



Organization of  
American States  

---

More rights for more people

# Cybersecurity

## Are We Ready in Latin America and the Caribbean?

---

**2016 Cybersecurity Report**

[www.cybersecurityobservatory.com](http://www.cybersecurityobservatory.com)

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

## **Gonzalo Garcia-Belenguer**

---

Cybersecurity Program Officer  
**Organization of American States**

Ggarcia-belenguer@oas.org  
@OASGonzalo

# What the OAS does on Cybersecurity issues?

- Development of National Cybersecurity Strategies
- Trainings, Workshops and Technical Missions
- Cybersecurity Exercises
- Development of national CSIRTs and a regional CSIRT Hemispheric Network
- Awareness Raising, Research and Expertise

# Why this report?

- Need for more tangible and reliable data
- Need for a baseline data to better monitor regional developments in cybersecurity
- OAS experience with previous reports
  - 2013: Latin American and Caribbean Trends and Government Responses
  - 2014: Latin American + Caribbean Cybersecurity Trends
  - 2015: Cybersecurity and Critical Infrastructure in the Americas
- Inter-American Development Bank (IDB) interest on cybersecurity issues
- Increasing interest from member states

# Overview-2016 Cybersecurity Report



## Expert Contributions

- Cyber Confidence Building and Diplomacy in Latin America and the Caribbean
- Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean
- Incident Response Capacity Building in the Americas
- The State of Cybercrime Legislation in Latin America and the Caribbean
- Digital Economy and Cybersecurity in Latin America and the Caribbean
- Sustainable and Secure Development: A Framework for Resilient Connected Societies



## Country Profiles

- 32 countries from Latin America and the Caribbean region

# “Backstage”

- OAS – IDB Agreement.
- Regional Activity in October 2014 for launching this initiative.
- Initial support from Microsoft to identify key areas of study.
- Partnership with the University of Oxford to develop an “Application Tool” based on the Cybersecurity Capability Maturity Model (CMM).
- 3-4 intense weeks of work, making substantial adaptations to CMM for the LAC region.

# “Backstage”

- In-country application of the CMM and distribution of digital survey.
- Desktop Research and consolidation of other sources of available data.
- Validation process of approximately 60 days of the application tool.
- Lots of trial & error, amendments and back and forth!

# Timeline

| May 2014                              | September 2014              | October 2014      | October-<br>November<br>2014    | December 2014                | February 2015                | March-April<br>2015                     | July 2015                    | August 2015                              | September 2015             | March 2016   |
|---------------------------------------|-----------------------------|-------------------|---------------------------------|------------------------------|------------------------------|---|------------------------------|--|----------------------------|--------------|
| OAS-IDB<br>Preliminary<br>discussions | Formal OAS-IDB<br>Agreement | Regional Activity | Preparation<br>Application Tool | Validation Process<br>Starts | Validation Process<br>Finish | Request for<br>Experts<br>Contributions | Collection of Data<br>Ends   | Receive Final<br>Expert<br>Contributions | Validation Process<br>Ends | Release Date |
|                                       |                             |                   |                                 | Desk Research                | Graphics Concepts<br>Starts  |   | Validation Process<br>Starts |  | Graphic Design             |              |
|                                       |                             |                   |                                 |                              | Collection of Data<br>Starts |   |                              |  | Editorial Process          |              |



# CMM - 5 Dimensions



Policy and Strategy



Legal Frameworks



Culture and Society



Technologies



Education



**Estrategia nacional de seguridad ciberné oficial o documentada**

Desarrollo de la estrategia ▶

Organización ▼

- INICIAL** ▼ No existe una entidad global para la coordinación de la seguridad cibernética; si hay los presupuestos, existen en oficinas públicas no relacionadas.  
■ □ □ □ □ □
- FORMATIVO** ▼ Se ha diseñado y difundido un programa de seguridad cibernética coordinada; todavía pueden distribuirse presupuestos; aún es limitada la cooperación interdepartamental.  
■ ■ □ □ □ □
- ESTABLECIDO** ▼ Se ha designado un solo programa cibernético dentro de cada entidad gubernamental; existe un dueño departamental o ente coordinador con un presupuesto consolidado; el programa se define, con metas, hitos e indicadores para medir el progreso; se han acordado las funciones y responsabilidades claras para las funciones de seguridad cibernética dentro del gobierno.  
■ ■ ■ □ □ □
- ESTRATÉGICO** ▼ Existen pruebas de la aplicación iterativa de las métricas y el perfeccionamiento resultante de las operaciones y la estrategia a través de los gobiernos involucrados en la seguridad cibernética, incluida la evaluación y gestión del riesgo.  
■ ■ ■ ■ □ □
- DINÁMICO** ▼ Un organismo nacional es designado para difundir e impulsar la aplicación de la estrategia de seguridad cibernética; existe una postura de seguridad cibernética nacional singular con la capacidad de reasignar tareas y presupuestos de forma dinámica de acuerdo a los cambios en la evaluación de riesgos del entorno de seguridad cibernética; se solidifica la cooperación internacional a nivel organizacional.  
■ ■ ■ ■ ■ □

