



Cybersecurity sector in Central America

SECTOR FICHE

1. Policy and regulatory framework

The Budapest Convention on Cybercrime¹ serves as a checklist for the development of domestic substantive and procedural law on cybercrime and electronic evidence. In Central America, only Costa Rica and Panama have ratified the Budapest Convention.

The Global Cybersecurity Index (GCI) is published by the International Telecommunication Union (ITU). It assesses cybersecurity preparedness of member states based on the analysis of five pillars: a) Legal, b) Technical, c) Organizational, d) Capacity Development and e) Cooperation. The Table below shows the position of each Central American country out of 175 member states evaluated.

Table. GCI ranking of Central American countries (2020)

Source: ITU

Country	Score	Regional Rank 2020	Regional Rank 2018	Global Rank 2020	Global Rank 2018
Panama	34.11	14	13	103	97
Guatemala	13.13	26	16	150	112
Costa Rica	67.45	18	8	76	115
Nicaragua	9	32	26	165	140
El Salvador	13.3	25	27	148	142
Honduras	2.2	35	32	178	165

As shown in the previous table, Costa Rica is the only Central American country that has advanced positions since the previous Global ranking (from 115 to 76), while its position in the Regional ranking has deteriorated (8 to 18).

Costa Rica has updated its national legislation creating a legal development of protection for the Costa Rican cyber society, allowing the possibility that people report violations suffered in the virtual world that previously had no legal response. Among them, stands out the Law of Protection of the Person against the treatment of his Personal Data and its Regulation, creating in this way the Agency of Protection of Data of the Inhabitants (PRODHAB). In 2012, Costa Rica approved Legislative Decree No. 9048 that reformed the criminal code to formally introduce provisions for cybercrime. It also has the Computer Crime Law No. 9048. However, despite having the

¹ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

regulations that allow and promote the use of the signature and digital certificates, it does not have a national cryptographic approach policy; that is, of technical and legal standards that cover the whole of the State in a single instrument for document management and authentication.

Costa Rica lacks a cybersecurity policy. By the end of 2017, the MICITT (Science, Technology and Telecommunications Ministry) presented what is called the National Cybersecurity Strategy (ENC)², a normative foundation comprehensive but which, however, does not represent an effective legal instrument in terms of securing the cyber security of the ICT user population.

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

Decree 40.862-MP-PLAN-MICITT lays the foundations for the creation of a Directorate of Digital Governance (DGD). This would aim to closely coordinate the Digital Signature and Information Security addresses and expand their functions with a project management perspective to centralize decision-making in ICT matters for the Central Government.

The Computer Security Incident Response Center (CSIRT) is in charge of ensuring cybersecurity in Costa Rica. It was open in 2015. This center is located in the facilities of the MICITT in Zapote, San José. In addition, CSIRT-CR is a member of the CSIRT Americas network.

2022 Cyber-attack in Costa Rica

The cyber-attack on the Government of Costa Rica was an extortive computer attack initiated on the night (UTC-6:00) of Sunday, April 17, 2022 to the detriment of almost thirty public institutions of the Republic of Costa Rica, including its Ministry of Finance, the Ministry of Science, Innovation, Technology and Telecommunications (MICITT), the National Meteorological Institute (IMN), the Radiográfica Costarricense S. A. (RACSA), the Costa Rican Social Security Fund, the Ministry of Labor and Social Security (MTSS), the Social Development and Family Allowances Fund (FODESAF) and the Administrative Board of the Cartago Municipal Electricity Service (JASEC).

The pro-Russian Conti Group claimed the first group of attacks and demanded a ransom of US\$10 million in exchange for not releasing the information stolen from the Ministry of Finance, which could include sensitive information such as the tax returns of citizens and companies operating in Costa Rica.

As a consequence, the government had to shut down the computer systems used to file tax returns, as well as for the control and management of imports and exports, causing losses to the productive sector in the order of US\$30 million per day. The MICITT web pages were also taken offline.

Costa Rica required technical assistance from the United States, Israel, Spain and Microsoft, among others, to deal with the cyber-attack. The attack consisted of infections to computer systems with ransomware, defacement of web pages, theft of e-mail files and attacks to the Social Security's human resources portal, as well as to its official Twitter account.

