline.bs/

74 https://www.fidelitygroup.com/bach-fraud-notice?

75 CISB 420 Computer Information Security, CISB 411 Information Systems Auditing, Control & Security.

76 https://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/2003-0002_1.pdf

77 https://laws.bahamas.gov.bs/cms/ilaws-search.html?zoom_query=Data%20Protection%20Act

78 https://www.royalbahamaspolice.org/aboutus/rbpforganizationalchart12231.pdf

79 https://www.centralbankbahamas.com/

80 https://urcabahamas.bs/

81 While not publicly available the NCS for Barbados was approved in 2023.

82 https://caricom.org/caricom-usaid-partner-on-cyber-resilience-strategy-2030-project/

83 https://www.lac4.eu/es/event/caribbean-regional-cybersecurity-exercise-cybercrabs-2022/

84 https://bb.usembassy.gov/united-states-and-barbados-collaborate-on-cyber-security/

85 https://www.centralbank.org.bb/viewPDF/documents/2023-09-07-09-07-47-Technology-and-Cyber-Risk-Management-Guideline.pdf

86 https://www.centralbank.org.bb/viewPDF/documents/2023-09-07-09-07-47-Technology-and-Cyber-Risk-Management-Guideline.pdf

87 https://www.southcom.mil/Media/Special-Coverage/Tradewinds-2024/

88 https://www.caricomimpacs.org/

89 https://www.lac4.eu/central-american-sme-s-focus-on-building-their-cyber-resilience/

90 https://www.eeas.europa.eu/eeas/europe-and-latin-america-caribbean-step-cooperation-cybersecurity_en

91 https://www.pressoffice.gov.bz/wp-content/uploads/2019/12/belize-cybersecurity-strategy-2020-2023.pdf https://cito.gov.bz/cyber-security/ - https://www.belizepolice.bz/ - https://www.belizepolice.bz/index.php?option=com_content&view=category&id=51 - https://lovefm.com/police-to-launch-cybercrime-education-campaign/ - https://cito.gov.bz/blog/ - https://www.getsafeonline.bz/ - https://www.sjc.edu.bz/_files/ugd/343ada_44fa967053f24aa99c5192ec4e224eb6.pdf - https://www.instagram.com/universityofbelize/p/Cyg_prfp0DB/ - https://bco.gov.bz/

92 https://www.agetic.gob.bo/ciudadania-digital/

93 https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/396020:El-Ministerio-TIC-refuerza-la-Seguridad-Digital-en-las-Entidades-Publicas-con-la-actualizacion-del-Modelo-de-Seguridad-y-Privacidad-de-la-Informacion

94 https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx - https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

95 https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20ENG.pdf

96 https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=104718&nValor3=146407&strTipM=TC

97 https://www.ccn-cert.cni.es/es/seguridad-al-dia/actualidad-ccn/13013-el-centro-criptologico-nacional-colabora-con-costa-rica-en-la-creacion-de-un-laboratorio-forense-y-de-ciberinteligencia-en-este-pais.html

98 https://cardtp.gov.dm/index.php/about-the-project/project-components/component-1-digital-enabling-environment - https://emonewsdm.com/the-caribbean-digital-transformation-project-conducts-four-day-training-oncybersecurity-for-the-establishment-of-a-national-cybersecurity-incident-responseteam-csirt-in-the-commonwealth-of-dominica/ - https://nbdominica.com/cybersecurity-awareness-competition/ - https://www.facebook.com/domleconline/photos/cybersecurity-awareness-month-2024-being-cyber-secure-is-very-mindful-very-demur/1351414602866973/?_rdr

99 https://cncs.gob.do/wp-content/uploads/2020/02/Decreto-230-18.pdf

100 https://presidencia.gob.do/decretos/313-22

101 https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

102 https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

103 https://cncs.gob.do/

104 https://digitalrd.citizenlab.co/es-CL/):contentReference[oaicite:1]{index=1

105 https://cncs.gob.do/wp-content/uploads/2022/12/Decreto-685-22.pdf

106 https://www.bancentral.gov.do/a/d/5696-sprics

107 DR-L1142, DR-L1147, DR-L1152

108 https://cncs.gob.do/wp-content/uploads/2024/08/Campana-Autenticacion-Multifactor-MFA.-Resultados-JUNIO-2024.pdf

109 https://cncs.gob.do/wp-content/uploads/2024/06/Resultados-Campana-Ciberseguridad-Para-Mujeres-Marzo-2024_20052024.pdf

110 https://www.ciberseguridad.gob.do/

111 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

112 https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

113 https://www.intec.edu.do/oferta-academica/postgrado/ingenieria/item/maestria-en-ciberseguridad-mcs

114 https://postgrado.unphu.edu.do/master-en-ciberseguridad-uax/

115 https://itla.edu.do/

116 Htttps://www.ciberlac.org

117 https://www.lac4.eu/es/

118 https://www.lac4.eu/es/

119 https://www.first.org/about/people/carlos-leonardo

120 https://www.opd.org.do/descargas/Ciberpolitica/Leyes/Ley-No.53-07-Sobre-Cri%CC%81menes-y-Delitos-de-Alta-Tecnologia.pdf

121 https://www.sb.gob.do/regulacion/leyes/ley-no-172-13-proteccion-de-los-datos/

122 https://cyber4dev.eu/2021/02/04/building-cyber-capacity-in-dominican-republic/

123 https://www.eucybernet.eu/eu-cybernet-work-in-dominican-republic-first-national-cyber-llamas-exercise/

124 https://presidencia.gob.do/noticias/rd-es-escogida-miembro-del-consejo-de-directores-del-foro-internacional-de-respuesta

125 https://www.caricomimpacs.org/articles/caricom-impacs-and-inl-to-strengthen-cbsi-connect

126 https://www.policianacional.gob.do/policia-nacional-de-la-republica-dominicana-recibe-informe-sobre-evaluacion-de-ciberseguridad/

127 https://cncs.gob.do/guia-de-identificacion-y-reporte-de-incidentes-ciberneticos-2/

128 https://www.gob.do/

129 https://agendadigital.gob.do/wp-content/uploads/2022/02/Agenda-Digital-2030-v2.pdf

130 The National Cybersecurity Strategy was approved by the National Cybersecurity Committee through Resolution No. CNC-2022-007 on August 3, 2022, and is based on the following pillars: 1. Cybersecurity governance and coordination, 2. Incident management and cyber resilience, 3. Tackling cybercrime, 4. National cyber defense, 5. Cybersecurity skills and capabilities, 6. International cooperation. Ecuador is currently in the planning stage for the implementation of the second phase of the National Cybersecurity Strategy as indicated in the records of the OAS survey.

131 https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf

132 https://www.ecucert.gob.ec/

133 OAS Survey

134 https://internetsegura.gob.ec/?wpbdp_listing=asociacin-ecuatoriana-de-ciberseguridad

135 https://www.epn.edu.ec/maestria-en-ciberseguridad/

136 https://www.telecomunicaciones.gob.ec/agenda-de-transformacion-digital-ecuador/

137 https://www.worldbank.org/en/programs/de4lac/publication/digital-economy-for-latin-america-and-the-caribbean-country-diagnostic-ecuador

138 https://www.iadb.org/en/project/EC-L1253

139 https://www.iadb.org/en/project/EC-L1294

140 https://www.eeas.europa.eu/delegations/panam%C3%A1/regional-alianza-digital-ue-am%C3%A9rica-latina-y-caribe_es

141 https://www.lac4.eu/es/ecuador-se-une-a-lac4/

142 https://clym.io/regulations/ecuador-lopdp

143 https://www.iadb.org/en/project/EC-L1294

144 https://www.innovacion.gob.sv/downloads/Agenda%20Digital.pdf

145 https://www.elsalvador.com/noticias/nacional/gobierno-propone-leyes-proteccion-datos-y-de-ciberseguridad/1178449/2024/

