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

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-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

Política y estrategia

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

Cultura y sociedad

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.

Educación

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 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

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

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 pais, con roles y responsabilidades identificadas; la actividad se concentra en la detección y respuesta a incidentes cibernéticos especificos 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 criticas; 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.

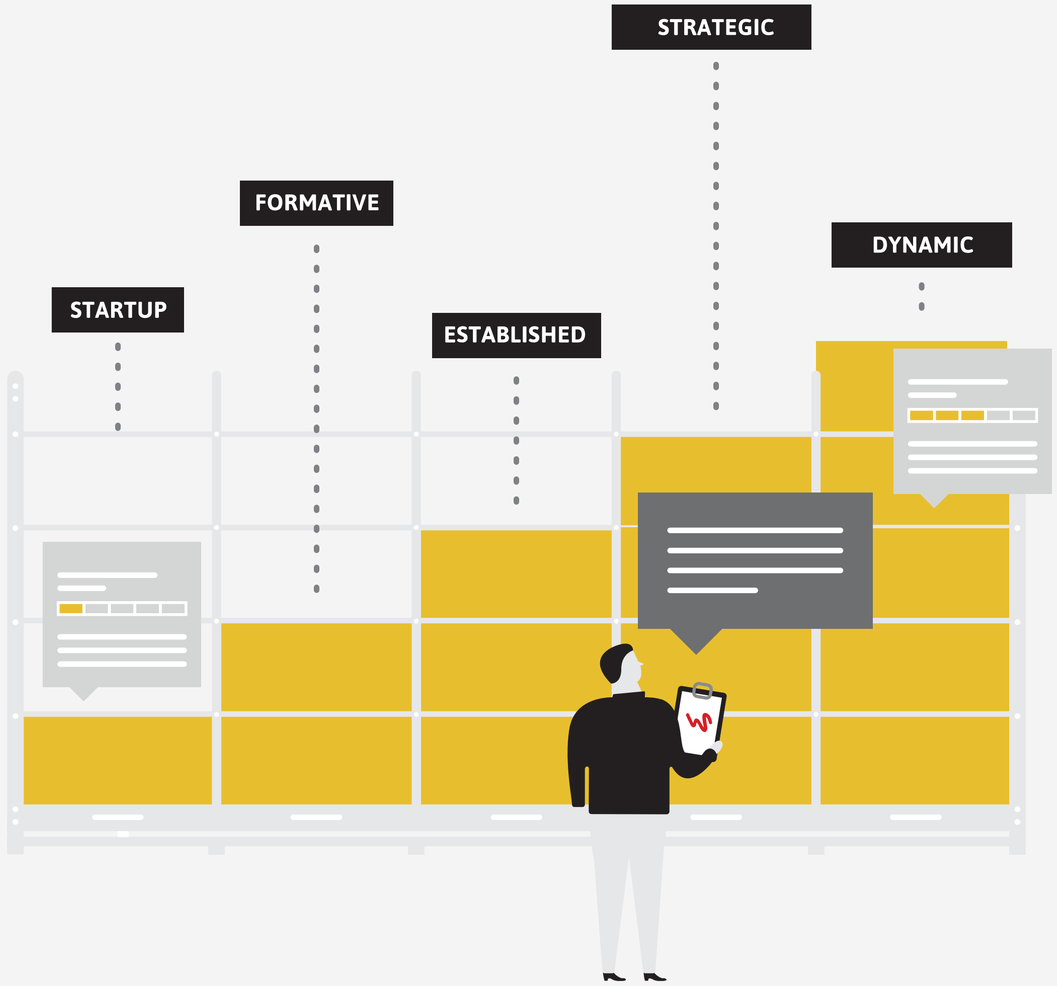
ESTRATÉGICO

La capacidad de respuesta a incidentes nacional apoya la creación de capacidades especificas 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.

