

# Revisión de capacidades de **Ciberseguridad**

**República Federativa de Brasil**



Global  
Cyber Security  
Capacity Centre



**OEA** Más derechos  
para más gente



Revisión de capacidades de

# Ciberseguridad

República Federativa de Brasil

# Agradecimientos

Esta publicación ha sido posible gracias a la colaboración de muchas personas e instituciones. Por ello, la Secretaría del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (CICTE/OEA), el Centro para la Capacidad de Ciberseguridad Global de la Universidad de Oxford, el Departamento de Seguridad de la Información - DSI de la Oficina de Seguridad Institucional de la Presidencia de la República de Brasil, y el Gobierno del Reino Unido agradece a las siguientes instituciones por haber participado en el proceso de elaboración y lanzamiento de este informe.

Ministerio de Defensa	Ministerio de Transporte	Grupos de respuesta a incidentes de seguridad en computadoras CAIXA (CSIRT / CAIXA)
Agencia Brasileña de Inteligencia (Abin)	Ministerio de Minas y Energía	Grupos de Respuesta a Incidentes de Seguridad Informática del Banco do Brasil (CSIRT / BB)
Centro de ciberdefensa (CDCIBER)	Oficina Federal de Asuntos Internos (CGU)	Grupo de respuesta a ataques SERPRO (GRA / SERPRO)
Ejército Brasileño (CIE)	Tribunal de Cuentas Federal (TCU)	Grupo de Respuesta a Incidentes de Seguridad Informática de la Cámara de Diputados (GRIS / CD)
Policía Federal de Brasil	Banco Central de Brasil	Rede-Rio de Computadores (CEO/Rede Rio)
Ministerio Público Federal	Ministerio de Industria, Comercio Exterior y Servicios	Grupo Abril Grupo de Respuesta a Incidentes de Seguridad (GRIS ABRIL)
Tribunal Superior de Justicia	Centro de coordinación e información de Ponto BR (NIC.BR)	Banco Caixa Geral
Ministerio de Justicia	Centro de Respuesta y Tratamiento Cibernético del Gobierno (CTIR.BR)	Banco de Brasil
Ministerio de Ciencia y Tecnología	Grupo de respuesta a incidentes de seguridad en Internet en Brasil (CERT.Br)	Telecomunicaciones brasileñas (Telebras)
Agencia Nacional de Telecomunicaciones (ANATEL)	Centro Nacional de Respuesta a Incidentes de Seguridad de la Red de Investigación e Incidentes (CAIS / RNP)	
Ministerio de Relaciones Exteriores	Centro de Coordinación de Incidentes de la Red del Ejército Brasileño (CCTIR / EB)	
Ministério de Educação	Centro de Manejo de Incidentes de la Red de la Fuerza Aérea Brasileña (CTIR.FAB)	
Ministerio de Trabajo y Empleo		
Ministerio de Planificación, Presupuesto y Gestión		
Ministerio de Hacienda		
Ministerio de Salud		

# Índice

- 7 Administración del Documento
- 8 Lista de Siglas
- 10 Resumen Ejecutivo**
- 27 Introducción**
- 29 Dimensiones de la Capacidad de Seguridad Cibernética
- 31 Etapas de Madurez de la Capacidad de Seguridad Cibernética
- 32 Metodología - Medición de la Madurez
- 35 Contexto de Seguridad Cibernética en Brasil**
- 37 Informe del Estudio**
- 38 Visión General



## 39 Dimensión 1 **Política y Estrategia de Seguridad Cibernética**

- 40 D 1.1 - Estrategia nacional de seguridad cibernética
- 43 D 1.2 - Respuesta a incidentes
- 46 D 1.3 - Protección de Infraestructura Crítica (IC)
- 49 D 1.4 - Gestión de Crisis
- 51 D 1.5 - Defensa Cibernética
- 52 D 1.6 - Redundancia de comunicaciones
- 53 Recomendaciones