146 https://www.iadb.org/en/project/ES-L1168

147 https://perspectivainternacional.com/america/la-evolucion-de-la-ciberseguridad-en-el-salvador-bajo-el-liderazgo-de-nayib-bukele/

148 https://www.innovacion.gob.sv/ciberseguridad.php

149 https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

150 https://www.lac4.eu/event/exchange-of-cybersecurity-best-practices-between-the-eu-and-the-government-of-el-salvador-via-taiex-instrument/

151 https://perspectivainternacional.com/america/la-evolucion-de-la-ciberseguridad-en-el-salvador-bajo-el-liderazgo-de-nayib-bukele/

152 https://investinelsalvador.gob.sv/es/el-salvador-se-fortalece-en-ciberseguridad/

153 https://perspectivainternacional.com/america/la-evolucion-de-la-ciberseguridad-en-el-salvador-bajo-el-liderazgo-de-nayib-bukele/

154 https://www.iadb.org/en/project/ES-T1382

155 https://www.trade.gov/market-intelligence/el-salvador-new-cybersecurity-policy

156 https://eulacfoundation.org/en/eu-latin-america-and-caribbean-digital-alliance

157 https://www.lac4.eu/women-in-cybertech-camplac4-to-start-today/

158 https://caricom.org/institutions/caricom-implementing-agency-for-crime-and-security-impacs/

159 https://www.getsafeonline.gd/ - https://www.laws.gov.gd/index.php/acts/search-result?filter_category_id=1344&filter_search=Electronic%20Crimes%20Act&show_category=0&searchphrase=all&show_searchform=0 - https://www.laws.gov.gd/index.php/acts/search-result?filter_category_id=1344&filter_search=data%20protection&show_category=0&searchphrase=all&show_searchform=0

160 https://conciber.gob.gt/

161 https://www.sie.gob.gt/portal/DOCS/ANRA/ANRA_2024.pdf

162 https://gtcert.mingob.gob.gt/; https://www.iadb.org/en/project/RG-T4577?utm_source=chatgpt.com

163 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Status_ITU_IMPACT.pdf

164 https://www.coe.int/en/web/cybercrime/glacyplus

165 https://www.eeas.europa.eu/delegations/guatemala/guatemala-se-convierte-en-el-und%C3%A9cimo-miembro-del-centro-de-competencia-cibern%C3%A9tica-de-am%C3%A9rica_es

166 https://www.eeas.europa.eu/eeas/eu-lac-digital-alliance-partners-promote-digital-citizen-engagement-central-america_en

167 https://www.congreso.gob.gt

168 https://conciber.gob.gt/wp-content/uploads/2022/08/ACUERDO-GUBERNATIVO-200-2021-2.pdf

169 https://banguat.gob.gt/sites/default/files/banguat/Publica/Res_JM/2021/Res_JM-104-2021.pdf

170 https://dpi.gov.gy/from-the-prime-minister-on-cybersecurity-month/

171 https://www.kaieteurnewsonline.com/2023/03/21/u-s-dept-of-justice-offers-technical-support-to-develop-guyanas-cyber-security-framework/

172

173 https://www.eeas.europa.eu/delegations/guyana/guyana-formally-joins-eu-lac-digital-alliance_en

174 https://cybilportal.org/projects/eu-cybernet-lac4-latin-america-and-caribbean-cyber-competence-centre

175 https://www.caricomimpacs.org/articles/caricom-impacs-bolsters-regional-skills-in-cyber-security

176 https://dpi.gov.gy/national-cyber-risk-workshop-critical-to-govts-security-framework-pm-phillips/

177 https://guyanachronicle.com/2023/10/27/cybersecurity-must-be-strengthened-amidst-increase-in-business/

178 https://www.stabroeknews.com/2022/12/19/news/guyana/cybercrime-act-to-be-repealed-ag/

179 https://guyanachronicle.com/2024/10/10/cybersecurity-month-pm-calls-for-collective-action-against-rising-cyber-threats/

180 https://ndi.edu.gy/

181 https://cybilportal.org/projects/eu-cybernet-lac4-latin-america-and-caribbean-cyber-competence-centre/

182 https://www.caricomimpacs.org/articles/regional-in-country-cyber-awareness-and-cyber-security-sensitization-and-training-2023-in-paramaribo-suriname

183 http://www.conatel.gouv.ht/node/565

184 https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

185 https://www.lac4.eu/event/national-cybersecurity-strategies-development-and-implementation-workshop-for-honduras

186 https://www.iadb.org/en/project/HO-L1202

187 https://www.cnbs.gob.hn/documentos-fintech/regulacion-tecnologias-habilitadoras/

188 https://www.diger.gob.hn/sites/default/files/2024-02/Plan%20de%20Gobierno%20Digital%20Honduras.pdf - https://www.conatel.gob.hn/wp-content/uploads/2024/06/PLAN-ESTRATEGICO-INSTITUCIONAL-2022-a-2026.pdf - https://ahiba.hn/mes-de-ciberseguridad/ - https://www.youtube.com/watch?v=zgpwsgT1SE0 - https://upi.edu.hn/euroinnova/diplomado-en-ciberseguridad/ - https://iies.unah.edu.hn/vinculacion/pcemp/ciberseguridad/ - https://udh.edu.hn/views/course/OA-DCC.html - https://www.uth.hn/executive-education/cursos-2/cursos-tegucigalpa/curso-ciberdelitos-en-instituciones-financieras/ - https://www.tsc.gob.hn/biblioteca/index.php/codigos/830-codigo-penal-2019 - https://www.tsc.gob.hn/biblioteca/index.php/codigos/168-codigo-penal

189 https://cabinet.gov.jm/wp-content/uploads/2022/10/NSC-Press-Release-August-2022-1.pdf?utm_source=chatgpt.com

190 https://www.iadb.org/en/project/JA-L1093

191 https://jis.gov.jm/jamaicas-cybersecurity-infrastructure-strengthened-through-stakeholder-initiatives/

192 https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

193 https://cybilportal.org/projects/eu-cybernet-lac4-latin-america-and-caribbean-cyber-competence-centre

194 https://jis.gov.jm/jamaicas-cybersecurity-infrastructure-strengthened-through-stakeholder-initiatives

195 https://jis.gov.jm/jamaicas-cybersecurity-infrastructure-strengthened-through-stakeholder-initiatives/

196 https://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf

197 https://www.jamaicaobserver.com/2021/05/18/cybercrimes-act-revisited-the-balancing-act/

198 https://jis.gov.jm/new-offences-recommended-for-inclusion-in-cybercrimes-act/

199 The Data Protection Act, 2020.pdf

200 https://jis.gov.jm/data-protection-act-takes-effect-today/

201 https://jis.gov.jm/new-offences-recommended-for-inclusion-in-cybercrimes-act/

202 https://www.fscjamaica.org/wp-content/uploads/2024/03/Cyber-Resilience-Principles.pdf

203 https://mytaxes.ads.taj.gov.jm/_/

204 https://elandjamaica.nla.gov.jm/elandjamaica/interactivemap.aspx

205 https://opm.gov.jm/news/jamaica-embracing-technological-transformation-through-egov/

206 https://www.iadb.org/en/project/JA-L1072

207 https://jis.gov.jm/2-3-billion-allocated-to-nids-project/

208 https://jacirt10.876dev.com/node/35

209 https://www.jtda.org/fortinet

210 https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

211 https://www.gob.mx/citicsi

212 https://www.gob.mx/gncertmx

213 https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

214 https://www.gob.mx/cms/uploads/attachment/file/680717/Guii_a_Parental_Digital_511.pdf

215 https://www.gob.mx/cms/uploads/attachment/file/941260/Avances_y_Resultados_2023-2024_PNPSVD_VF.__1__low.pdf

216 https://ciberseguridad.ift.org.mx/files/guias_y_estudios/percepcion_de_las_personas_en_ciberseguridad.pdf