Contenido ▶

Política y estrategia ▼

**Estrategia nacional de seguridad ciberné oficial o documentada**

Desarrollo de la estrategia □ □ □ □ □ □

Organización □ □ □ □ □ □

Contenido □ □ □ □ □ □

**Defensa cibernética**

Estrategia □ □ □ □ □ □

Organización □ □ □ □ □ □

Coordinación □ □ □ □ □ □

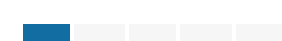
**Mentalidad de seguridad cibernética**

En el gobierno ▶

En el sector privado ▶

En la sociedad ▼

**INICIAL**



La sociedad desconoce las amenazas cibernéticas y no puede tomar medidas concretas de seguridad cibernética o la sociedad es consciente de las amenazas cibernéticas, pero no toma medidas proactivas para mejorar su seguridad cibernética.

**FORMATIVO**



Se adopta una mentalidad de seguridad cibernética, pero de manera inconsistente, en toda la sociedad; los programas y materiales han sido puestos a disposición para entrenar y mejorar las prácticas de seguridad cibernética.

**ESTABLECIDO**



Se ha desarrollado una conciencia social del uso seguro de los sistemas en línea; una proporción creciente de usuarios tienen las habilidades para manejar su privacidad en línea y protegerse de la intromisión, interferencia o acceso no deseado a la información por otros.

**ESTRATÉGICO**



Un número creciente de usuarios están empleando seguras prácticas en línea como una costumbre, la conciencia de la seguridad está arraigada; la mayoría de los usuarios tienen la información, confianza y herramientas prácticas para protegerse en línea, mientras que se proporcionan el apoyo y los recursos a los miembros vulnerables de la sociedad, incluida la protección de menores.

**DINÁMICO**



Los usuarios demuestran una mentalidad de seguridad cibernética y emplean habitualmente las prácticas más seguras en su uso cotidiano de las redes en línea; el conjunto de habilidades en seguridad cibernética de la población de un país está avanzado de manera que los usuarios pueden abordar de manera efectiva las amenazas que enfrenta la sociedad.

Cultura y sociedad ▼

**Mentalidad de seguridad cibernética**

En el gobierno



En el sector privado



En la sociedad



**Conciencia de seguridad cibernética**

Sensibilización



**Confianza en el uso de Internet**

En los servicios en línea



En el gobierno electrónico



En el comercio electrónico



**Privacidad en línea**

Normas de privacidad



Privacidad del empleado





### Disponibilidad nacional de la educación y formación cibernéticas

Educación ▼

INICIAL



▼ No hay, o es mínima, oferta educativa en seguridad de la información pero no hay un proveedor reconocido de educación en seguridad cibernética; no existe una acreditación en educación de seguridad cibernética.

FORMATIVO



▼ Existe mercado para la educación y la formación en seguridad de la información con evidencia de asimilación; las iniciativas de los profesionales están dirigidas a incrementar el atractivo de las carreras en seguridad cibernética y la pertinencia de roles de liderazgo más amplias.

ESTABLECIDO



▼ Existe alguna educación en seguridad cibernética a nivel nacional e institucional, que va desde el nivel elemental hasta postgrado, incluyendo la formación profesional en forma modular.

ESTRATÉGICO



▼ La oferta educativa se pondera y se centra basada en una comprensión de los riesgos actuales y las necesidades de habilidades; se desarrollan métricas para asegurar que las inversiones educativas respondan a las necesidades del entorno de la seguridad cibernética; el acceso a los educadores está disponible en la seguridad cibernética específicamente para especialistas en seguridad cibernética.

DINÁMICO



▼ Existe integración y sinergia entre elementos educativos; los requisitos de seguridad cibernética que prevalecen son tomados en consideración en el re-desarrollo de todo programa general de estudios; la investigación y el desarrollo son una consideración principal en la educación la seguridad cibernética; el contenido en los programas de educación se alinea con desafíos operacionales y seguridad cibernética práctica.