## 57 Dimensión 2 **Cultura cibernética y sociedad**

- 58 D 2.1 - Mentalidad de Ciberseguridad
- 60 D 2.2 - Confianza y seguridad en Internet
- 62 D 2.3 - Comprensión del usuario de la protección de la información personal en línea
- 64 D 2.4 - Mecanismos de información
- 65 D 2.5 - Medios y redes sociales
- 66 Recomendaciones



## 68 Dimensión 3 **Educación, Capacitación y Habilidades en Seguridad Cibernética**

- 68 D 3.1 - Sensibilización
- 71 D 3.2 - Marco para la educación
- 72 D 3.3 - Marco para la formación profesional
- 74 Recomendaciones



## 78 Dimensión 4

### Marcos jurídicos y regulatorios

- 79 D 4.1 - Marcos jurídicos
- 84 D 4.2 - Sistema de justicia penal
- 87 D 4.3 - Marcos de cooperación formal e informal para combatir el delito cibernético
- 89 Recomendaciones



## 93 Dimensión 5

### Estándares, organizaciones y tecnologías

- 93 D 5.1 - Adhesión a los estándares
- 95 D 5.2 - Resiliencia de la infraestructura de Internet
- 96 D 5.3 - Calidad del Software
- 97 D 5.4 - Controles técnicos de seguridad
- 99 D 5.5 - Controles criptográficos
- 100 D 5.6 - Mercado de la ciberseguridad
- 101 D 5.7 - Divulgación responsable
- 102 Recomendaciones
  
- 106 Reflexiones adicionales
- 108 Referencias

---

# ADMINISTRACIÓN DEL DOCUMENTO

## Investigadores principales (2018):

Dr Ioannis Agrafiotis, Dr Eva Nagyfejeo, Dr Maria Bada

## Investigadores principales (2019):

Dr Andraz Kastelic

## Revisado por:

Profesor William Dutton, Profesor Michael Goldsmith,  
Profesor Basie von Solms

## Aprobado por:

Profesor Michael Goldsmith

Versión	Fecha	Notas
<b>1</b>	3 de agosto de 2018	Primer borrador para la Junta Técnica
<b>2</b>	16 de agosto de 2018	Segundo borrador revisado por la Junta Técnica
<b>3</b>	11 de septiembre de 2018	Tercer borrador revisado por la OEA
<b>4</b>	3 de julio de 2019	Primer borrador revisado después del taller de validación
<b>5</b>	21 de abril de 2020	Segundo borrador revisado entregado a la OEA después del taller de validación
<b>6</b>	18 de mayo de 2020	Tercera versión entregada a la OEA
<b>7</b>	5 de junio de 2020	Versión final entregada a la OEA

---

# LISTA DE SIGLAS

## ABIN

Agencia Brasileña de Inteligencia (Brazilian Intelligence Agency)

## ANATEL

Agencia Nacional de Telecomunicaciones (National Telecommunications Agency)

## CA

Autoridad de Certificación

## CEPESC

Centro para la Investigación y Desarrollo de Comunicaciones Seguras (Center for Research and Development of Secure Communications)

## CERT

Equipo de respuesta a emergencias informáticas (Computer Emergency Response Team)

## CGSIC

Comité Gestor de Seguridad de la Información y Comunicaciones (Committee on Information Security and Communications)

## CI

Infraestructura Crítica (Critical Infrastructure)

## CICTE

Comité Interamericano contra el Terrorismo (Inter-American Committee against Terrorism)

## CISM

Gerente Certificado de Seguridad de la Información (Certified Information Security Manager)

## CISSP

Profesional Certificado en Seguridad de Sistemas de Información (Certified Information Systems Security Professional)

## CMM

Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (Cybersecurity Capacity Maturity Model for Nations)

## CMU CERT

Equipo de Respuesta a Emergencias Informáticas de la Universidad Carnegie Mellon University (Carnegie Mellon University Computer Emergency Response Team)