217 https://www.gob.mx/gncertmx?tab=guias

218 https://www.gob.mx/cms/uploads/attachment/file/738533/MANUAL_B_SICO_CIBERSEGURIDAD_MIPYMES_2022_04_07.pdf

219 https://mexicociberseguro.org.mx/

220 https://www.nist.gov/cyberframework

221 https://www.iso.org/standard/27001

222 https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

223 https://elpais.com/mexico/2025-01-30/mexico-anuncia-una-estrategia-digital-contra-la-burocracia-y-la-corrupcion-en-los-tramites-gubernamentales.html

224 https://www.dataguidance.com/opinion/panama-developments-cybersecurity

225 https://cert.pa/?p=3011

226 https://cert.pa/?page_id=400

227 https://cert.pa/?p=2952

228 https://www.iadb.org/en/project/PN-L1171

229 https://web.archive.org/web/20250201044140/https://www.usaid.gov/sites/default/files/2024-06/USAID_Panama_DECA.pdf

230 https://web.archive.org/web/20250201044140/https://www.usaid.gov/sites/default/files/2024-06/USAID_Panama_DECA.pdf

231 https://www.eeas.europa.eu/delegations/panam%C3%A1/regional-alianza-digital-ue-am%C3%A9rica-latina-y-caribe_es

232 https://www.lac4.eu/es

233 https://mitic.gov.py/eoj0cad9uplo/2024/11/ENC-Paraguay-2024-2028-14Nov2024-1.pdf

234 https://www.iadb.org/es/proyecto/PR-L1153

235 https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

236 https://www.lac4.eu

237 https://mitic.gov.py/declaracion-conjunta-sobre-ciberseguridad-y-cooperacion-digital-entre-estados-unidos-y-paraguay/

238 https://mitic.gov.py/ministro-del-mitic-se-reune-con-lideres-tecnologicos-en-taiwan/

239 https://mitic.gov.py/mitic-y-el-consejo-de-ciberseguridad-de-eua-acuerdan-fortalecimiento-en-ciberseguridad-a-traves-de-memorandum-de-entendimiento/

240 https://www.cert.gov.py/estrategia-nacional-de-ciberseguridad/ - https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqIB7UhNg - https://www.iadb.org/es/proyecto/PR-L1153 - https://mitic.gov.py/declaracion-conjunta-sobre-ciberseguridad-y-cooperacion-digital-entre-estados-unidos-y-paraguay/ - https://mitic.gov.py/ministro-del-mitic-se-reune-con-lideres-tecnologicos-en-taiwan/ - https://www.instagram.com/miticpy/p/C6oTxB7NMfW/ - https://www.cert.gov.py/wp-content/uploads/2024/07/CNC_mayo-2024.pdf - https://www.cert.gov.py/wp-content/uploads/2024/01/RESOLUCION-MITIC-N%C2%B0-032-2024-Coordinador-Nacional-de-Ciberseguridad.pdf - https://www.cert.gov.py/rfc-2350/ - https://www.cert.gov.py/ciberejercicios-simulacro-de-ciberataque/ - https://www.cert.gov.py/modelo-de-gobernanza-de-seguridad-de-la-informacion/ - https://www.conectateseguro.gov.py/ - https://mitic.gov.py/gobierno-esta-siempre-abierto-al-dialogo-y-a-romper-la-desinformacion-senala-ministro/ - https://www.cert.gov.py/estandares-y-normas/reglamentacion-sobre-reporte-obligatorio-de-incidentes-ciberneticos-de-seguridad-en-el-estado/#

241 https://cdn.www.gob.pe/uploads/document/file/4912522/Decreto%20Supremo%20N.%C2%B0085-2023-PCM.pdf

242 https://www.gob.pe/17303-presidencia-del-consejo-de-ministros-centro-nacional-de-seguridad-digital-cnsd

243 https://www.bcrp.gob.pe/docs/Transparencia/planeamiento/plan-de-gobierno-digital-bcrp-2024-2026.pdf

244 https://www.iadb.org/es/proyecto/PE-L1286?utm

245 https://www.iadb.org/en/project/PE-T1571

246 https://publications.iadb.org/en/publications/english/viewer/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

247 https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

248 https://www.lac4.eu

249 https://www.cybersecurityintelligence.com/pecert-2770.html

250 https://www.afi-global.org/wp-content/uploads/2021/03/Peru_DFS_CaseStudy_WEB_final_V6.pdf

251 https://engage.isaca.org/limachapter/cursos/cybersecurityfundamentals

252 https://www.gob.pe/63178-participar-del-ciclo-de-webinars-para-el-fortalecimiento-de-capacidades-en-seguridad-digital

253 https://www.gob.pe/13326-reglamento-de-la-ley-de-gobierno-digital

254 https://publicadministration.un.org/egovkb/en-us/data/country-information/id/133-peru

255 https://www.innovacion.gob.sv/

256 https://www.lac4.eu/es/event/caribbean-regional-cybersecurity-exercise-cybercrabs-2022/

257 https://caricom.org/caricom-usaid-partner-on-cyber-resilience-strategy-2030-project/

258 https://canadacaribbeaninstitute.org/2025/02/19/government-of-st-kitts-and-nevis-officially-launches-training-programme-to-build-cybersecurity-workforce-and-digital-resilience/

259 https://www.getsafeonline.org/get-safe-online-around-the-world/

260 https://thecommonwealth.org/our-work/commonwealth-cyber-declaration-programme

261 https://www.southcom.mil/Media/Special-Coverage/Tradewinds-2024/

262 https://attorneygeneralchambers.com/laws-of-saint-lucia/computer-misuse-act

263 https://attorneygeneralchambers.com/laws-of-saint-lucia/criminal-code/section-267#:~:text=Inducing%20sexual%20intercourse%20or%20sexual%20connection%20by%20force%2C%20duress%2C%20etc.

264 https://www.govt.lc/consultancies/request-for-expressions-of-interest-for-the-consulting-services-to-develop-a-computer-incident-response-team-cirt-establishment-plan

265 https://stlucia.loopnews.com/content/digigov-launches-new-services-service-bureaus-ict-centers

266 https://www.oas.org/ext/en/security/prog-cyber

267 https://thecommonwealth.org/news/caribbean-tackle-escalating-cybercrime-regional-approach

268 https://www.coe.int/en/web/cybercrime/-/octopus-project-online-workshop-on-cybercrime-legislation-and-electronic-evidence-organised-with-national-authorities-from-saint-lucia

269 https://www.pgaction.org/pdf/2023/2023-07-06-presentation-by-hon-alvina-reynolds-president-of-senate-saint-lucia.pdf

270 https://www.lac4.eu/event/advanced-cyber-incident-response-cyber-threat-hunting-endpoint-security-training-programs

271 https://cyberpolicyportal.org/states/saint-vincent-and-the-grenadines

272 https://dig.watch/resource/st-vincent-and-the-grenadines-cybercrime-act-2016

273 St-Vincent-&-the-Grenadines-Cybercrime-Bill-2016.pdf

274 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

275 Cite the country indicator in the Report.

276 https://www.worldbank.org/en/news/press-release/2020/06/22/first-time-financing-by-world-bank-for-digital-economy-in-the-eastern-caribbean-approved-for-us94-million

277 https://oecs.int/en/driving-the-digital-transformation-in-the-eastern-caribbean

278 https://www.caricomimpacs.org/articles/caricom-impacs-hosts-final-workshop-to-develop-cirt-establishment-plan

279 https://www.lac4.eu/event/advanced-cyber-incident-response-cyber-threat-hunting-endpoint-security-training-programs

280 https://www.isoc.vc/

281 https://dtp.gov.vc/index.php/news/29-government-s-e-payment-platform-underway