Formación ▶

Educación ▼

Disponibilidad nacional de la educación y formación cibernéticas

Educación

Formación

Desarrollo nacional de la educación de seguridad cibernética

Desarrollo nacional de la educación

Formación e iniciativas educativas públicas y privadas

Capacitación de empleados

Gobernanza corporativa, conocimiento y normas

En las empresas estatales y privadas



### Marcos jurídicos de seguridad cibernética

Para la seguridad de las TIC ▶

Privacidad, protección de datos y otros derechos humanos ▶

Derecho sustantivo de delincuencia cibernética ▼

- INICIAL** ▼

El derecho penal sustantivo específico para la delincuencia cibernética no existe, o existe el derecho penal general y se aplica ad-hoc a la delincuencia cibernética.
- FORMATIVO** ▼

Existe una legislación parcial en el derecho penal sustantivo que aplica los marcos legales y regulatorios a algunos aspectos de los delitos cibernéticos; está siendo discutido el derecho penal sustantivo para la delincuencia cibernética entre los legisladores, pero ha comenzado el desarrollo de la ley.
- ESTABLECIDO** ▼

La legislación vigente tipifica una serie de delitos relacionados con pruebas electrónicas que pueden ser objeto de una legislación específica o abordados en el código penal.
- ESTRATÉGICO** ▼

El país se adhiere a las mejores prácticas y normativas regionales e internacionales pertinentes sobre derecho de delito cibernético y asigna los recursos de acuerdo a las prioridades nacionales.
- DINÁMICO** ▼

El país continuamente busca incluir el desarrollo de las mejores prácticas internacionales sobre delito cibernético en la legislación nacional y es un colaborador activo en el discurso global sobre la mejora de los instrumentos de la lucha contra delitos cibernéticos internacionales; existen medidas para superar en el país las líneas de base mínimas de seguridad internacional.

Derecho procesal de delincuencia cibernética ▶

### Marcos legales ▼

#### Marcos jurídicos de seguridad cibernética

Para la seguridad de las TIC

Privacidad, protección de datos y otros derechos humanos

Derecho sustantivo de delincuencia cibernética

Derecho procesal de delincuencia cibernética

#### Investigación jurídica

Cumplimiento de la ley

Fiscalía

Tribunales

#### Divulgación responsable de la información

Divulgación responsable de la información

## Organizaciones de coordinación de seguridad cibernética

Centro de mando y control ▶

Capacidad de respuesta a incidentes ▼

INICIAL



La capacidad de respuesta de incidentes no es coordinada y se lleva a cabo de manera ad-hoc.



FORMATIVO



Existe un equipo o personal de respuesta a incidentes en el país, con roles y responsabilidades identificadas; la actividad se concentra en la detección y respuesta a incidentes cibernéticos específicos de la organización.



ESTABLECIDO



Se establece una capacidad de respuesta a incidentes nacional e involucra a los interesados clave, en especial a través de asociaciones público-privadas; la sostenibilidad financiera de la capacidad de respuesta a incidentes es considerada y planificada a través de la participación de las principales partes interesadas; se desarrolla e implementa un plan de gestión de vulnerabilidades; los incidentes se clasifican en consonancia con los planes de respuesta; los planes de respuesta y recuperación están operando y se gestionan; existe una evaluación nacional de la base de datos de vulnerabilidad del impacto en las funciones críticas; la información se comparte en consonancia con los planes de respuesta; los principales interesados son conscientes de la capacidad de respuesta a incidentes nacional y sus responsabilidades.



ESTRATÉGICO



La capacidad de respuesta a incidentes nacional apoya la creación de capacidades específicas del sector; se comparten los recursos y la información a través de una mayor coordinación y colaboración con los equipos locales, regionales e internacionales de respuesta a incidentes; la evaluación de la eficacia del CERT informa la dotación de recursos del CERT; los informes de incidentes ocurren en todos los sectores y planes de respuesta y se ponen a prueba los correspondientes planes de recuperación; se ofrecen servicios forenses; el intercambio de información se promueve de manera voluntaria entre las partes interesadas externas.



DINÁMICO



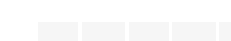
La capacidad de respuesta a incidentes nacional es completamente sostenible financieramente y políticamente apoyada, independientemente de la transición política; existe una cooperación internacional orientada a la formación de mejores prácticas entre los grupos de expertos.