## CNPJ

Registro Nacional de entidades Jurídicas (Identification number issued to Brazilian companies)

## CoE

Consejo de Europa (Council of Europe)

## CPF

Registro Nacional de Personas Naturales (Brazilian individual taxpayer registry identification)

## C-PROC

Programa sobre el delito cibernético de la Oficina del Consejo de Europa (Cybercrime Programme Office of the Council of Europe)

## CSIRT

Equipo de respuesta a incidentes de seguridad informática (Computer Security Incident Response Team)

## CTIR gov

Centro de Tratamiento y Respuesta a Incidentes de Gobierno (Brazilian Government Response Team for Computer Security Incidents)

## DDOS

Negación del servicio distribuida (Distributed Denial of Service)

## ECA

Estatuto de los Niños y Adolescentes (Child and Adolescent Statute)



## **FIRST**

Foro de Equipos de Respuesta a Incidentes y Seguridad (Forum of Incident Response and Security Teams)

## **FPA**

Administración Pública Federal (Federal Public Administration)

## **GCSCC**

Centro Global de Capacidad en Seguridad Cibernética (Global Cyber Security Capacity Centre)

## **GSI**

Oficina de Seguridad Institucional de la Presidencia de la República (Institutional Security Cabinet of the Presidency)

## **ICT**

Information and Communication Technologies Tecnología de la Información y las Comunicaciones (Information and Communication Technologies)

## **IDS**

Sistema de Detección de Intrusos (Intrusion Detection Systems)

## **ISP**

Proveedor de Servicios de Internet (Internet Service Provider)

## **KPIs**

Indicadores Clave de Desempeño (Key Performance Indicators)

## **LACNIC**

Registro de Direcciones de Internet de América Latina y el Caribe (Latin American and Caribbean Internet Addresses Registry)

## **NGO**

Organizaciones No Gubernamentales (Non-Governmental Organization)

## **NIST**

Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology)

## **OAS**

Organización de los Estados Americanos (Organization of American States)

## **RNP**

Red Nacional de Educación e Investigación (Brazilian National Research and Educational Network)

## **SENAC**

Servicio Nacional de Aprendizaje Comercial (National Service for Commercial Education)

## **SERPRO**

Servicio Federal de Procesamiento de Datos (Federal Data Processing Service)

## **SIAFI**

Sistema Integrado de Administración Financiera del Gobierno Federal (Integrated System of Financial Administration of the Federal Government)

## **SIEM**

Información de Seguridad y Gestión de eventos (Security Information and Event Management)  
SME PYMES Pequeñas y medianas empresas (Small and medium-sized enterprises)

## **SPED**

Sistema Público de Contabilidad Digital (Public System of Digital Bookkeeping)

## **SSH**

Secure Shell

## **STIX**

Structured Threat Information eXpression

## **TCU**

Tribunal Federal de Cuentas (Federal Court of Accounts)

## **TLP**

Protocolos de semáforos (Traffic Light Protocols)

## **URCC**

Unidad de Crímenes Cibernéticos (Federal Police Unit for Combating Cybercrime)

# RESUMEN EJECUTIVO

El Centro Global de Capacidad en Seguridad Cibernética (GCSCC o “el Centro”) realizó un estudio de la madurez de la capacidad en materia de seguridad cibernética en Brasil por invitación de la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OAS), a través de su programa de seguridad cibernética y en colaboración con dicha Secretaría. El objetivo del estudio es permitir que el Gobierno comprenda su capacidad en materia de seguridad cibernética a fin de priorizar estratégicamente la inversión en capacidades de seguridad cibernética.

Durante los días 19 y 20 de marzo de 2018, las siguientes partes interesadas participaron en las consultas de mesa redonda: la justicia penal, los organismos encargados de la aplicación de la ley, la comunidad de defensa, funcionarios de tecnología de la información, representantes de entidades del sector público, propietarios de infraestructura crítica, los encargados de la formulación de políticas, los equipos de respuesta a emergencias informáticas, funcionarios de tecnología de la información del sector privado (incluidas las instituciones financieras), las empresas de telecomunicaciones, el sector bancario y los socios internacionales.