282 OAS, 2017 Cybersecurity Report, p. 161

283 https://conciber.sr/estrategia-ciberseguridad-2024/

284 https://csirt.sr/status/

285 https://www.coe.int/en/web/octopus/-/suriname

286 https://caricom.org/caricom-usaid-partner-on-cyber-resilience-strategy-2030-project/

287 https://www.caricomimpacs.org/articles/regional-in-country-cyber-awareness-and-cyber-security-sensitization-and-training-2023-in-paramaribo-suriname

288 https://www.coe.int/en/web/cybercrime/glacyplus

289 https://thegfce.org/

290 https://www.southcom.mil/Media/Special-Coverage/Tradewinds-2024/

291 https://gov.sr/ministeries/kabinet-van-de-president/e-government/educatie/cisco/

292https://gov.sr/cisco-certified-support-technician-ccst-training-voor-ict-medewerkers-van-de-overheid/

293 https://conciber.sr/legislacion-ciberseguridad/

294 https://www.dna.sr/media/138146/S.B._2015_no._44_wet_van_30_mrt_15_wijz._wetboek_van_strafrecht.pdf

295 https://politie.sr/digitale-recherche-kps-beschikt-over-app-nummer-8744580/

296 https://csirt.sr/status/

297 https://www.dna.sr/wetgeving/surinaamse-wetten/wetten-na-2005/id-kaartenwet-2018/

298 https://www.dna.sr/media/192966/SB_2017___86.pdf

299 https://gov.sr/digitale-id/

300 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/TrinidadTobago_2012_National_Cyber_Security%20Strategy_Final.pdf

301 https://mdt.gov.tt/digital-transformation-strategy/

302 https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Trinidad_y_Tobago_Vision_%202030_2016_2030_tiny.pdf

303 https://www.iadb.org/en/project/TT-L1061

304 https://www.caf.com/en/currently/news/caf-approves-usd-120-million-to-support-trinidad-and-tobago-s-digital-transformation/

305 https://www.elibrary.imf.org/view/journals/002/2024/151/article-A004-en.xml

306 https://ttcsirt.gov.tt/about-us/

307 https://newsday.co.tt/2024/02/11/issues-arising-from-new-cybercrime-laws/

308 https://www.ttcs.tt/2017/05/06/cybercrime-bill-2017/

309 https://ttcsirt.gov.tt/wp-content/uploads/2024/07/Data_Protection_Act_2011.pdf

310 https://education.apwg.org/download/document/247/STC_CAMPAIGN_DATA_SHEET_OAS_APWG_NCSA.pdf

311 https://www.caricomimpacs.org/articles/caricom-impacs-bolsters-regional-skills-in-cyber-security

312 https://www.lac4.eu/successful-training-for-caricom-countries-government-representatives-and-cybersecurity-experts-concluded

313 https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

314 https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciberseguridad-del-uruguay-2024-2030/estrategia

315 https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciberseguridad-del-uruguay-2024-2030/estrategia

316 https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-sociedad-digital-resiliente/agenda-uruguay - https://www.iadb.org/es/proyecto/UR-L1152 - https://www.impo.com.uy/bases/leyes/20212-2023 - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/ - https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/ - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/cocreacion-estrategia-nacional-ciberseguridad - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/curso-ciberseguridad-abierto-toda-ciudadania - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/infografias-sobre-roles-ciberseguridad - https://www.anep.edu.uy/programas-ebi-2023-2023 - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/seguro-te-conectas - https://capacitacion.agesic.gub.uy/course/index.php?categoryid=10 - https://moodlesinae.presidencia.gub.uy/moodlesinae/ - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/datos-y-estadisticas/estadisticas/formacion-ciberseguridad - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/datos-y-estadisticas/estadisticas/caracterizacion-demanda-formacion-ciberseguridad - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/posgrados-especializaciones-ciberseguridad - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/oferta-educativa-desarrollo-profesional-ciberseguridad - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/sintesis-del-plan-estudios-carrera-analista-tecnico-ciberseguridad - https://www.impo.com.uy/bases/leyes-originales/20327-2024 - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/marco-ciberseguridad - https://www.gub.uy/agencia-reguladora-compras-estatales/ - https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/reportar-incidente

REFERENCES

i. https://www.pressoffice.gov.bz/wp-content/uploads/2019/12/belize-cybersecurity-strategy-2020-2023.pdf

ii. https://cito.gov.bz/cyber-security/

iii. https://www.belizepolice.bz/

iv. https://www.belizepolice.bz/index.php?option=com_content&view=category&id=51

v. https://lovefm.com/police-to-launch-cybercrime-education-campaign/

vi. https://cito.gov.bz/blog/

vii. https://www.getsafeonline.bz/

viii. https://www.sjc.edu.bz/files/ugd/343ada_44fa967053f24aa99c5192ec4e224eb6.pdf

ix. https://www.instagram.com/universityofbelize/p/Cyg_prfp0DB/

x. https://bco.gov.bz/

xi. https://www.dnp.gov.co/LaEntidad/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

xii. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

xiii. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208390:Gobierno-Nacional-crea-Modelo-de-Gobernanza-para-liderar-coordinacion-entre-actores-del-entorno-digital

xiv. https://ciberpaz.gov.co/portal/

xv. https://cibereduca.renata.edu.co/

xvi. https://www.colombiaaprende.edu.co/contenidos/coleccion/generacion-digital-segura

xvii. https://www.mineducacion.gov.co/portal/salaprensa/Comunicados/419639:Mujeres-colombianas-pueden-inscribirse-al-curso-gratuito-de-Ciberseguridad-hasta-el-29-de-febrero

xviii. https://www.oecd.org/en/publications/building-a-skilled-cyber-security-workforce-in-latin-america_9400ab5c-en.html

xix. https://hecaa.mineducacion.gov.co/consultaspublicas/programas

xx. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

xxi. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MGRSD/

xxii. https://www.colcert.gov.co/800/w3-channel.html

xxiii. https://www.colcert.gov.co/800/w3-article-208774.html#:~:text=El%20CSIRT%20de%20Gobierno%20brinda,de%20conciencia%20en%20seguridad%20digital.

xxiv. https://www.mindefensa.gov.co/ministerio/csirt

xxv. https://cc-csirt.policia.gov.co/

xxvi. https://revistasumma.com/costa-rica-micitt-e-ina-lanzan-programa-de-becas-de-ciberseguridad-para-mujeres/

xxvii. https://www.youtube.com/watch?v=wBkhCJZmSbY

xxviii. Draft Cybersecurity Bill No. 23.292 en https://www.asamblea.go.cr/Centro_de_informacion/Consultas_SIL/SitePages/ConsultaProyectos.aspx

xxix. https://www.micitt.go.cr/gobierno-digital/ciberseguridad

xxx. https://cardtp.gov.dm/index.php/about-the-project/project-components/component-1-digital-enabling-environment

xxxi. https://emonewsdm.com/the-caribbean-digital-transformation-project-conducts-four-day-training-oncybersecurity-for-the-establishment-of-a-national-cybersecurity-incident-responseteam-csirt-in-the-commonwealth-of-dominica/

xxxii. https://nbdominica.com/cybersecurity-awareness-competition/

xxxiii. https://www.facebook.com/domleconline/photos/cybersecurity-awareness-month-2024-being-cyber-secure-is-very-mindful-very-demur/1351414602866973/?_rdr

xxxiv. https://www.csirt.gov.gd/

xxxv. https://www.getsafeonline.gd/

xxxvi. https://www.laws.gov.gd/index.php/acts/search-result?filter_category_id=1344&filter_search=Electronic%20Crimes%20Act&show_category=0&searchphrase=all&show_searchform=0

xxxvii. https://www.laws.gov.gd/index.php/acts/search-result?filter_category_id=1344&filter_search=data%20protection&show_category=0&searchphrase=all&show_searchform=0