Tecnologías ▼

**Adhesión a las normas**

Aplicación de las normas y prácticas mínimas aceptables



Adquisiciones



Desarrollo de software



**Organizaciones de coordinación de seguridad cibernética**

Centro de mando y control



Capacidad de respuesta a incidentes



**Respuesta a incidentes**

Identificación y designación



Organización



Coordinación



**Resiliencia de la infraestructura nacional**

Infraestructura tecnológica



Resiliencia nacional



**Protección de la infraestructura crítica nacional (ICN)**

Identificación



Organización



Planeación de respuesta



Coordinación



Gestión de riesgos



**Gestión de crisis**

Planeación



Evaluación

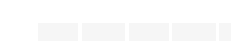


**Redundancia digital**

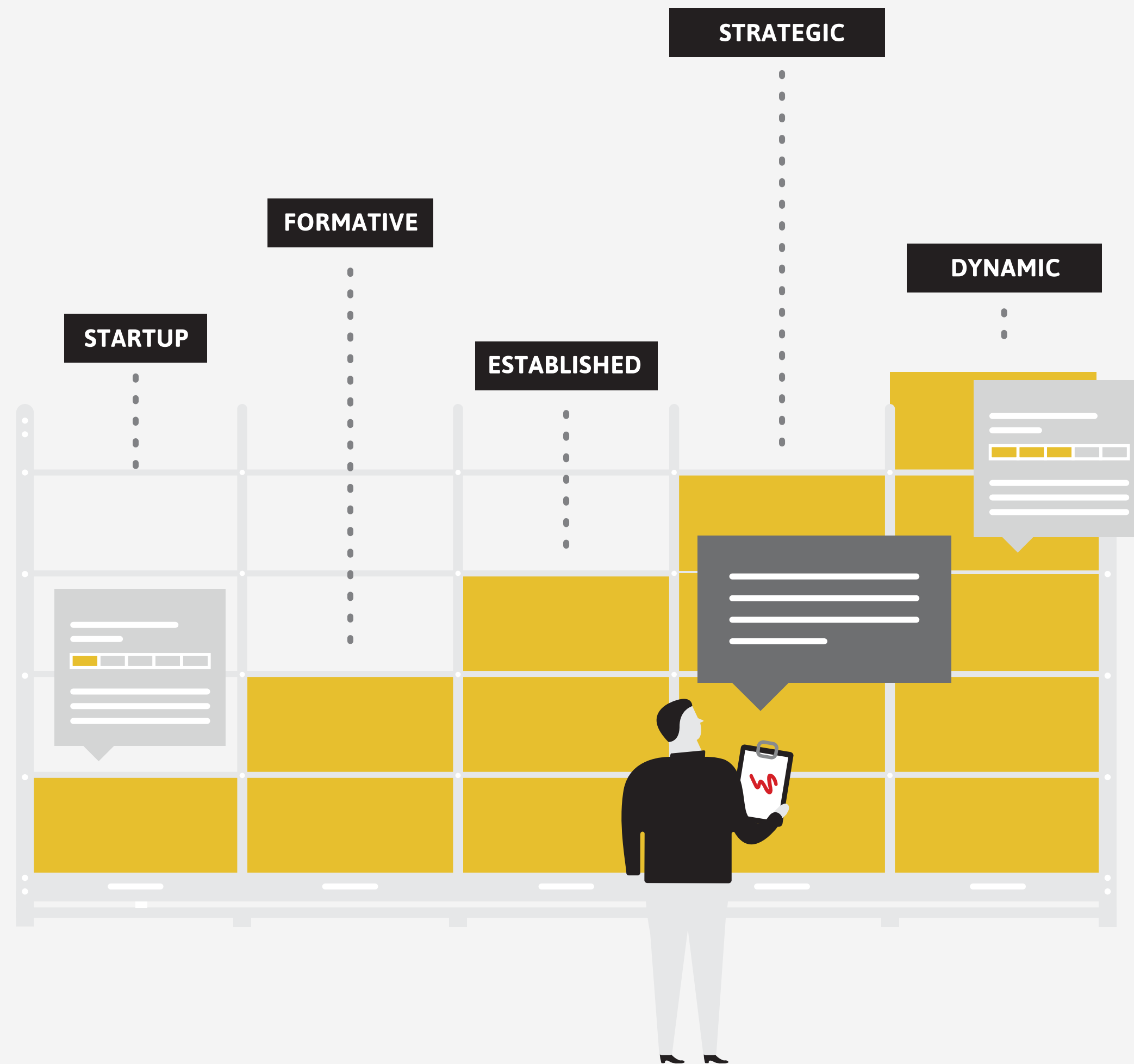
Planeación



Organización



# CMM - 5 Levels of Maturity



# Observatory

This site shows the levels of maturity on Cybersecurity in Latin America and The Caribbean. Please select the countries you want to compare and **scroll down** to see the results.