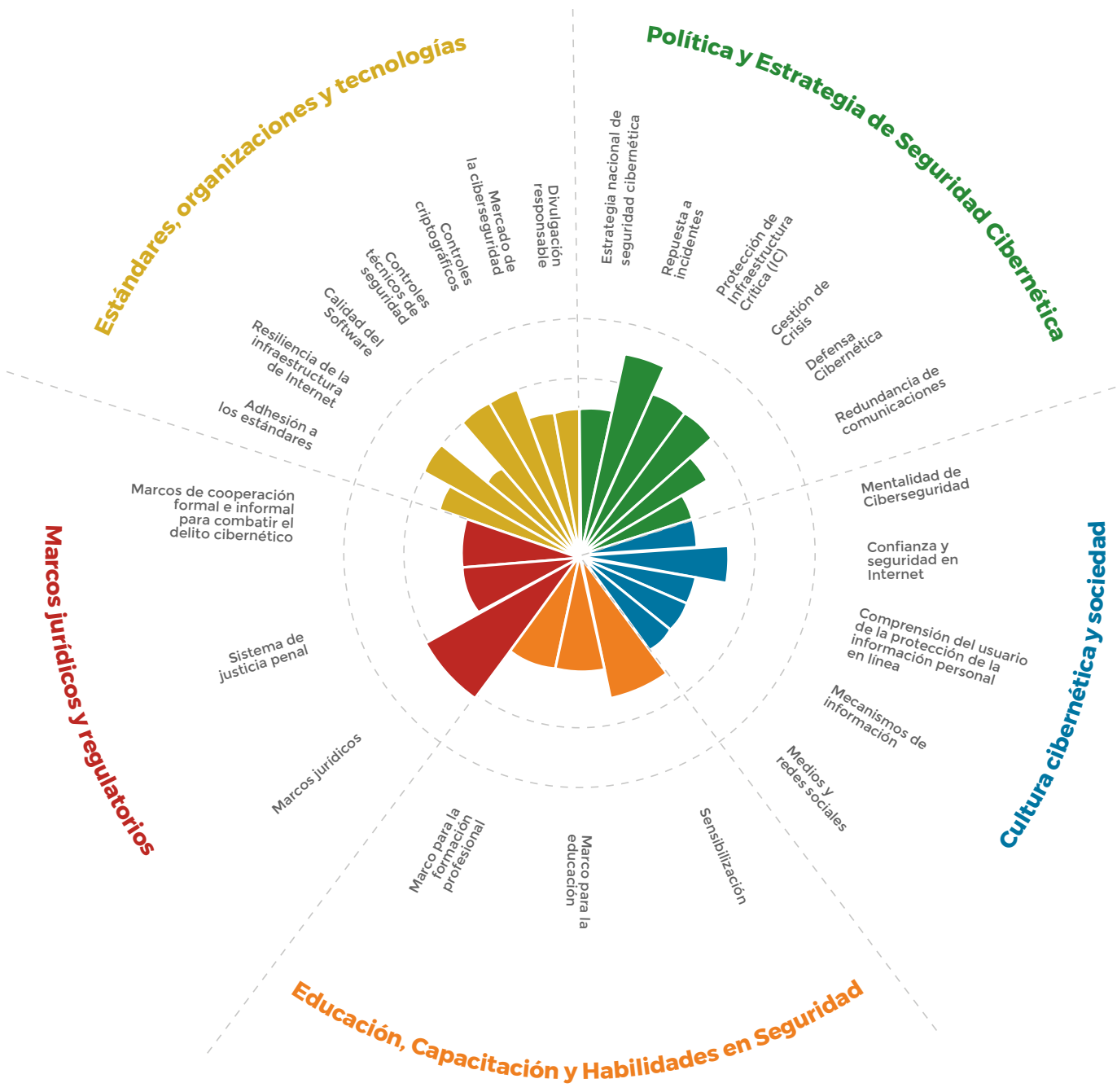
Los investigadores del Centro Global de Capacidad en Seguridad Cibernética (GCSCC) visitaron Brasilia una vez más al año siguiente para validar los resultados de 2018 y actualizar el borrador del correspondiente informe de Revisión de la Capacidad de Ciberseguridad. La metodología de recopilación de datos utilizada en marzo de 2019 fue similar a la utilizada el año anterior. Entre los interesados que participaron en las entrevistas de los grupos de discusión figuraban representantes del mundo académico, operadores de infraestructura crítica nacional, proveedores de telecomunicaciones y otras entidades del sector privado, los ministerios de gobierno, el poder judicial, los organismos encargados de la aplicación de la ley, la comunidad de defensa, el sector financiero, los equipos de respuesta a emergencias informáticas (CERT), los medios de comunicación, el sector privado y la sociedad civil.