xxxviii. https://www.iadb.org/en/project/HA-J0010

xxxix. https://www.obsnumerique.org/tag/cybersecurite/

xl. http://www.conatel.gouv.ht/node/565

xli. https://www.diger.gob.hn/sites/default/files/2024-02/Plan%20de%20Gobierno%20Digital%20Honduras.pdf

xlii. https://ahiba.hn/mes-de-ciberseguridad/

xliii. https://www.youtube.com/watch?v=zgpwsgT1SE0

xliv. https://upi.edu.hn/educacion-continua/

xlv. https://iies.unah.edu.hn/vinculacion/pcemp/ciberseguridad/

xlvi. https://udh.edu.hn/views/course/OA-DCC.html

xlvii. https://www.uth.hn/executive-education/cursos-2/cursos-tegucigalpa/curso-ciberdelitos-en-instituciones-financieras/

xlviii. https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf

xlix. https://www.tsc.gob.hn/biblioteca/index.php/codigos/168-codigo-penal

l. https://www.cert.gov.py/estrategia-nacional-de-ciberseguridad/

li. https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

lii. https://www.cert.gov.py/wp-content/uploads/2024/07/CNC_mayo-2024.pdf

liii. https://www.cert.gov.py/wp-content/uploads/2024/01/RESOLUCION-MITIC-N%C2%B0-032-2024-Coordinador-Nacional-de-Ciberseguridad.pdf

liv. https://www.cert.gov.py/rfc-2350/

lv. https://www.cert.gov.py/ciberejercicios-simulacro-de-ciberataque/

lvi. https://www.cert.gov.py/modelo-de-gobernanza-de-seguridad-de-la-informacion/

lvii. https://www.conectateseguro.gov.py/

lviii. https://mitic.gov.py/gobierno-esta-siempre-abierto-al-dialogo-y-a-romper-la-desinformacion-senala-ministro/

lix. https://www.cert.gov.py/estandares-y-normas/reglamentacion-sobre-reporte-obligatorio-de-incidentes-ciberneticos-de-seguridad-en-el-estado/#

lx. https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-sociedad-digital-resiliente/agenda-uruguay

lxi. https://www.iadb.org/es/proyecto/UR-L1152

lxii. https://www.impo.com.uy/bases/leyes/20212-2023

lxiii. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/

lxiv. https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/

lxv. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/cocreacion-estrategia-nacional-ciberseguridad

lxvi. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/curso-ciberseguridad-abierto-toda-ciudadania

lxvii. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/infografias-sobre-roles-ciberseguridad

lxviii. https://www.anep.edu.uy/programas-ebi-2023-2023

lxix. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/seguro-te-conectas

lxx. https://capacitacion.agesic.gub.uy/course/index.php?categoryid=10

lxxi. https://moodlesinae.presidencia.gub.uy/moodlesinae/

lxxii. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/datos-y-estadisticas/estadisticas/formacion-ciberseguridad

lxxiii. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/datos-y-estadisticas/estadisticas/caracterizacion-demanda-formacion-ciberseguridad

lxxiv. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/posgrados-especializaciones-ciberseguridad

lxxv. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/oferta-educativa-desarrollo-profesional-ciberseguridad

lxxvi. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/sintesis-del-plan-estudios-carrera-analista-tecnico-ciberseguridad

lxxvii. https://www.impo.com.uy/bases/leyes-originales/20327-2024

lxxviii. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/marco-ciberseguridad

lxxix. https://www.gub.uy/agencia-reguladora-compras-estatales/

lxxx. https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/reportar-incidente

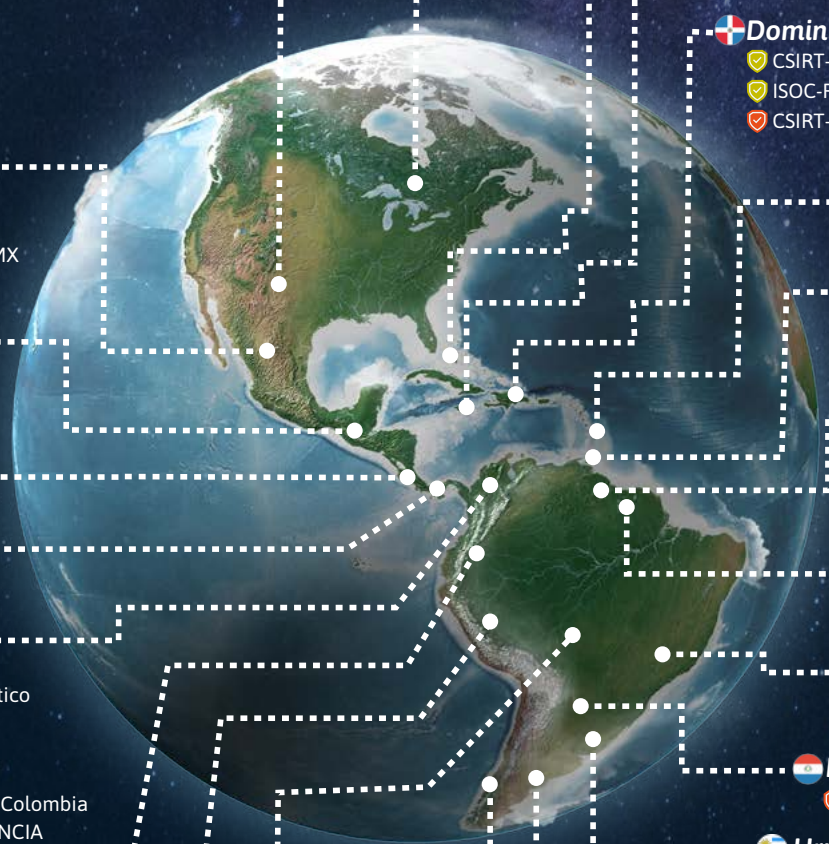
INTERNET CONNECTIVITY DATA

Country	Population	Cell Phone Subscriptions	Persons with Internet Access	Internet Penetration (%)	Government Electronic Strategies	EGDI (2022)
Antigua and Barbuda	94,149	202,700 (2024)	86,400 (2024)	91,4% (2024)	TBA	0.6864
Argentina	46 million	62.7 million (2023)	42 million	91%	National Digital Agenda	0.8112
Bahamas	400,000	0.318 million	340,000	85%	E-Government Strategy	0.7488
Barbados	287,000	0.13 million	260,000	90%	Barbados Digital Strategy	0.7453
Belize						0.5907
Bolivia	~12 million	10.2 million	~7.8 million	~65%	Digital Government Plan	0.6308
Brazil	~215 million	258 million	~180 million	~84%	Digital Transformation Strategy	0.7662
Chile	~19 million	26.22 million	~17 million	~89%	Digital Government Strategy	0.8653
Colombia	~52 million	83.3 million	~45 million	~87%	Digital Government Plan	0.7879
Costa Rica	~5 million	7.1 million	~4.5 million	~90%	National Digital Strategy	0.7779
Dominica						0.6351
Dominican Republic	~11 million	9.73 million	~8 million	~73%	E-Government Strategy	0.6788
Ecuador	~18 million	17.5 million	~12 million	~67%	Digital Government Plan	0.7356
El Salvador	~6.5 million	8.8 million	~4.5 million	~69%	Digital Government Strategy	0.6777
Grenada						0.6750
Guatemala	~18 million	19.1 million	~10 million	~55%	National Digital Agenda	0.6267
Guyana						0.6038
Haiti						0.3916
Honduras						0.6427
Jamaica						0.7267
Mexico						0.7798
Panama	~4.5 million	4.96 million	~3.5 million	~78%	Digital Government Plan	0.7356
Paraguay	7,031,341	9.18 million			National Cybersecurity Strategy, Digital ID Law No. 7177/2023	0.6669
Peru	35,015,825	41.3 million	27.9 million	79.5%	National Digital Transformation Program, IDB support	0.7251
St. Kitts and Nevis	55,229	54,000	35,800	76.4%	National ICT Strategic Plan, eTA portal, Digital ID system	0.6448
St. Lucia	184,000					0.6691
St. Vincent and the Grenadines	103,613					0.6653
Suriname	639,860					0.6317
Trinidad and Tobago	1,540,942					0.7326
Uruguay	~3.5 million	~5 million	~3.3 million	~94%	Digital Government Strategy	0.8508