On May 6, 2022, the U.S. government through the FBI offered a \$10 million reward for information leading to the identification of a person or persons in a leadership position within the Conti Group,

² <https://www.micitt.go.cr/wp-content/uploads/2022/05/englishEstrategia-Nacional-de-Ciberseguridad-Costa-Rica.pdf>

and an additional \$5 million for information leading to the capture or conviction, in any country, of persons who aided or conspired in carrying out Conti ransomware attacks

On May 8, 2022, Costa Rica's new president, Rodrigo Chaves Robles, decreed a state of national emergency due to the cyberattacks, deeming them an act of terrorism. Days later, in a press conference, he stated that the country was in a state of war¹²¹³ and that there was evidence that people inside Costa Rica were helping Conti, for which he called them "traitors" and "filibusters."

On May 31, 2022 in the early hours of the morning, Hive Ransomware Group carried out an attack against the Costa Rican Social Security Fund (CCSS), forcing the institution to shut down all its critical systems, including the Single Digital Health Record (EDUS) and the Centralized Collection System (SICERE). The former stores the sensitive medical information of the patients attended by the Social Security, while the latter is used to collect insurance premiums from the population.

Although **El Salvador** does not currently have a national cybersecurity strategy, one of the objectives of the 2018–2022 E-government Strategy was to have a National Cybersecurity Policy, as a "result of a consultation process involving international experts, academia, government institutions, private sector and civil society organizations."

On May 13, 2022 the government of El Salvador published Executive Order Number 163³, establishing guidelines to prevent and manage cybersecurity risk. The Executive Order, named Cybersecurity Policy of El Salvador (Política de Ciberseguridad de El Salvador), lays out criteria to develop cybersecurity capacities aimed to protect critical infrastructure, strengthen response mechanisms, and develop the technical and administration skills, so that the public and private institutions in El Salvador as well as citizens are aware of cybersecurity and risks related to the use of information technologies.

This document describes creating a committee with key infrastructure operators who use strategic assets, creating a computer emergency response team coordinated by the national emergency response team, and a dedicated computer security incident response and security center (CSIRT).

The policy also includes specific objectives, including: the creation of an entity to coordinate cybersecurity efforts; the promotion of educational campaigns to raise awareness; the adoption of good practices and the creation of specialized protection centers; the analysis of the current laws to promote the creation of a wide-ranging legal framework and the training needed within the judicial sector to investigate and prosecute cybercrimes; also, encourages risk assessment as the method to reduce cyber incidents; and promotes international cooperation through technical assistance and collaboration with international organizations and friendly countries.

The policy will be implemented by all entities within the executive branch. It is also strongly encouraged to be implemented by official institutions, autonomous and private, that manage strategic assets of critical infrastructure within the country which are exposed to cyberthreats and have a relationship with public institutions.

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

In 2016, the Special Law against Computer-Related Crimes was approved with the aim of protecting legal rights against criminal acts committed using ICTs, as well as the prevention of crimes committed against stored, processed, and/or transferred data. Articles 24–26 of Decree No. 260 of the Special Law against Computer-Related Crimes refer to protection against the use, hiring, and transfer, and the undue disclosure, of personal data. In addition, Decree No. 133 of

³ <https://www.diariooficial.gob.sv/>

the Electronic Signature Law protects the personal data needed by service providers. However, there is no comprehensive legislation on the subject, so data protection and privacy are not adequately addressed.

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

It is also worth mentioning that there exists a “Manual to Obtaining Communication Service Provider Evidence from US”, whose purpose is to guide Salvadoran law enforcement agencies on the different mechanisms that exist to request and obtain user's data and digital evidence of Internet service providers strengthening of the capacities of El Salvador National Police to effectively identify and investigate cybercrime cases.