Tanto en 2018 como en 2019, las consultas se realizaron utilizando el Modelo de Madurez de la Capacidad de Ciberseguridad del Centro, que define cinco dimensiones de la capacidad de ciberseguridad;

- Política y estrategia de ciberseguridad
- Cultura cibernética y sociedad
- Educación, capacitación y habilidades en Ciberseguridad
- Marcos jurídicos y regulatorios
- Estándares, organizaciones y tecnologías

Cada dimensión está compuesta por un número de factores que describen lo que significa poseer la capacidad de ciberseguridad. Cada factor presenta un número de aspectos y para cada aspecto hay indicadores que describen los pasos y acciones que, una vez observados, definen el estado de madurez de dicho aspecto. Existen cinco etapas de madurez, desde la etapa inicial hasta la etapa dinámica. La etapa inicial implica un enfoque ad hoc de la capacidad, mientras que la etapa dinámica representa un enfoque estratégico y la capacidad de adaptarse dinámicamente o de cambiar en respuesta a consideraciones externas. En el documento del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM, por sus siglas en inglés) se presentan más detalles sobre las definiciones de cada una de las etapas en todas sus dimensiones.<sup>1</sup>

La Figura 1 (abajo) ofrece una representación general de la capacidad de ciberseguridad en Brasil e ilustra los estimados de madurez en cada dimensión. Cada dimensión representa una quinta parte del gráfico, con las cinco etapas de madurez de cada factor extendiéndose hacia afuera desde el centro del gráfico; el “inicio” está más cerca del centro del gráfico y el “dinámico” está situado en el perímetro.



**Figura 1: Representación general de la capacidad de seguridad cibernética en Brasil**



# Política y estrategia de ciberseguridad

En el momento del estudio, en marzo de 2018, no existía ningún documento oficial nacional sobre seguridad cibernética en el que se detallara cómo establecer la coordinación entre las principales partes interesadas gubernamentales y no gubernamentales en materia de seguridad cibernética. La falta de colaboración entre las instituciones gubernamentales y el sector privado, así como la “fragmentación de las respuestas” se abordaron potencialmente con la Estrategia (2015-2018). El objetivo de la Estrategia fue detallar las directrices estratégicas para la seguridad de la información y las comunicaciones, así como coordinar esta labor entre los diversos actores participantes con el fin de mitigar los riesgos a los que están expuestas las organizaciones y la sociedad. La estrategia se centró en la Administración Pública Federal (FPA), y los críticos destacaron la ausencia de una autoridad central para aplicar ese enfoque sistemático y de múltiples interesados, así como la ausencia de organizaciones de la sociedad civil, de partes interesadas de Internet y del público en general en el diseño de la estrategia. En cuanto a la organización del programa de seguridad cibernética, los participantes expresaron su preferencia por un modelo descentralizado, en el que los sectores comerciales serían supervisados por los organismos regulatorios ya establecidos con un organismo nacional de reciente creación que coordinaría la labor.<sup>2</sup>