MAP of CSIRTS Americas

CSIRT Type

National Military Government



Canada
- CCCS

United States of America
- US-CERT

Mexico
- CERT-MX
- Defensa-CERT
- CSIRT-SEMAR-MX

Guatemala
- CRIC-GT
- CSIRT-GT

Costa Rica
- CSIRT-CR

Panama
- CSIRT Panamá

Colombia
- COCIB
- CSIRT Aeronáutico
- CSIRT-CCOCI
- CSIRT-PONAL
- CSIRT-EJC
- CSIRT-Defensa Colombia
- CSIRT-PRESIDENCIA
- colCERT

Ecuador
- COCIBER
- CSIRT-ARE
- CSIRT Ecuador
- EcuCERT

Peru
- CITELE-EP
- CSIRT-CCFFAA
- CSIRT-MGP
- CSIRT-FAP
- CSIRT-COCID
- CSTPERU
- CSIRT-MGP

Bolivia
- CSIRT-Bolivia

Chile
- CCCD
- CSIRT Armada
- CSIRT-CL

Argentina
- CERTUNLP
- BA-CSIRT
- CSIRT Córdoba
- CSIRT-MINSEG
- CSIRT-NQN
- CSIRT-PBA
- CERT.ar

Uruguay
- CERTuy
- DCSIRT

Paraguay
- CERT-PY

Brazil
- CTIR Gov

Suriname
- SURCSIRT

Guyana
- CIRT.GY

Trinidad and Tobago
- TT-CSIRT

Barbados
- CIRT-BB

Dominican Republic
- CSIRT-Defensa
- ISOC-RD
- CSIRT-RD

Jamaica
- JaCIRT

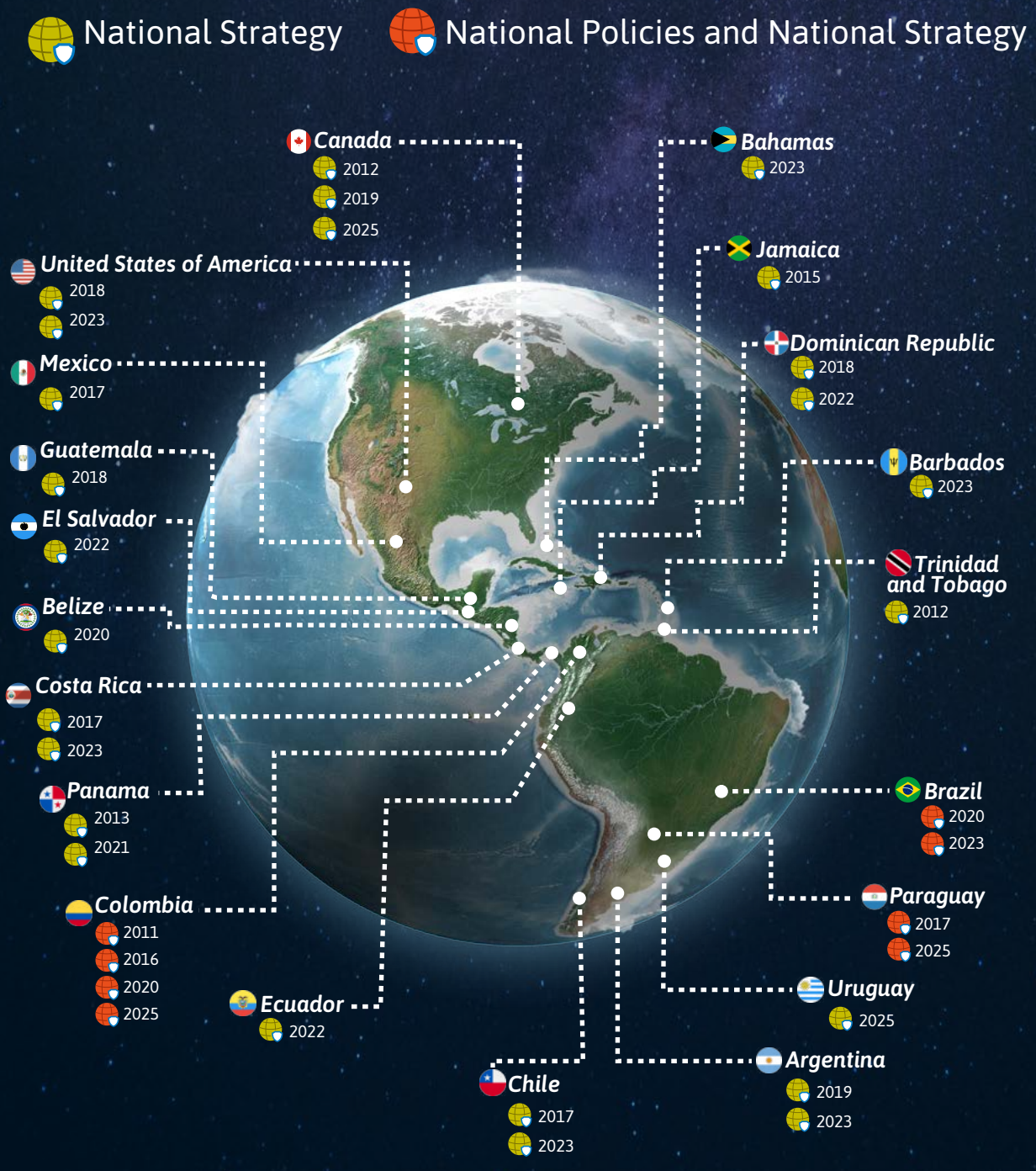
Bahamas
- CIRT-BS

* The CSIRTAmericas Network of the Organization of American States (OAS) includes 52 CSIRTs representing 22 member countries.

Country	Type	CSIRT	CSIRT Website	Host Institution	CSIRT Americas
Argentina	Government	BA-CSIRT	Link	Ciudad de Buenos Aires	Yes
	Government	CERTUNLP	Link	Universidad Nacional de la Plata	Yes
	National	CERT.ar	Link	Jefatura de Gabinete de Ministros Argentina (Dirección Nacional de Ciberseguridad)	Yes
	Government	CSIRT Córdoba	Link	Provincia de Córdoba (varias entidades)	Yes
	Government	CSIRT-MINSEG	Link		Yes
	Government	CSIRT-NQN	Link	Gobierno de la Provincia del Neuquén (SEGPyCE, Subsecretaría de la Gestión Pública, OPTIC)	Yes
	Government	CSIRT-PBA	Link	Subsecretaría de Gobierno Digital (Departamento de Seguridad Informática)	Yes
Bahamas	National	CIRT-BS	Link	Ministry of Economic Affairs	Yes
Barbados	National	CIRT-BB	Link	Government of Barbados	Yes
Bolivia	National	CSIRT-Bolivia	Link	Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (Centro de Gestión de Incidentes Informáticos)	Yes
Brazil	National	CTIR Gov	Link	Gabinete de Seguridad Institucional	Yes
Canada	National	CCCS	Link	Communications Security Establishment	Yes
Chile	Military	CCCD	Link	Estado Mayor Conjunto (EMCO)	Yes
	Military	CSIRT Armada	Link	Armada de Chile	Yes
	National	CSIRT-CL	Link	Agencia Nacional de Ciberseguridad	Yes
Colombia	Military	COCIB	Link	Armada Nacional	Yes
	Military	CSIRT-Aeronáutico	Link	Fuerza Aeroespacial Colombiana	Yes
	Military	CSIRT-CCOCI			Yes
	Government	CSIRT-Defensa Colombia	Link	Ministerio de Defensa	Yes
	Military	CSIRT-EJC	Link	Ejército Nacional	Yes
	Military	CSIRT-PONAL	Link	Policía Nacional	Yes
	Government	CSIRT-PRESIDENCIA	Link	Presidencia de la República	Yes
	National	ColCERT	Link	Ministerio de Tecnologías de la Información y las Comunicaciones	Yes
Costa Rica	National	CSIRT-CR	Link	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones	Yes
Dominican Republic	Government	CSIRT-Defensa			Yes
	National	CSIRT-RD	Link	Centro Nacional de Ciberseguridad	Yes
	Government	ISOC-RD			Yes
Ecuador	Military	COCIBER		Comando de Ciberdefensa	Yes
	National	CSIRT Ecuador	Link	Gobierno Nacional	Yes
	Military	CSIRT-ARE	Link	Armada Nacional	Yes
	Government	EcuCERT	Link	Agencia de Regulación y Control de las Telecomunicaciones del Ecuador	Yes
Guatemala	Military	CRIC-GT			Yes
	National	GTCERT	Link	Ministerio de Gobernación	Yes
Guyana	National	CIRT.GY	Link	Office of the Prime Minister (National Data Management Authority)	Yes
Jamaica	National	JaCIRT	Link	Ministry of Science, Energy, and Technology	Yes
Mexico	Military	CERT-MX	Link	Guardia Nacional (Dirección General Científica)	Yes
	National	CSIRT-SEMAR-MX	Link	Secretaría de Marina	Yes
	Military	Defensa-CERT	Link	Secretaría de la Defensa Nacional	Yes