The **Guatemala** 2018 National Cybersecurity Strategy (Estrategia Nacional de Seguridad Cibernética) is the first step towards establishing the guidelines and objectives that were proposed in the National Security Policy and calls to: a) Regulate the protection of digital information systems in the public and private sectors in order to guarantee the continuity of their services; b) Establish coordination organizations (CSIRT-GT) to implement the national cyber security; and c) Design a national protection plan for critical infrastructures for strengthen contingency and recovery plans. Guatemala's CSIRT-GT is an incident response team under the supervision of the Ministry of the Interior 196 and is a member of the CSIRT Americas network.

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

Guatemala's National Plan for an Open Government (Title 4) presents the Electronic Government and online public services. Furthermore, the Digital Government Law develops the legal framework for Digital Identity.

On August 4, 2022, the Congress of the Republic of Guatemala approved Decree 39-2022, which contains the Law on Prevention and Protection against Cybercrime. The law includes criminal sanctions for cyber activities that violate personal data, sensitive computer data, confidentiality, integrity, and availability of information and data stored in computer systems or systems that use information technology and communications to transmit information by such means. The regulations issued seek to strengthen computer security and promote the responsible use of digital tools. In addition, they create the Institutional Security Center for Technical Response to Computer Incidents.

On August 24, 112 deputies to the Congress of the Republic of Guatemala voted in favor of the objections to Decree and as a consequence, the so-called Cybercrime Prevention and Protection Law, created by bill 5601, was shelved.

Due to its filing, the Law will no longer be sent to the Executive for sanction and publication, nor will it take effect. Several experts, academics and several other opponents concluded that said decree is dangerous because it could be used to limit freedom of expression and criminalize comments towards officials and political figures who have been criticized and questioned for the performance of their duties.

A group of deputies who voted in favor considered that the content of the Law could have generated “diverse interpretations” creating a legal gap, which would even serve as a legal tool for repressive purposes, prohibiting the dissemination of images of satire or information about officials or politicians, who could claim to be affected by their honor, dignity, that of their family and other social environments.

Likewise, the law sought to protect Guatemalans and their personal data from cybercriminals, typifying crimes such as harassment by cybernetic means, cyberbullying, cybercrime, cyberdefense, computer fraud and protection of personal data on the Internet.

Since its approval, the Law has generated concern about the possible violation of the constitutional right of the freedom of expression.

Honduras has developed the National Cybersecurity Law and Measures for Protection against Hate and Discrimination Acts on the Internet and Social Networks bill, which identifies the need to create a national cybersecurity strategy as well as an Interinstitutional Cybersecurity Committee that is in charge of strategy development and implementation. In addition, Honduras reached an agreement with Israel in 2016 for cooperation focused on “strengthening the capabilities of prevention, defense and reaction to possible cyberattacks to government institutions, infrastructure managers and critical services.

The Interinstitutional Cybersecurity Committee is tasked with formulating, designing, implementing and monitoring compliance of the National Cybersecurity Strategy. It seeks to establish an Executive Cybersecurity Directorate as the entity in charge of overseeing the execution of the policies approved by the Committee.

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

To protect data and privacy, the bill on the protection of personal information was approved in National Congress after the third and last debate in April 2018. This new law applies to public and private-sector databases.

Honduras' new Penal Code codifies cybercrimes, including hacking, phishing, identity theft, pornography (child and adult) and sexual provocation.

Nicaragua approved a national cybersecurity strategy in 2020⁴, which contains within its axes, among others, the creation of a cybersecurity incident response center and updating of the legal, administrative, criminal and procedural frameworks to allow for the prevention, investigation, judgment, and punishment of cybercrime. Currently, the Cybercrime Unit of the National Police attends cybersecurity incidents together with the Specialized Unit against Organized Crime of the Public Ministry and other institutions specialized in the field.

Nicaragua’s Cybercrime law was passed in 2008. Article 30 foresees to jail anyone who spreads “false or distorted” information that produces “alarm or fear” with two to four years in prison, and up to three years in prison for false information that damages a person’s “honor” or reputation

4

<http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/bed236921a6bc847062585f30068db3e?OpenDocument>

and up to five years for false information that “incites hate or violates, jeopardizes economic stability, public order, public health or sovereign security. Moreover, the law would punish “illegally intercepting any type of written communication” with up to three years in jail.

