OAS More rights for more people

Cybersecurity

Are We Ready in Latin America and the Caribbean?

2016 Cybersecurity Report

www.cybersecurityobservatory.com

#OEAFIRST

@OEA_Cyber

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!

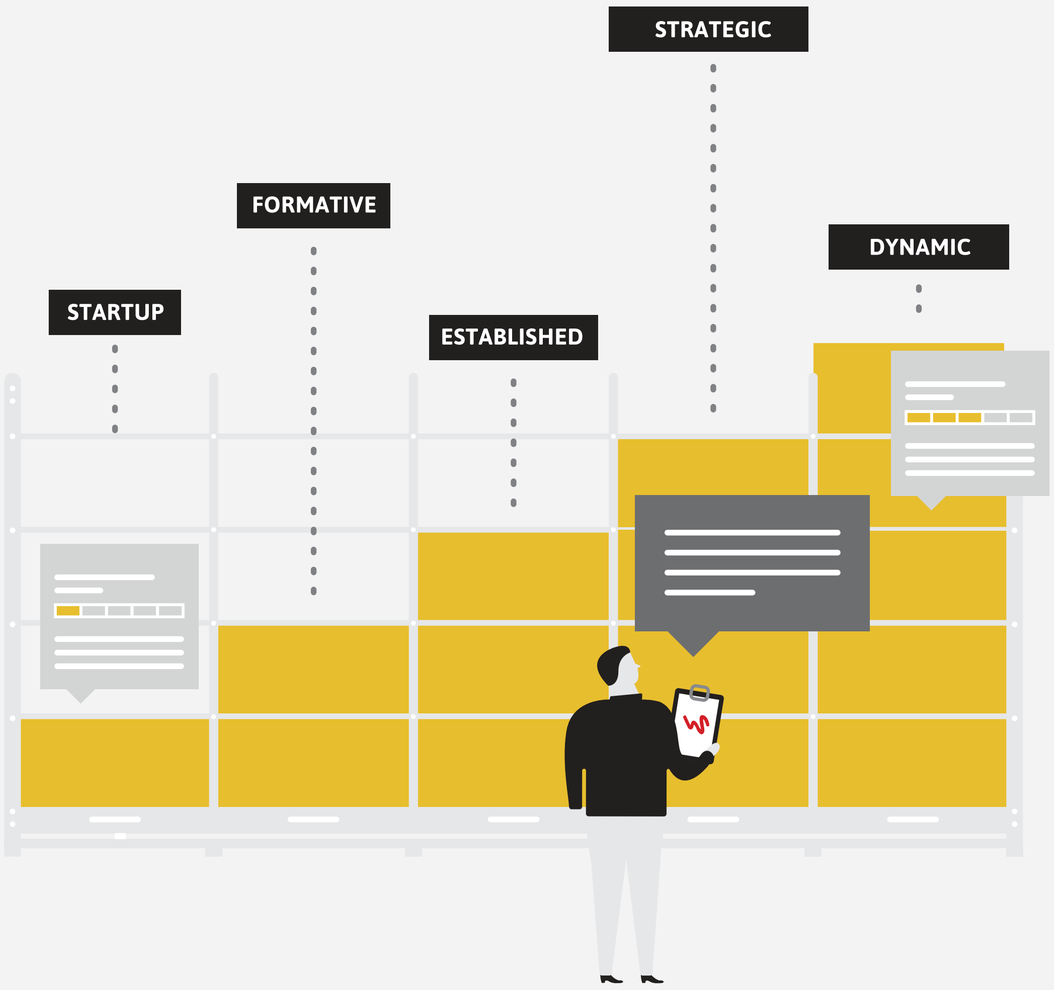
Timeline

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