Tras la validación de las entrevistas de los grupos de discusión realizadas en marzo de 2019, se confirmó que la Estrategia Nacional de Ciberseguridad (Decreto Federal N° 10.222) se aprobó finalmente en febrero de 2020.<sup>3</sup> De acuerdo con las fuentes gubernamentales la estrategia se centra en diez acciones estratégicas que deben guiar a la Administración Pública Federal para idear sus propias acciones hacia la ciberseguridad.

Con relación a respuesta a incidentes, hay muchos Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT),<sup>4</sup> desde las entidades gubernamentales hasta el sector privado y las instalaciones académicas. Según la función que desempeñe un CERT, esas entidades pueden participar exclusivamente en la gestión de la seguridad de los sistemas, hacer cumplir las directrices de seguridad cibernética o encargarse de coordinar la labor entre las autoridades nacionales y locales. El Equipo nacional de respuesta a emergencias informáticas (CERT.br) es un organismo certificado por el Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST) que se encarga de la tramitación de los informes de incidentes para el sector privado.<sup>5</sup> El Equipo de Respuesta a Incidentes de Seguridad Informática del Gobierno del Brasil (CTIR Gov) proporciona una respuesta a los incidentes para la Administración Pública Federal (FPA), mientras que los Equipos de respuesta a emergencias informáticas (CERT) se dedican a sectores específicos y partes interesadas en la infraestructura crítica. Además, hay un CERT militar que protege las redes militares. Todas estas instituciones tienen directrices y funciones claras en lo que respecta a la respuesta a los incidentes. El CERT.br mantiene el registro de incidentes nacionales y publica anualmente datos estadísticos de amenazas e incidentes. Todos los CERT presentan informes a través de canales oficiales al CERT.br. Los sistemas automatizados que siguen las normas internacionales, tales como la Expresión estructurada de información sobre amenazas (STIX) y los Protocolos de semáforo (TLP), garantizan que la información sobre amenazas se comparta con los CERT que colaboran con el CERT.br. La labor jurídica actual se centra

en la racionalización del intercambio de información sobre amenazas entre todos los CERT, ya que no todas las partes interesadas en la infraestructura crítica privada tienen derecho a recibir información sobre amenazas. A medida que aumenta la gama de partes interesadas en la infraestructura crítica, es necesario contar con una mayor participación de las instituciones de investigación.

La madurez de la capacidad de Brasil para proteger la infraestructura crítica difiere entre los operadores de infraestructura crítica (IC) públicos y privados. Todas las instituciones federales deben realizar evaluaciones del riesgo cibernético que se actualizan anualmente en función de las lecciones aprendidas de los principales eventos. Las partes interesadas de infraestructura crítica pública incluyen empresas de telecomunicaciones, transporte, energía e instituciones financieras, todas las cuales cooperan y coordinan a través de canales formales de comunicación con el Ministerio de Defensa. Existen políticas y procedimientos claramente definidos que todas las instituciones públicas deben seguir en función de la información proporcionada por la herramienta de conocimiento de la situación de CERT.br. Se facilita el acceso de la Policía Federal a esos protocolos y a los servicios de inteligencia para aumentar la cooperación entre las partes interesadas de la infraestructura crítica. Actualmente no se considera que el sector privado forme parte de la infraestructura crítica del país. Dado que Brasil ha respaldado la privatización en sectores críticos como el financiero, es imperativo que se vuelva a examinar la lista de partes interesadas de la infraestructura crítica, para considerar las instituciones privadas. Las instituciones privadas no tienen ninguna obligación de informar al Gobierno de un incidente importante; se restringe su acceso a la información de inteligencia sobre amenazas y no tienen en cuenta las evaluaciones de riesgos y los procesos que el Gobierno tiene en marcha para los operadores públicos de infraestructura pública. Por consiguiente, las instituciones privadas deben elaborar sus propias evaluaciones internas de riesgos y políticas de seguridad, cuya eficacia dependerá de su grado de madurez. La mayoría de los participantes instaron al Gobierno a que creara un mecanismo para determinar el grado de madurez de la gobernanza de la tecnología de la información tanto en el sector público como en el privado, un protocolo de comunicación para distribuir alertas en los sectores público y privado y una iniciativa para evaluar las normas y los estándares aplicados por las organizaciones privadas y públicas.