The National Cybersecurity Strategy “guarantees the sovereign, secure, and trustworthy use of the cyber-space” and serves to protect “information and services to the general population”.

Other relevant legislation includes the following:

1. Political Constitution of the Republic: protects the national communication systems and the administration and management of the radio and satellite spectrum.
2. Law No. 983 (Constitutional Justice Law): regulates the appeal of Habeas Data.
3. Law No. 919 (Sovereign Security Law): identifies threats to sovereign security, including external attacks on cybersecurity.
4. Law No. 787 (Law on Protection of Personal Data): protects the automated processing of personal data of Nicaraguan society, in order to guarantee informational self-determination.
5. Law No. 641 (Criminal Code): typifies some behaviors of cybercrimes.

Panama has a sound governance framework for developing digital government, although its cybersecurity institutions are still in development stages. The Panamanian government is committed to the digital transformation of the public sector and has invested heavily in e-government. More accessibility also brings more significant security challenges that create opportunities for companies that offer cybersecurity solutions that prevent and deter cybercrimes. With an increased focus on the disruptive and expensive consequences of cyber threats, both private and public need to increase their IT security investment.

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

The Computer Security and Incident Response Team of Panama (CSIRT) operates under the Government Innovation Authority (AIG). In addition to preventing, treating, identifying, and solving cybersecurity incidents, CSIRT Panamá also has the task of increasing the country’s general knowledge about cybersecurity. CSIRT Panamá is a member of CSIRT Americas.

Additionally, the government aims to move beyond awareness and actively combating cyber threats and online services disruption. In March 2019, Panama’s national assembly passed the Personal Data Protection Law, effective as of 2021. This law regulates the principles, rights, obligations, and procedures regarding personal data protection and compensate individuals for the improper use of their data.

Regarding legislation, Panama’s criminal code has some provisions that deal with cybercrime. In addition, Bill No. 558 of 2017 seeks to modify the criminal code to “comply with international cybersecurity standards,” including the Budapest Convention on Cybercrime, approved by Panama in 2013.

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

2. Market assessment

2.1.1. Market overview

The Latin American cybersecurity market was valued at USD 5.73 billion in 2021, and it is expected to register a CAGR of 11.8% during the forecast period (2022-2027).⁵ While there are no specific data for Central America, the adoption of cybersecurity solutions is expected to grow with the increasing penetration of the Internet in the region. Also, the expanding wireless network for mobile devices has increased data vulnerability, making cybersecurity an integral part of every single organization across Central America. The rising incidents of cyberattacks and regulations requiring reporting are driving the growth of the cybersecurity market.

The Central American region is a key strategic target for logistics, transportation, telecommunications and commerce. As each country begins to adapt to a new, unprecedented, post-COVID 19 world, cybersecurity becomes increasingly imperative to secure digital infrastructures.

The region is accelerating the development over cybersecurity matters, and while some countries have achieved an intermediate level of preparedness for cybersecurity, yet their capabilities are still limited due to the lack of regional advancements. The majority of the countries count with no coordinated capabilities to fully respond to cyber-threats, meaning that their vulnerability to cyberattacks in any sector is high.

Nearly 2.1 million cyber-attacks were detected in Central American companies in 2021, of which 206,000 were in El Salvador, according to ESET's latest security report.

The company, which specializes in proactive threat detection, detailed that Guatemala ranked as the country with the most detections during 2021, with a total of 865,000 cyberattacks; followed by Honduras with 439,000. In third place was Nicaragua with 263,000 detections. Most of these detections were of the ransomware type (malicious software used for extortion).

Costa Rican and Panamanian companies reported the fewest detections, with 168,000 and 141,000, respectively. In relation to 2020, Guatemala was the country with the highest increase in cyber-attacks, with 0.8% more. El Salvador had no variation.

The Global Cybersecurity Exposure Index 2020 From 0 to 1, the Cybersecurity Exposure Index (CEI) calculates the level of exposure to cybercrime for 108 countries. The higher the score, the higher the exposure. In Latin America, El Salvador is the most exposed country, followed by Honduras, Nicaragua, and Panama.