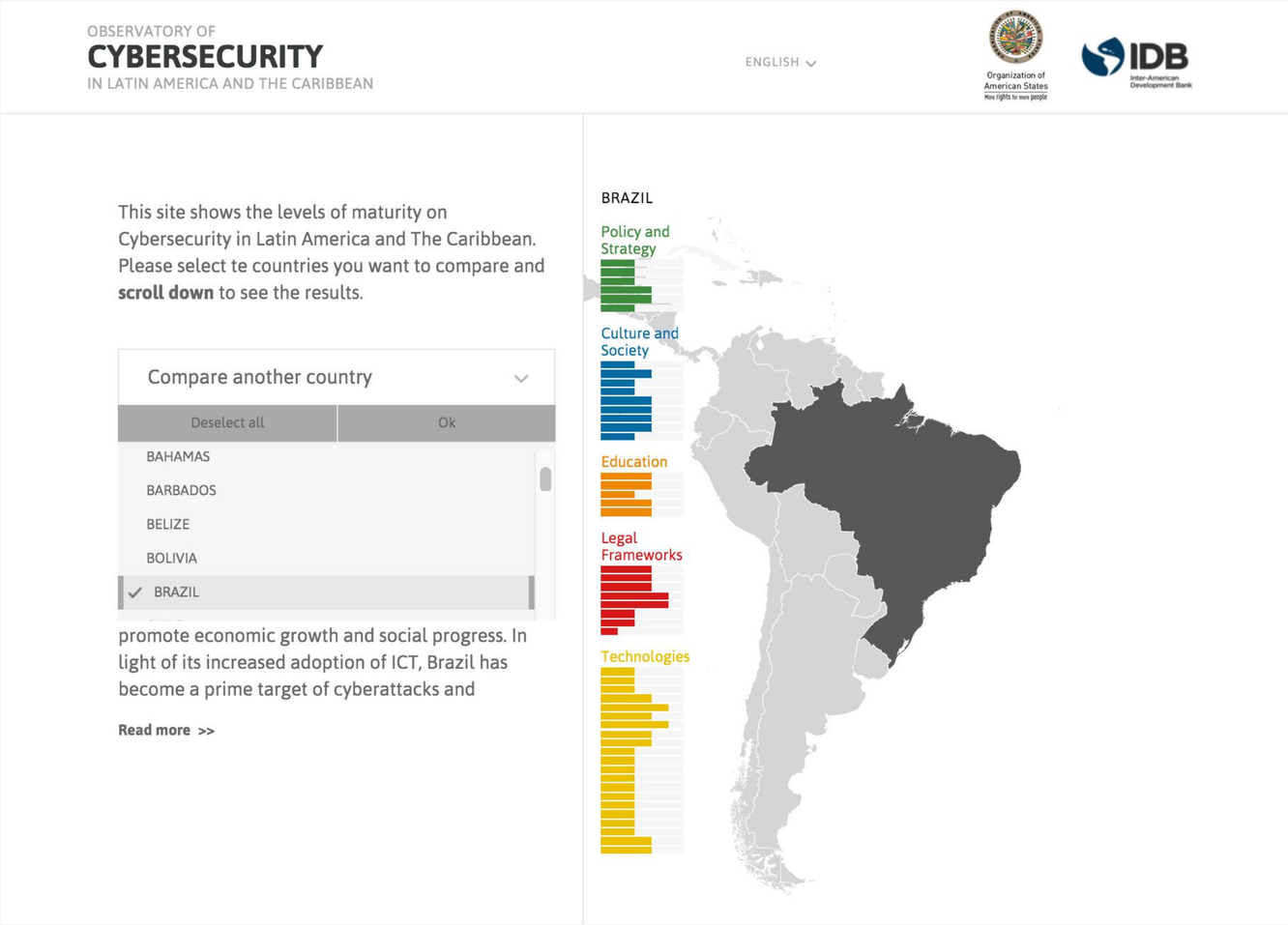
CMM - 5 Dimensions

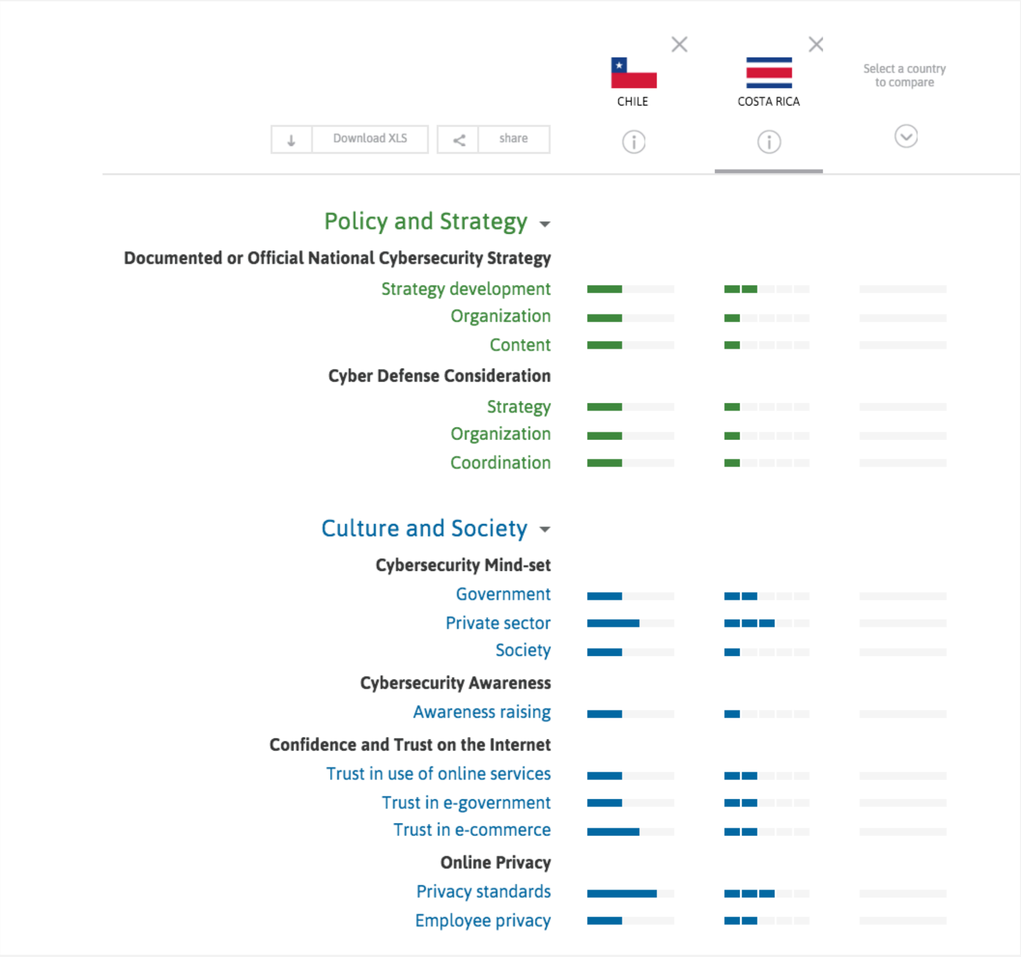
- Policy and Strategy
- Legal Frameworks
- Culture and Society
- Technologies
- Education