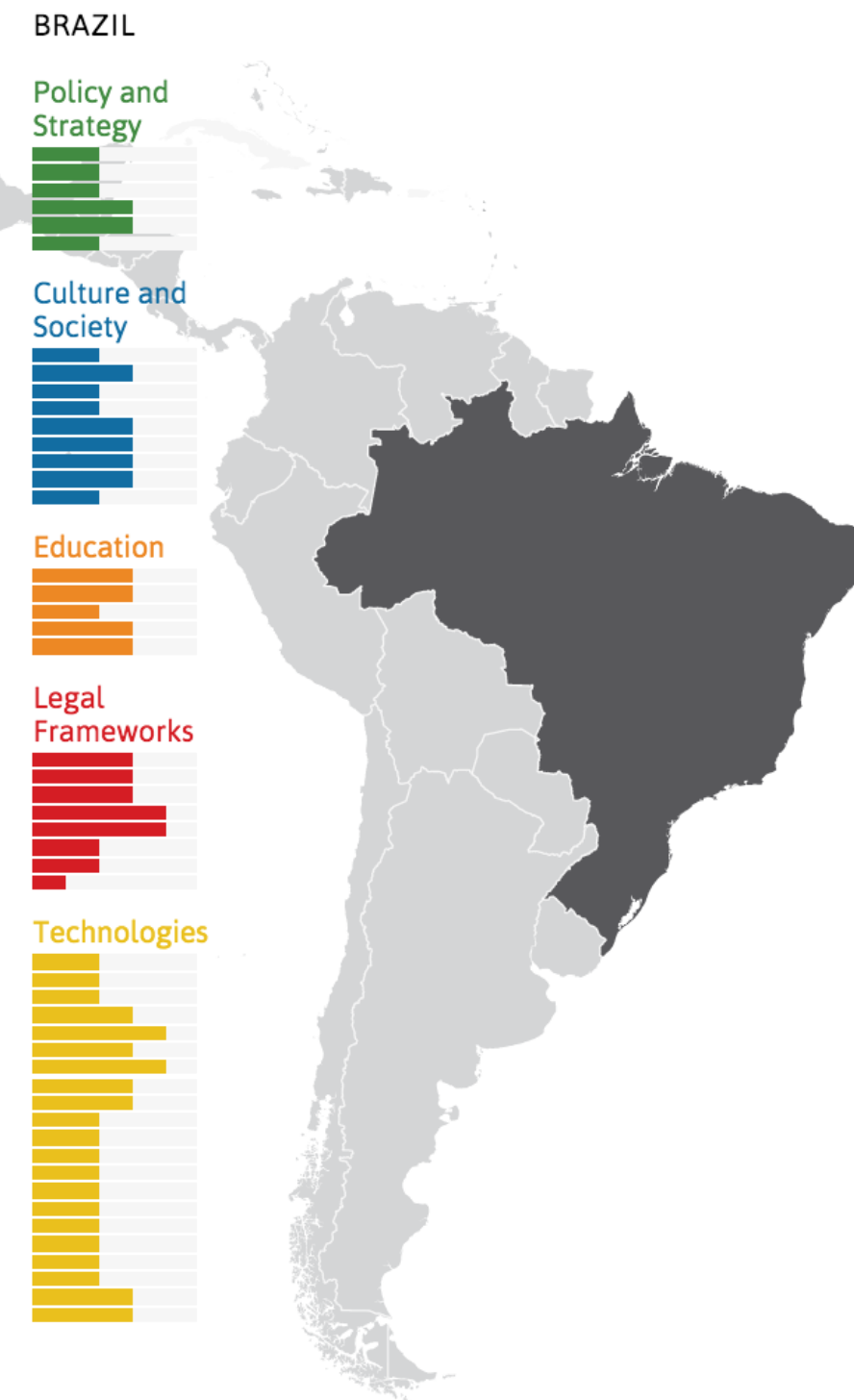
Compare another country ▾

Deselect all      Ok

- BAHAMAS
- BARBADOS
- BELIZE
- BOLIVIA
- ✓ BRAZIL

promote economic growth and social progress. In light of its increased adoption of ICT, Brazil has become a prime target of cyberattacks and

[Read more >>](#)



