Cybersecurity

Are We Ready in Latin America and the Caribbean?

2016 Cybersecurity Report

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.

Belisario Contreras

Cybersecurity Program Manager
Organization of American States
BContreras@oas.org

@belisarioc
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?

- Inter-American Development Bank (IDB) support to cybersecurity issues
- 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
- 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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>OAS-IDB Preliminary discussions</td>
<td>Formal OAS-IDB Agreement</td>
<td>Regional Activity</td>
<td>Preparation Application Tool</td>
<td>Validation Process Starts</td>
<td>Validation Process Finish</td>
<td>Request for Experts Contributions</td>
<td>Collection of Data Ends</td>
<td>Receive Final Expert Contributions</td>
<td>Validation Process Ends</td>
<td>Release Date</td>
</tr>
</tbody>
</table>
CMM - 5 Dimensions

- Policy and Strategy
- Legal Frameworks
- Culture and Society
- Technologies
- Education
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.

Comparison options:
- Documented or Official National Cybersecurity Strategy
- Strategy development
- Organization
- Content
- Cyber Defense Consideration
- Strategy
- Organization
- Coordination
- Cybersecurity Mind-set
- Government
- Private sector
- Society
- Cybersecurity Awareness
- Awareness raising
- Confidence and Trust on the Internet
- Trust in use of online services
- Trust in e-government
- Trust in e-commerce
- Online Privacy
- Privacy standards
- Employee privacy

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 >>
How the report looks?
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

---

**MEXICO**

In 2012, the Government of Mexico created the Specialized Information Security Committee, which was tasked with the development of a National...
<table>
<thead>
<tr>
<th>Country</th>
<th>Policy and Strategy</th>
<th>Culture and Society</th>
<th>Education</th>
<th>Legal Frameworks</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uruguay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Incident Response Capacity Building in the Americas

FIRST | Forum of Incident Response and Security Teams
Maarten Van Horenbeeck, Cristine Hoepers and Peter Allor

“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 vary 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 some of the national CSIRTs within OAS member states.”
Challenges in the region

- 18 countries have NOT identified “key elements” of their National Critical Infrastructure
- 24 do not count with mechanism for planning and coordination on Critical Infrastructure Issues
- 27 of 32 countries do not have cyber security strategies
Challenges in the region

In **20 countries** no command and control center exist, and in another 7 this function is performed without formality.

**26 countries** in the region do not have a structured cybersecurity education program.

In **30 of the 32 countries**, there is no national cyber security awareness programs.
“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

Belisario Contreras
Cybersecurity Program Manager
Organization of American States
BContreras@oas.org
@belisarioc