Panama	*National*	CSIRT Panamá	Link	*Autoridad Nacional para la Innovación Gubernamental*	Yes
Paraguay	*National*	CERT-PY	Link	*Ministerio de Tecnologías de la Información y Comunicación*	Yes
Peru	*Military*	CITELE-EP	Link	*Comando de Telemática del Ejército*	Yes
	Military	CSIRT-CCFFAA	Link	*Comando Conjunto de las FF.AA*	Yes
	Government	CSIRT-COCID	Link	*Fuerzas Armadas del Perú*	Yes
	Military	CSIRT-FAP	Link	*Fuerza Aérea del Perú*	Yes
	Government	CSIRT-GRSM	Link	*Gobierno Regional San Martín*	Yes
	Military	CSIRT-MGP	Link	*Marina de Guerra del Perú*	Yes
	National	PeCERT	Link	*Secretaria de Gobierno y Transformación Digital (Centro Nacional de Seguridad Digital)*	Yes
Suriname	*National*	SURCSIRT	Link	*De Centrale Inlichting en Veiligheidsdienst (CIVD)*	Yes
Trinidad and Tobago	*National*	TT-CSIRT	Link	*Ministry of National Security*	Yes
United States of America	*National*	US-CERT	Link	*Department of Homeland Security (America's Cyber Defense Agency)*	Yes
Uruguay	*National*	CERTuy	Link	*Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC)*	Yes
	Military	DCSIRT-UY	Link	*Ministerio de Defensa Nacional*	Yes

Map of National Cybersecurity Strategies and Cybersecurity Legislation



Across the Americas, a total of 34 National Cybersecurity Strategy formulation processes have been undertaken in 21 countries. The Organization of American States, through its Secretariat of the Inter-American Committee against Terrorism (OAS/CICTE), has provided support in 21 of these processes, spanning 16 countries.

LIST OF ACRONYMS

ABIF - Chilean-American Chamber of Commerce

ACE - State Cybersecurity Agency of El Salvador

AECI - Ecuadorian Cybersecurity Association

AGCID - Chilean Agency for International Development Cooperation

AGESIC - Agency for the Development of Electronic Government and the Information and Knowledge Society of Uruguay

AGETIC - E-Government and the Information and Communication Technologies Agency of Bolivia

AHIBA - Honduran Association of Banking Institutions

AIEP - Andrés Bello University Academy of Languages and Professional Studies

AIG - Authority for Government Innovation of Panama

ALADI - Latin American Integration Association

AMCS - Mexico CyberSecure Alliance

ANCI - National Cybersecurity Agency of Chile

ANDJE - National Agency for Legal Defense of the State of Colombia

ANPD - National Data Protection Authority of Brazil

ANRA - National Agenda of Threats and Risks of Guatemala

ANTAI - National Authority for Transparency and Access to Information of Panama

APEPCIT - Peruvian Association of Professionals in Cybersecurity

ARCOTEL - Agency for the Regulation and Control of Telecommunications of Ecuador

ASFI - Supervisory Authority for the Financial System

ATDT - Digital Transformation and Telecommunications Agency of Mexico

BA-CSIRT - Buenos Aires Computer Security Incident Response Team

BanCERT - Cybersecurity Banking Community of Guatemala

BCO - Belize Crime Observatory

BCRP - Digital Government Plan of the Central Reserve Bank of Peru

BDF - Barbados Defence Force

BPD - Belize Police Department

CAF - Latin American and Caribbean Development Bank

CAHSI - Honorary Advisory Council on Information Security of Uruguay

CAIS - Security Incident Response Center of Brazil

Camp@LAC4 - Women in CyberTech Camp

CARDTP - Caribbean Digital Transformation Project

CARICOM - Caribbean Community

CARICOM IMPACS - CARICOM Implementation Agency for Crime and Security

CBMs - Confidence-Building Measures

CCCD - Defense CSIRT Coordinating Center of Chile

CCCS - Canadian Centre for CyberSecurity

CCMIN - Mining Cybersecurity Corporation of Chile

CCN - National Cryptologic Center of Spain

CCSCAP - CARICOM Caribbean Cybersecurity and Cybercrime Action Plan

CCST - Cisco Certified Support Technician

CDTP - Caribbean Digital Transformation Project

CERT - Computer Emergency Response Team

CERT.ar - National CSIRT of Argentina

CERT.br - National CSIRT of Brazil

CERT-MX - National CSIRT of Mexico

CERT-PY - National CSIRT of Paraguay

CERT-UNLP - CSIRT of La Plata National University

CERTuy - National CSIRT of Uruguay

CGE - Strategic Management Council of Uruguay

CGII - Cyber Incident Management Center of Bolivia

CIBERCOM-AM - Cyber Command of the Navy of Mexico

CiberLAC - Network of Excellence in Cybersecurity in Latin America and the Caribbean

CICTE - Inter-American Committee Against Terrorism

CIO - Chief Information Officer

CIRT - Computer Incident Response Team

CIRT-BB - National CSIRT of Barbados

CIRT-BS - National CSIRT of The Bahamas

CIRT.GY - National CSIRT of Guyana

CISC Gov.br - Brazilian Digital Government Integrated Cybersecurity Center

CITICSI - National Inter-Ministerial Commission on Information and Communication Technologies and Information Security of Mexico