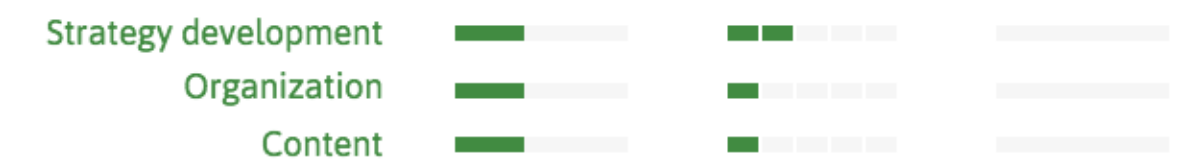
Download XLS      share

CHILE      COSTA RICA      Select a country to compare

▾

## Policy and Strategy ▾

### Documented or Official National Cybersecurity Strategy

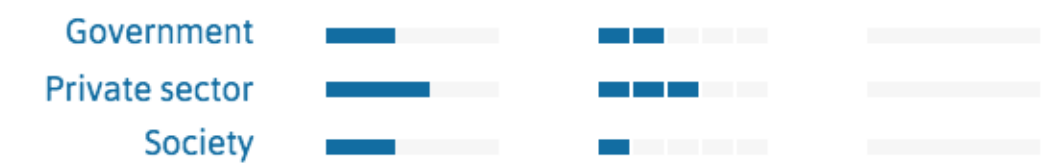


### Cyber Defense Consideration

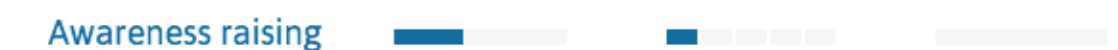


## Culture and Society ▾

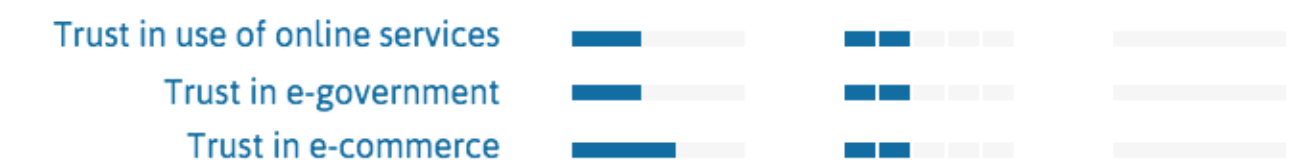
### Cybersecurity Mind-set



### Cybersecurity Awareness



### Confidence and Trust on the Internet



### Online Privacy





# How the report looks?

OBSERVATORY  
**CYBERSECURITY**  
IN LATIN AMERICA AND THE CARIBBEAN

## Cybersecurity

Are We Ready in Latin America and the Caribbean?

2016 Cybersecurity Report

www.cybersecurityobservatory.com



Organization of American States  
More rights for more people



Download Report

**Mariela Maciel**  
Researcher and coordinator of the Center for Technology and Society of the Getulio Vargas Foundation School of Law in Rio de Janeiro. She serves as a coordinator of the Generic Name Supporting Organization of the Internet Corporation for Assigned Names and Numbers (ICANN) representing the Non-commercial Stakeholder Group. She is a member of the Advisory Board on Internet Security, created under the Brazilian Internet Steering Committee. Mariela is a PhD candidate in International Relations at the Pontifical Catholic University (PUC-Rio de Janeiro).

**Nathalia Fedrich**  
Researcher at the Center for Technology and Society of the Getulio Vargas Foundation School of Law in Rio de Janeiro. She has worked for international organizations, the Brazilian Federal Government, as well as law firms and think tanks on communications law and policy matters. Fedrich has earned attorney and holds a Master's degree in Law and another in Public Policy, both from the American University.

**Luca Belli**  
Researcher at the Center for Technology and Society of the Getulio Vargas Foundation School of Law in Rio de Janeiro. He holds a PhD in Public Law from the Universidad Pontificia Avila (PVA) and is a founder and coordinator of the Dynamic Coalition on Network Neutrality, as well as of the Dynamic Coalition on Platform Responsibility, multi-stakeholder components of the United Nations Internet Governance Forum.

**Nicolás Castellón**  
Visiting researcher at the Center for Technology and Society of the Foundation School of Law in Rio de Janeiro. He specializes in cybersecurity governance, focusing on critical infrastructures and humanitarian uses for Big Data. He holds a Master's degree in Crisis and Security Management from London University's Faculty of Governance and Global Affairs.

**FGV DIREITO RIO**  
UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

**FQV Fundação Getulio Vargas**  
www.fgv.br

12

### Incident Response Capacity Building in the Americas

**FIRST** | Team of Incident Response and Security Teams  
Maarten Van Horebeek, Cristine Hoopes and Peter Altor

**SACERT** | St. Vincent  
**CERT-CA** | Costa Rica  
**hCERT** | Colombia  
**hCERT** | Ecuador  
**PGCERT** | Peru  
**CERT-BO** | Bolivia  
**CERT-CL** | Chile