Table. Central American countries in the Global Cybersecurity Exposure Index 2020⁶

Source: PasswordManagers.co

Country	Global ranking	Score
Costa Rica	37	0.438
Panama	50	0.569
Nicaragua	56	0.600
Honduras	57	0.603
El Salvador	59	0.617

⁵ Latin America Cyber Security Market - Growth, Trends, Covid-19 Impact, and Forecasts (2021 - 2026), Mordor Intelligence

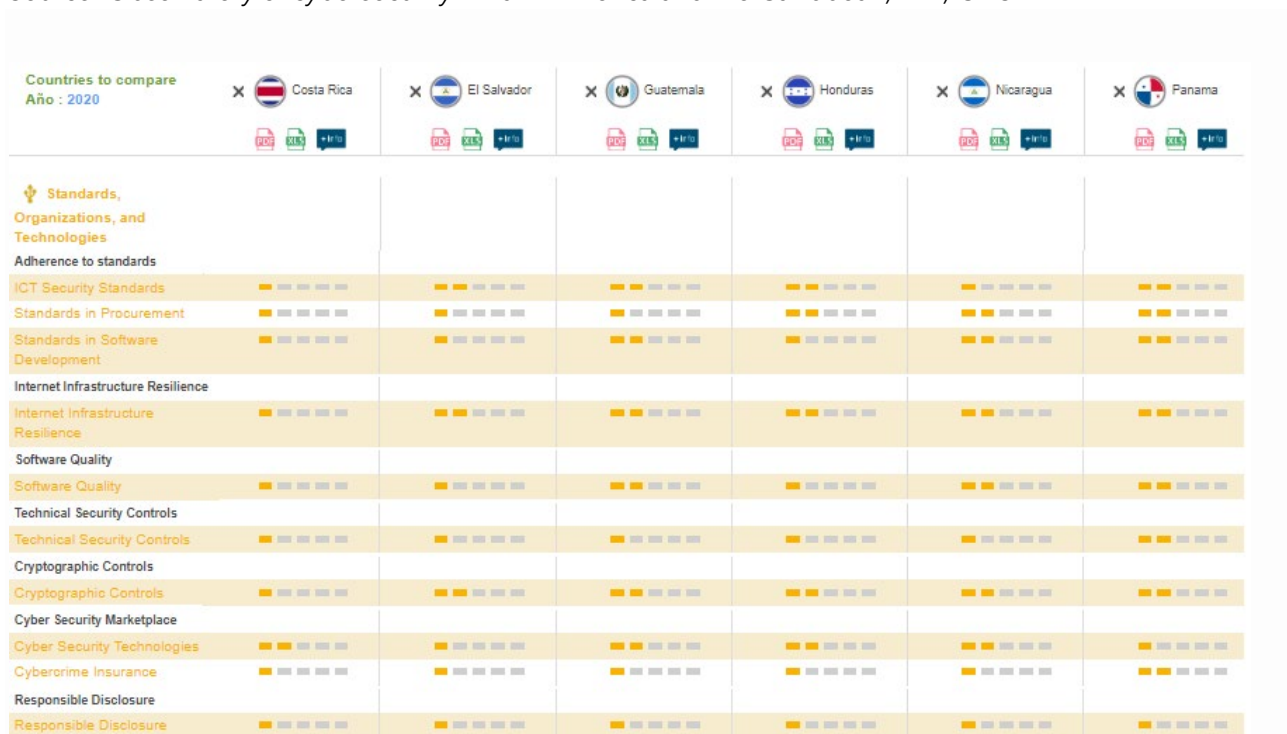
⁶ Guatemala is not assessed in this index.

Regarding national cybersecurity strategies and cybercrime laws, it is of the essence that countries share similarities and a certain harmony between them in order to guarantee a successful functionality. In the region, only Costa Rica, Guatemala and Panama are parties to the Budapest Convention on Cybercrime.

Central American countries have achieved important milestones into developing a strong foundation for national cybersecurity. Although political and strategic instruments already exist and have been recently implemented in countries like Costa Rica, Guatemala and Panama, while others like El Salvador are taking initial steps. However, there is still a significant gap between them and the operational field.