CITO - Central Information Technology Office of Belize

CIVD - Central Intelligence and Security Agency of Suriname

CMM - Cybersecurity Capacity Maturity Model

CNBS - National Banking and Insurance Commission of Honduras

CNCS - National Cybersecurity Center of the Dominican Republic

CNCiber - National Cybersecurity Committee of Brazil

CNI - Critical National Infrastructure

CNSD - National Center for Digital Security of Peru

COCIB - Naval Cyber Command of Colombia

ColCERT - National CERT of Colombia

CONATEL - National Telecommunications Commission of Honduras

CONCIBER - National Cybersecurity Committee of Guatemala

CONPES - National Council for Economic and Social Policy of Colombia

COS - Security Operations Centers of Colombia

CRI - International Counter Ransomware Initiative

CSIRT Aeronáutico - CSIRT of the Colombian Aerospace Force

CSIRT Armada - CSIRT of the Navy of Chile

CSIRT Bolivia - National CSIRT of Bolivia

CSIRT Cordoba - CSIRT of the Province of Córdoba

CSIRT-CCFFAA - CSIRT of the Joint Command of the Armed Forces of Peru

CSIRT-COCID - CSIRT of the Cyber Defense Operational Command of Peru

CSIRT-CR - National CSIRT of Costa Rica

CSIRT-Defensa Colombia - CSIRT of the Ministry of Defense of Colombia

CSIRT-EJC - CSIRT of the National Army of Colombia

CSIRT-FAP - CSIRT of the Peruvian Air Force

CSIRT-GRSM - CSIRT of the Regional Government of San Martín

CSIRT-GT - National CSIRT of Guatemala

CSIRT-CL - National CSIRT of Chile

CSIRT-NQN - CSIRT of the Province of Neuquén

CSIRT-Panama - National CSIRT of Panama

CSIRT-PBA - CSIRT of the Province of Buenos Aires

CSIRT-PONAL - CSIRT of the National Police of Colombia

CSIRT-PRESIDENCIA - CSIRT of the Presidency of Colombia

CSIRT-RD - National CSIRT of the Dominican Republic

CSIRT-SEMAR-MX - CSIRT of the Secretariat of the Navy of Mexico

CSIRTs - Computer Security Incident Response Teams

CSIRT Ecuador - CSIRT of the Government of Ecuador

CSIRT Gov - CSIRT of the Government of Colombia

Cyber4Dev - Cyber Resilience for Development Project

DCIBER - Directorate for Combating Cybercrime of Brazil

DCSIRT-UY - CSIRT of the Ministry of National Defense of Uruguay

Defensa-CERT - CSIRT of the Secretariat of Defense of Mexico

DIAN - National Tax and Customs Directorate of Colombia

DIGER - Results-Based Management Directorate of Honduras

DIGETIC/FFAA - General Directorate of Information and Communication Technologies of the Armed Forces of Paraguay

DINI - National Intelligence Directorate of Peru

E-ID - Electronic Identification

EBI - Integrated Basic Education Programs of Uruguay

EcuCERT - National CSIRT of Ecuador

EDGI - Environmental Data & Governance Initiative

EGDI - UN E-Government Development Index

EPN - National Polytechnic School of Ecuador

EU - European Union

EU CyberNet - European Union Cyber Capacity Building Network

FIRST - Forum of Incident Response and Security Teams

FORCIC - Program for the Strengthening of Cybersecurity and Cybercrime

FSSC - Financial System Stability Committee of Jamaica

GACCTI - Special Task Force for Combating Cybercrime and Offenses Committed through the Use of Information Technologies of Brazil

GBC - Gender-based crimes

GBV - Gender-based violence

GCI - Global Cybersecurity Index

GCSCC - Global Cybersecurity Capacity Centre

GFCE - Global Forum on Cyberexpertise

GLACY+ - Global Action on Cybercrime Extended Project

GLACY-e - Global Action on Cybercrime Enhanced Project

GPEN - Global Prosecutors E-Crime Network

GSI - Institutional Security Cabinet of Brazil

ICCN - National Critical Cyber Infrastructure of Colombia

ICT - Information and communication technology

IDB - Inter-American Development Bank

IEC - International Electrotechnical Commission

IFT - Federal Telecommunications Institute of Mexico

iGOVTT - National Information and Communication Technology Company Limited of Trinidad and Tobago

IMF - International Monetary Fund

INACAP - National Professional Training Institute of Chile

INEES - National Institute of Strategic Security Studies of Guatemala

INTEC - Santo Domingo Institute of Technology

INTECAP - Technical Institute for Training and Productivity of Guatemala

IoCs - Indicators of Compromise

ISACA - Information Systems Audit and Control Association

ISC2 - International Information System Security Certification Consortium

ISO - International Organization for Standardization

ISOC - Internet Society Organization

ISPs - Internet Service Providers

IT - Information Technology

ITLA - Technological Institute of the Americas of the Dominican Republic

ITU - International Telecommunications Union

ITU-IMPACT - International Multilateral Partnership Against Cyber Threats

JaCIRT - National CSIRT of Jamaica

JTDA - Jamaica Technology & Digital Alliance

LAC - Latin America and the Caribbean

LAC4 - Latin America and Caribbean Cyber Competence Centre

LFPDPPP - Federal Law on the Protection of Personal Data Held by Individuals of Mexico

LFPPI - Federal Law on the Protection of Industrial Property of Mexico

LGDNNA - General Law on the Rights of Children and Adolescents of Mexico

LGPD - General Data Protection Law of Brazil

LGPDPPSO - General Law on the Protection of Personal Data in Possession of Obliged Subjects of Mexico

LOPDP - Organic Law on the Protection of Personal Data of Ecuador

MDT - Ministry of Digital Transformation of Trinidad and Tobago

MEF - Ministry of Economy and Finance of Ecuador

MERCOSUR - Southern Common Market

MICITT - Ministry of Science, Innovation, Technology, and Telecommunications of Costa Rica

MinTIC - Ministry of Technology and Communications of Colombia

MITIC - Ministry of Information and Communication Technologies of Paraguay

MoUs - Memoranda of Understanding

MSPI - Information Security and Privacy Framework of Colombia

NCRA - National Cyber Risk Assessment of Guyana

NCS - National Cybersecurity Strategy

NDI - National Defense Institute of Guyana

NDMA - National Data Management Authority of Guyana

NGO - Non-governmental organization

NIST - National Institute of Standards and Technology

NSCS - National Security Council Secretariat of Belize

OAS - Organization of American States

OECD - Organization for Economic Cooperation and Development

OECS - Organization of Eastern Caribbean States

OEE - State Agencies and Entities of Paraguay

OIV - Operators of Vital Importance of Chile

ONP - Pension Normalization Office of Peru

PeCERT - National CSIRT of Peru

PCI - Payment Card Industry

PCI DSS - Payment Card Industry Data Security Standard

PDI - Investigations Police of Chile

PITU - Police Information Technology Unit of Belize

PMC - Council of Minister Presidency of Peru

PNE - National Police of Ecuador

PUC - Public Utilities Commission of Belize

REDGEALC - Inter-American Network on Digital Government

RNP - National Education and Research Network

RSS - Regional Security System of Barbados

SENAE - National Customs Service of Ecuador

SGD - Digital Government Secretariat

SGTD - Digital Government and Transformation Secretariat of Peru

SICA - Central American Integration System

SINA - National Intelligence System of Peru

SINAE - National Emergency System of Uruguay

SISP - Information Technology Resources Management System of Brazil

SMEs - Small- and medium-sized enterprises

SOC - Security Operations Center

SPRICS - Payment System Cybersecurity Incident Response Center of the Dominican Republic

SSPC - Secretariat of Security and Citizen Protection of Mexico

SURCSIRT - National CSIRT of Suriname

SWIFT - Society for Worldwide Interbank Financial Telecommunication

TAJ - Tax Administration Jamaica

TLS - Transport Layer Security

TT-CSIRT - National CSIRT of Trinidad and Tobago

TW24 - Tradewinds 2024 Training Exercise

UAFE - Unit for Financial and Economic Analysis of Ecuador

UMSA - Universidad Mayor de San Andrés of Bolivia

UMSS - Universidad Mayor de San Simon of Bolivia

UN - United Nations

UNICEF - United Nations Children's Fund

UNIDIR - United Nations Institute for Disarmament Research

UNPUH - Pedro Henríquez Ureña National University of the Dominican Republic

URCA - Utilities Regulation and Competition Authority of The Bahamas

US-CERT - National CSIRT of the United States of America

USAID - United States Agency for International Development

USFX - Universidad San Francisco Xavier of Bolivia

UWI - University of the West Indies

VPN - Virtual Private Network


IDB
ORGANIZATION OF AMERICAN STATES
OAS
CICTE