**CERT-MX** | Mexico  
**CERT-GT** | Guatemala  
**IT-CERT** | Trinidad and Tobago  
**hCERT** | Venezuela  
**CERT-GY** | Guyana  
**CERT-BR** | Brazil  
**CERT-PY** | Paraguay  
**CERT-UY** | Uruguay  
**IC-CERT** | Argentina

**IC-CERT**  
A Computer Security Incident Response Team (CSIRT) is defined as a team or an entity within an agency that provides services and support to a particular group (target community) in order to prevent, manage and respond to information security incidents. These teams are usually comprised of multidisciplinary specialists who act according to predefined procedures and policies in order to respond quickly and effectively to security incidents and to mitigate the risk of cyberattacks. There are hundreds of CSIRTs in the world that deal in mission and scope. One of the chief ways to classify CSIRTs is to group them by the sector or community they serve. Below are the names of the national CSIRTs within OAS member states.

13

### Argentina

**Policy and Strategy**  
Strategic development  
Control  
Cyber Defense  
Cyber Defense Coordination

**Culture and Society**  
Cybersecurity Mind Set  
Government  
Private Sector  
Security  
Cybersecurity Awareness  
Awareness raising

**Legal Frameworks**  
Confidence and Trust on the Internet  
Trust in e-commerce  
Trust in government  
Trust in companies  
Online Privacy  
Privacy standards  
Employee privacy

**Technologies**  
National Infrastructure Resilience  
Critical National Infrastructure Protection  
National Development of Cybersecurity Education  
National Development of Cybersecurity Training  
Training and Educational Initiatives  
Corporate Governance, Knowledge and Standards  
Private and State Owned Companies' Understanding

Lea by the National Program for Critical Information Infrastructure and Cybersecurity (PCIC) in coordination with various agencies, academic institutions and the private sector, the Government of Argentina has developed a draft National Cybersecurity Strategy that is currently awaiting adoption. Argentina is notable for forming one of the first national CSIRTs in 1996. Since 2011, it has functioned under the ICIC. ICIC-CERT maintains a central registry of cybersecurity events and threats. The Armed Forces run annual Cyber Incident Response Exercises to share best practices and review command and control functions, however, they currently have limited capacity for cyber-resilience.

Previously, CNI was managed more or less informally, however, in June 2013, the Presidency of the Republic of Argentina issued Decree No. 1267/2013, which restructured government control of CNI, establishing a National Office within the Under-secretariat for the Protection of Critical Information and Cybersecurity Infrastructure, under the Head Office of the Cabinet of Ministers-Cabinet Secretariat. This new program will work to develop cybersecurity norms and standards, as well as collaborate with the private sector to improve CNI resilience.

Amid increases in cybercrime, the Government of Argentina constructed a comprehensive legal framework for ICT, including Penal Code Law 26,388 and Law 27,326 on data protection. It is also developing procedural law for handling digital evidence. While mechanisms are in place for disclosure, the private sector is not legally required to report breaches to cybersecurity authorities, awareness of cybersecurity risks among businesses has grown significantly. The Technology Crimes Division of the Argentina Federal Police Force is responsible for investigating cases of cybercrime.

And takes on a number of capacities, including providing information on how to detect and report cyberattacks. Recently, the Government of Argentina also established a Fiscal Point on Cybercrime under the Public Prosecutor's office.

As Argentina's e-government and e-commerce services continue to expand, government agencies have led awareness-raising campaigns to educate the public about cybersecurity. Two notable examples are Internet Seguro (Healthy-on-Secure) - initiated by the ICIC, which focuses on best practices for safe internet use, and With You on the Web under the Ministry of Justice and Human Rights, which teaches children, parents and teachers about the threat of online grooming. The predatory handing of children on the web to lure them into sexual abuse or trafficking. In addition, a number of universities offer degree programs in cybersecurity and digital forensics.

**TOTAL POPULATION IN THE COUNTRY** 42,980,026  
**Internet penetration** 65%  
**Mobile phone subscriptions** 66,356,509  
**People with Internet access** 27,937,016

10

**Policy and Strategy**  
Strategic development  
Control  
Cyber Defense  
Cyber Defense Coordination

**Culture and Society**  
Cybersecurity Mind Set  
Government  
Private Sector  
Security  
Cybersecurity Awareness  
Awareness raising

**Legal Frameworks**  
Confidence and Trust on the Internet  
Trust in e-commerce  
Trust in government  
Trust in companies  
Online Privacy  
Privacy standards  
Employee privacy

**Technologies**  
National Infrastructure Resilience  
Critical National Infrastructure Protection  
National Development of Cybersecurity Education  
National Development of Cybersecurity Training  
Training and Educational Initiatives  
Corporate Governance, Knowledge and Standards  
Private and State Owned Companies' Understanding