CMM - 5 Levels of Maturity

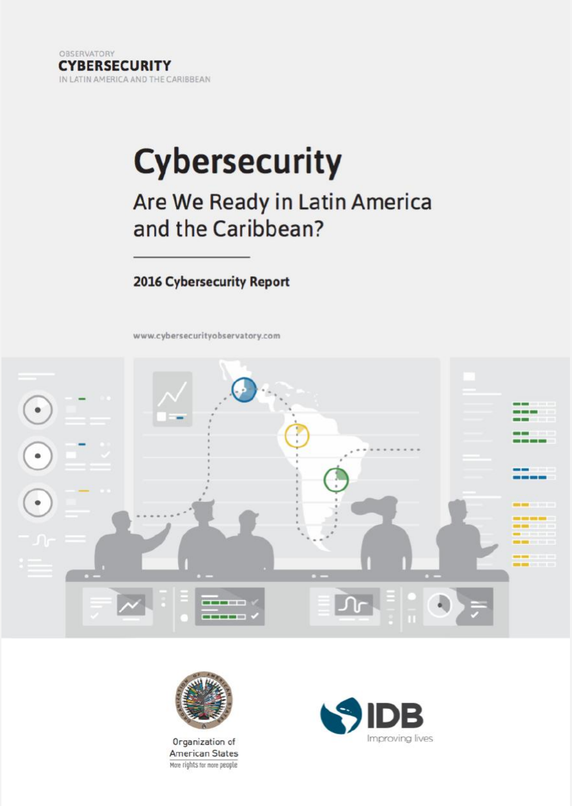


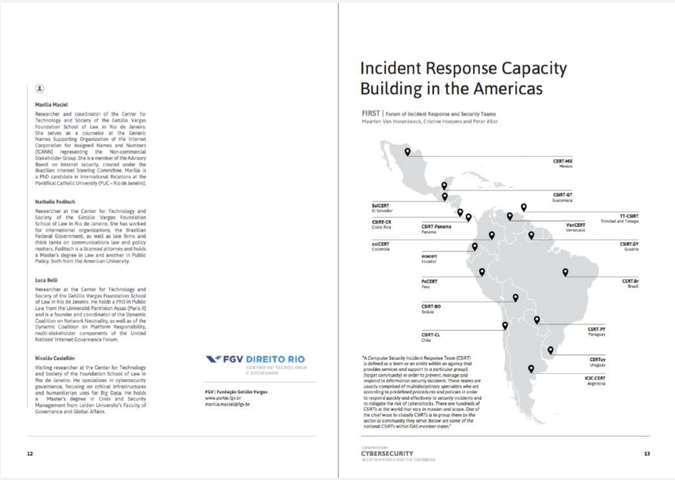
Observatory

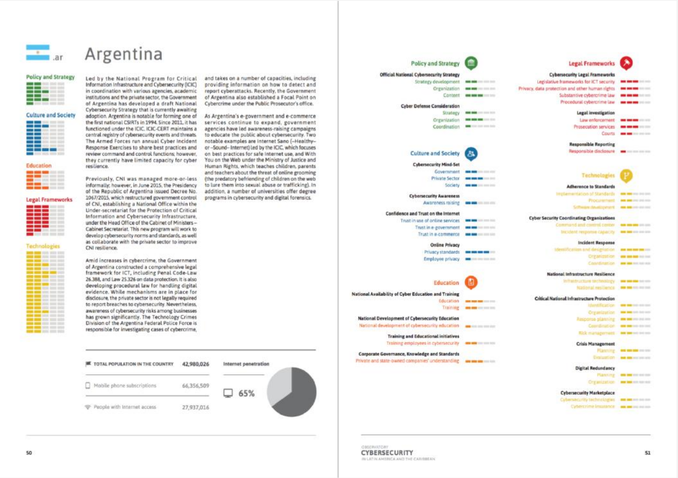


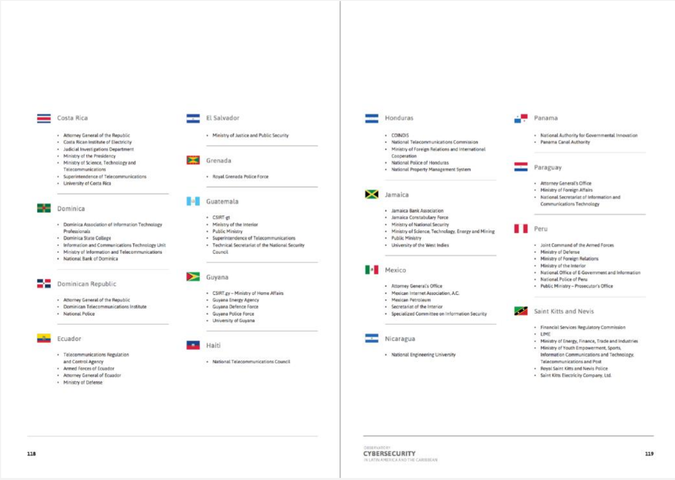


How the report looks?