Image. Cybersecurity capacity in selected areas

Source: Observatory of cybersecurity in Latin America and the Caribbean, IDB, OAS



2.1.2. Trends and opportunities

Cybersecurity trends, as the sector itself, are global and no specific to particular markets. Rather, cybersecurity opportunities rely on the connectivity of the economy, society and governments, as well as the maturity of their corresponding cybersecurity regulatory frameworks and cybersecurity infrastructure and systems.

Nonetheless, some industries face a higher risk of cyberattacks than others. This includes industries that typically have high-value organizations or hold a large amount of personal data, such as financial and healthcare. As a result, those countries with a larger share of Multinational Enterprises (MNEs) -i.e. Costa Rica and Panama in the region- offer more opportunities for the development of a dynamic cybersecurity market. From this same perspective, attention has to be given to the development of a consistent framework that facilitates the operationalization of the cybersecurity strategies that have been developed (see chapter on “Policy and Regulatory Assessment”).

From a complementary perspective, Central American countries - in particular Costa Rica, but also, to a more limited extent, other countries- are gradually developing ecosystems favorable to the entry of international cybersecurity suppliers. Indeed, the internationalization process of SMEs

in the sector relies to a large extent on cooperation and business alliances, which require an environment that provides qualified human resources and a critical mass of dynamic start-ups.


















The National Cyber Security Index⁷, developed by e-Governance Academy, measures 151 countries' level of cyber security and identifies the main fields of priority that need to be tackled in order to improve status of cyber security. The index also provides an overview of countries' preparedness to prevent, and fight cyberattacks and crimes.

The "Difference" shows the relationship between the NCSI score and Digital Development Level (DDL) in each country. A positive result shows that the country's cyber security development is in accordance with, or ahead of, its digital development. A negative result shows, that the country's digital society is more advanced than the national cybersecurity area, which increases the risk for and vulnerability to cyberattacks.

The following table shows the Central American countries assessed through the National Cybersecurity Index.⁸

Image. Central American countries in the National Cyber Security Index

Source: e-Governance Academy

Rank	Country	National Cyber Security Index	Digital development	Difference
60.	 Costa Rica	53.25 	59.11 	-5.86
67.	 Panama	48.05 	48.43 	-0.38
101.	 Nicaragua	29.87 	32.70 	-2.83
109.	 El Salvador	24.68 	39.17 	-14.49
108.	 Guatemala	24.68 	35.43 	-10.75
144.	 Honduras	10.39 	35.09 	-24.70

There seems to be limited knowledge on cybersecurity issues on the part of the private sector in the region, although after recent cyber-attacks more companies have focused on providing cybersecurity solutions and services begun to proliferate.

- Costa Ricans have many opportunities to continue studying cybersecurity, and some universities offer shorter training and certificate programs. Several capacity-building events have also been carried out in collaboration with international institutions, such as the training provided by the National Cryptologic Center of Spain for public servants and professional training in collaboration with the OAS and Citi Foundation.
- The private sector in El Salvador participates in the provision of cybersecurity services, ranging from analysis to training. With respect to cybersecurity education, there are some study opportunities in some universities, and some private companies offer training

⁷ <https://ncsi.ega.ee/>

⁸ The Index ranks 151 countries based on its National Cyber Security Index (NCSI) score. The "Difference" shows the relationship between the NCSI score and Digital Development Level (DDL) in each country. A positive result shows that the country's cyber security development is in accordance with, or ahead of, its digital development. A negative result shows, that the country's digital society is more advanced than the national cybersecurity area.

courses in cybersecurity. Companies have also learned that there is a gap in this field in higher-education institutions.