11

**Costa Rica**

- Attorney General of the Republic
- Costa Rican Institute of Electricity
- Judicial Investigations Department
- Ministry of the Presidency
- Ministry of Science, Technology and Telecommunications
- Superintendence of Telecommunications
- University of Costa Rica

**El Salvador**

- Ministry of Justice and Public Security

**Grenada**

- Royal Grenada Police Force

**Dominica**

- Dominica Association of Information Technology Professionals
- Dominica State College
- Information and Communications Technology Unit
- Ministry of Information and Telecommunications
- National Bank of Dominica

**Dominican Republic**

- Attorney General of the Republic
- Dominican Telecommunications Institute
- National Police

**Ecuador**

- Telecommunications Regulation and Control Agency
- Armed Forces of Ecuador
- Attorney General of Ecuador
- Ministry of Defense

**Guatemala**

- CSIRT-GT
- Ministry of the Interior
- Public Ministry
- Superintendence of Telecommunications
- Technical Secretariat of the National Security Council

**Guyana**

- CSIRT-GY - Ministry of Home Affairs
- Guyana Energy Agency
- Guyana Defence Force
- Guyana Police Force
- University of Guyana

**Haiti**

- National Telecommunications Council

118

**Honduras**

- CONADES
- National Telecommunications Commission
- Ministry of Foreign Relations and International Cooperation
- National Police of Honduras
- National Property Management System

**Jamaica**

- Jamaica Bank Association
- Jamaica Constabulary Force
- Ministry of National Security
- Ministry of Science, Technology, Energy and Mining
- Public Ministry
- University of the West Indies

**Mexico**

- Attorney General's Office
- Mexican Internet Association, A.C.
- Mexican Penitentiary
- Secretariat of the Interior
- Specialized Committee on Information Security

**Nicaragua**

- National Engineering University

**Panama**

- National Authority for Governmental Innovation
- Panama Canal Authority

**Paraguay**

- Attorney General's Office
- Ministry of Foreign Affairs
- National Secretariat of Information and Communications Technology

**Peru**

- Joint Command of the Armed Forces
- Ministry of Defense
- Ministry of Foreign Relations
- Ministry of the Interior
- National Office of Government and Information
- National Police of Peru
- Public Ministry - Prosecutor's Office

**Saint Kitts and Nevis**

- Financial Services Regulatory Commission
- LINE
- Ministry of Energy, Finance, Trade and Industries
- Ministry of Youth Employment, Sports, Information Communications and Technology, Telecommunications and Post
- Royal Saint Kitts and Nevis Police
- Saint Kitts Electricity Company, Ltd.

119

**Corporate Governance, Knowledge and Standards**

**Private and State Owned Companies' Understanding**

**ESTONIA**

- Boards have minimal or no understanding of cybersecurity and fiduciary duty considerations are not discussed.

**HONGKONG**

- Executive boards have some awareness of cybersecurity issues, but not how they might affect the organization or what direct threats they may be faced with.

**ESTONIA (continued)**

- Executive boards understand how companies are at risk, in general, some of the primary methods of attack, and how their company deals with cyber issues (usually entrusted to the Chief Information Officer's) and incident management is largely reactive.

**FRANCE**

- Executive boards are aware of their strategic assets, have put specific measures in place to protect them, and know the mechanism which protects them; the executive board can allocate specific funding and assign people to prevent cyber risks; corporate contingency plans are in place to address various cyber-based attacks and their aftermath; executive board members are provided with some cybersecurity education; and the board has a clear sense of cyber fiduciary duties.

**FRANCE (continued)**

- Executive boards are able to change cybersecurity strategy quickly and appropriately; new threats are considered at every board meeting, and funding and attention is reallocated to address those threats; the executive board is looked to as a source of knowledge in corporate cybersecurity governance; governance is based on cyber risk and improves governance, specifically in this area.

146

### Legal Frameworks

**Cybersecurity Legal Frameworks**  
Legislative Frameworks for ICT security  
Privacy, data protection and other human rights  
Substantive cybercrime law  
Procedural cybercrime law

**Legal Investigation**  
Law enforcement  
Prosecution services  
Courts

**Responsible Reporting**  
Responsible disclosure

147

“Through the driving force of the IDB and OAS, the region is the **first in the world** to undertake this deep and broad understanding of cybersecurity capacity across an entire region using the CMM.”



**Thank you!**  
**Merci**  
**Gracias**  
**Obrigado**

## **Gonzalo Garcia-Belenguer**

---

Cybersecurity Program Officer  
**Organization of American States**

Ggarcia-belenguer@oas.org  
@OASGonzalo