Download Report

on Cybersecurity in Latin America and The Caribbean. Please select te 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

Read more >>

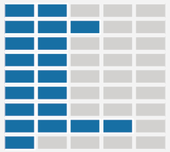
Advances in the region

Argentina

.ar

Policy and Strategy

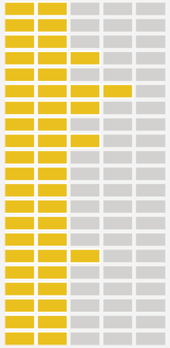
Culture and Society



Education

Legal Frameworks

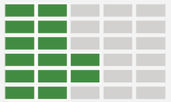
Technologies



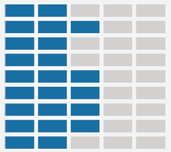
Brazil

.br

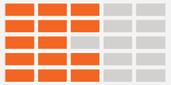
Policy and Strategy



Culture and Society

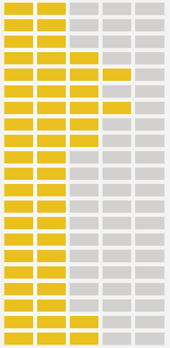


Education



Legal Frameworks

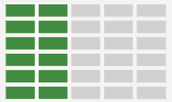
Technologies



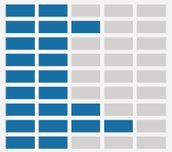
Chile

.cl

Policy and Strategy



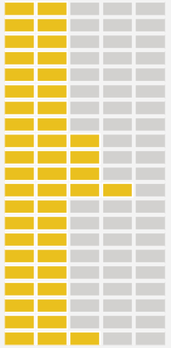
Culture and Society



Education

Legal Frameworks

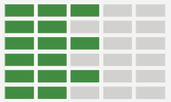
Technologies



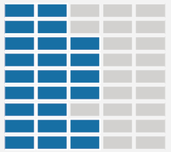
Colombia

.co

Policy and Strategy



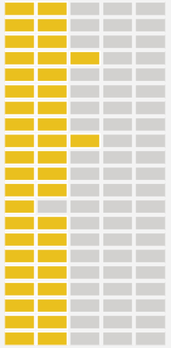
Culture and Society



Education

Legal Frameworks

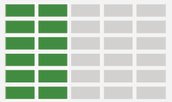
Technologies



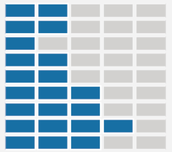
Mexico

.mx

Policy and Strategy



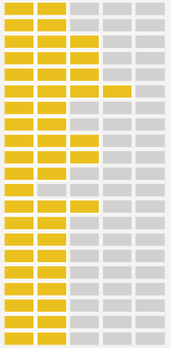
Culture and Society



Education

Legal Frameworks

Technologies

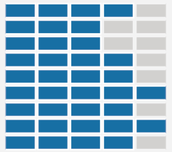


Uruguay

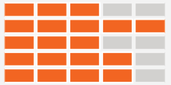
.uy

Policy and Strategy

Culture and Society

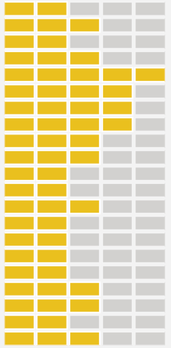


Education



Legal Frameworks

Technologies



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 group1 (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

27 of 32 countries do not have cyber security strategies

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

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."

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Thank you!
Merci
Gracias
Obrigado

Belisario Contreras

Cybersecurity Program Manager
Organization of American States

BContreras@oas.org
@belisarioc