- Guatemala has several cybersecurity service providers as well as a CERT for the private sector. In addition, some companies have been looking to raise awareness about cybersecurity. Equally, the Guatemala Chapter of the Internet Society has a working group that, among other things, aims to raise awareness about cybersecurity and offer workshops on how to manage incidents. While there are not many opportunities to continue tertiary education in cybersecurity, some further education options are available. In addition, the national cybersecurity strategy has an educational axis with the purpose of increasing the offer of education and training in cybersecurity in Guatemala to meet the technical and professional demand in all sectors. There have also been several training events provided by the government, in collaboration with other entities, such as the workshop on cyberthreats, or training for the first CSIRT in collaboration with the OAS.
- In Honduras there are several private entities providing incident response services. Although there is much to be done in terms of cybersecurity service providers, the main private-sector firms have begun to prioritize cybersecurity and take action in this regard.
- There are private-sector providers in Panama offering a variety of cybersecurity services, from database security to a range of training courses. In addition, there is a great opportunity for Panamanian citizens to continue their education in cybersecurity and information technologies, including masters' programs. To encourage the study of cybersecurity, the National Authority for Governmental Innovation, in collaboration with Citi and the OAS, has offered scholarships in the past for cybersecurity training in order to reduce the shortage of cybersecurity professionals in the region. In addition, CSIRT Panamá offers ongoing training in cybersecurity for professionals in the technology departments of government institutions.

3. Entry barriers

From a general perspective, it is evident that physical distance, limited exposure and awareness, cultural differences and language may act as barriers for many new EU entrants to the Central American markets. Also, economies of scale may be difficult to achieve in several sectors due to limited market size, as well as logistics costs, and as a result these may also act as trade disincentives.

High-tech services face often lower entry barriers, as many of the impediments previously mentioned do not impact exports-or do so to a limited extent. In other cases, some entry barriers may be overcome by using one country as a platform, while considering the entire region as the target market. Although it must be acknowledged that integration at the political and regulatory levels is somehow limited, there is a growing de facto market integration driven by the private sector and the development of commercial networks at the regional level.

As a cross border, IT services sector, there are very few -if any- significant entry barriers affecting cybersecurity suppliers. One relevant challenge that is worth considering, is often related to the withholding tax that is usually paid in the country where the service is provided, i.e. where the client resides.

The Central American client will usually withhold a percentage of the total invoice, around 15% or higher (up to 35%), in many cases unknowingly to the EU exporter until the payment is received.





Besides a general recommendation of gathering accurate information on withholding (and other) taxes before quoting for required services, it is also advisable to identify which EU countries may have signed double-taxation avoidance agreements with Central American countries, in order to limit or avoid the impact of this tax.

Another barrier that new entrants may face relates to the limited number of qualified human resources and dynamic start-ups in the cybersecurity sector, which are necessary to facilitate technological cooperation and alliances in the sector. Although some countries -notably Costa Rica- are developing environments favorable to the development of cybersecurity, there are some constraints at the regional level.

4. SWOT Analysis

The SWOT analysis presented below uses the following definitions:

- Strengths: positive, favorable features of the current development of the sector, and that make it attractive to EU businesses (e.g., favorable regulations or incentives, etc.)
- Weaknesses: constrains or negative features of the current development of the sector, that as result make it less attractive to EU businesses (e.g., small market size, costs of logistics of exports from the EU, etc.)
- Opportunities: external factors to the sector itself, or currently absent in the corresponding market, that may increase the attractiveness of the sector for EU businesses (e.g., growth drivers)
- Threats: external or potential, negative factors that may reduce the attractiveness of the sector for EU businesses or hinder their competitiveness (e.g., increasing competition).

			
STRENGTHS	WEAKNESSES	OPPORTUNITIES	THREATS
<p>Policy and regulatory supportive framework.</p> <p>Global sector.</p>	<p>Limited institutional capacities.</p> <p>Limited supply of qualified human resources.</p>	<p>Increasing cybersecurity risks, in particular in Panama and Costa Rica.</p> <p>Insufficient supply of specialized services at the regional level.</p> <p>Central American region (in particular Costa Rica) as a platform to reach larger markets (time zone, language, etc.).</p> <p>Developing favorable ecosystems for cybersecurity actors and start-ups Business cooperation model very attractive SMEs market entry.</p>	<p>Limited number of double taxation avoidance agreements with EU countries to avoid impact of withholding tax may hinder potential for new entrants.</p> <p>Ongoing cooperation of Costa Rica with Israel and US.</p>



This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the AESA - EY consortium, and do not necessarily reflect the views of the European Union.