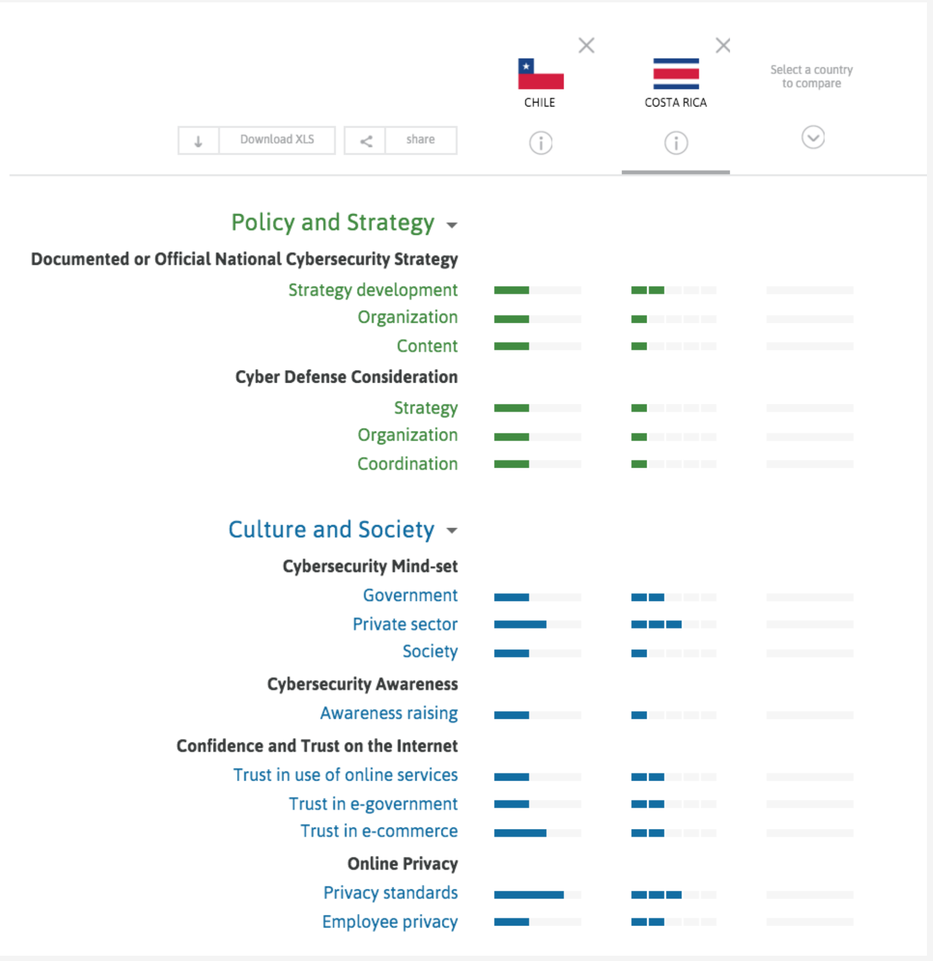
DINÁMICO

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.

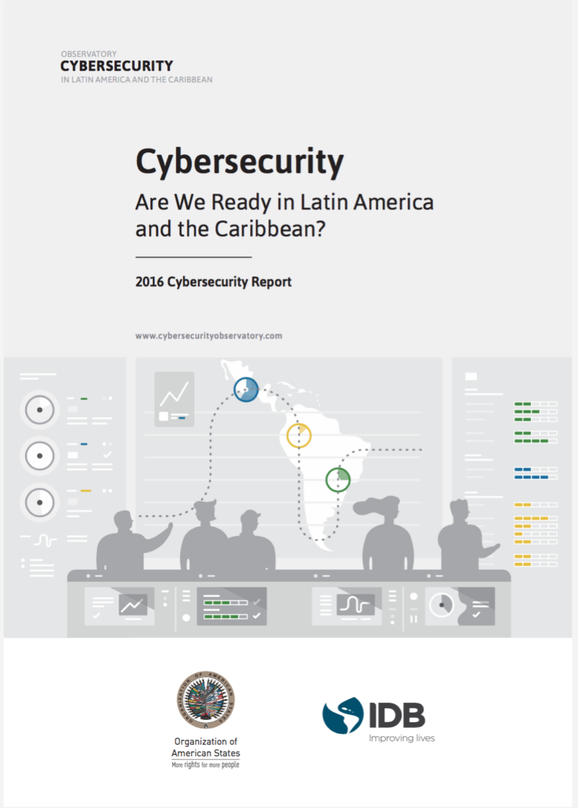
CMM - 5 Levels of Maturity

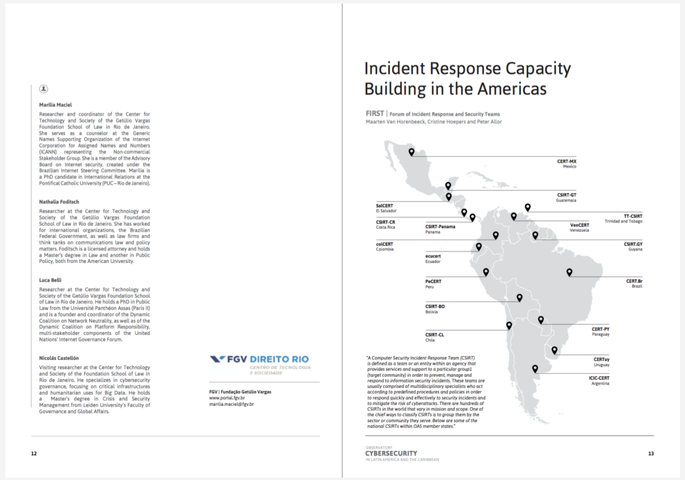


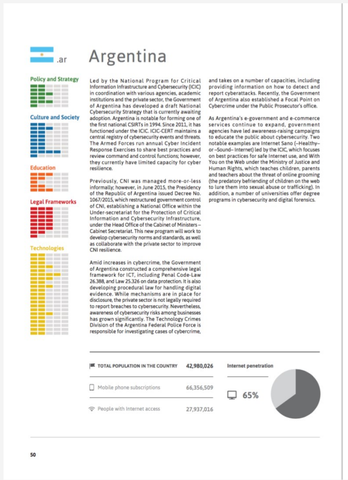
Observatory

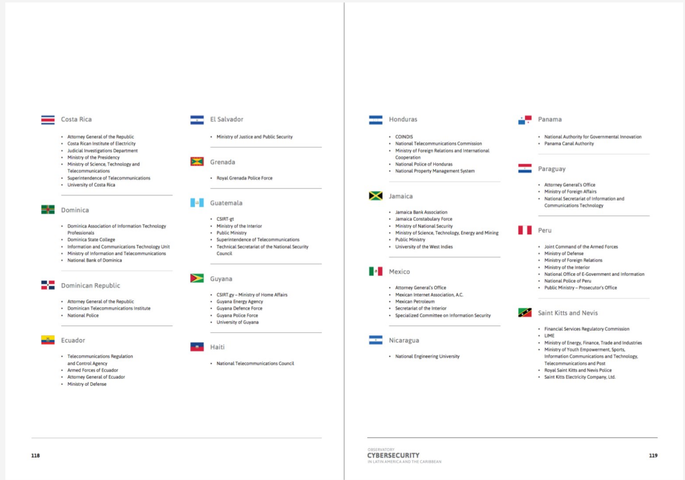


How the report looks?









Download Report

“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

Gonzalo Garcia-Belenguer

Cybersecurity Program Officer
Organization of American States

Ggarcia-belenguer@oas.org
@OASGonzalo