Durante el último decenio, Brasil fue anfitrión de una serie de eventos importantes y, como era de esperar, el país experimentó una serie de ataques cibernéticos durante dichos eventos. Los procesos de manejo de incidentes durante esos eventos demostraron que las organizaciones críticas para la ciberdefensa fueron capaces de colaborar y mitigar eficazmente el impacto de estos ataques. Las organizaciones que participaron en la gestión de crisis tenían funciones claras, contaban con protocolos transparentes sobre la forma de difundir la información y cómo frenar la escalada del incidente, así como con orientaciones específicas sobre la forma de proteger los sistemas. Sin embargo, los procesos de gestión de crisis se adaptaron a esos eventos específicos. La experiencia y las lecciones aprendidas de esos eventos deberían servir de base para la labor actual en materia de gestión de crisis. Es necesario diseñar protocolos de gestión de crisis y crear una red de organizaciones públicas y privadas para manejar las crisis. Se sugirió que la capacitación y los ejercicios de simulación de eventos de crisis eran la forma óptima de validar los protocolos de comunicación, aumentar la conciencia sobre la seguridad cibernética y poner a prueba los procesos de manejo de incidentes. En ese sentido, los participantes mencionaron el ejercicio Cyber Guardian, que utiliza la planificación de alto nivel para concebir escenarios y plataformas de simulación de operaciones cibernéticas que pueden emular los sistemas críticos de los sectores financiero, nuclear y público.

En cuanto a la gobernanza de la seguridad cibernética, el Gobierno de Brasil asignó los aspectos político y estratégico al Gabinete de Seguridad Institucional de la Presidencia de la República (GSI) y los procedimientos estratégicos, operacionales y de ciberdefensa al Ministerio de Defensa. En los últimos años,

las fuerzas armadas se reestructuraron para adaptarse a las necesidades de un sistema democrático en evolución, centrándose en las nuevas amenazas transfronterizas y los eventos de seguridad interna. Existe un documento oficial de ciberdefensa, publicado en 2012, así como directrices sobre políticas en materia de ciberseguridad. El ejército opera un CERT y proporciona formación sobre gestión de riesgos y respuesta a incidentes. Los participantes señalaron que el ejército posee capacidades tanto ofensivas como defensivas y se centra en la mejora de las medidas defensivas. Indicaron que los militares despliegan sistemas que proporcionan conocimientos de la situación y defienden proactivamente contra los ataques de denegación de servicio distribuido (DDoS) o la desfiguración de la web. Existen laboratorios de análisis de programas informáticos maliciosos y un número importante de personal está recibiendo capacitación para ejecutar esas tareas.

No fue posible obtener una visión completa con respecto a la redundancia de comunicaciones en el curso del estudio del CMM. Los participantes señalaron que el sector público dispone de medios de respuesta a las emergencias integrados en la estrategia nacional y en su red de comunicaciones de emergencia, con recursos apropiados para evaluar los actuales protocolos en materia de redundancia, evaluar los sistemas redundantes, ejecutar ejercicios y realizar simulacros de comunicación. Hay múltiples centros de crisis designados en lugares geográficos dispersos para garantizar la participación de todas las partes interesadas en caso de emergencia. En marcado contraste, el sector privado está descuidado y excluido de estos planes, con la excepción de los CERT privados.

# Cultura cibernética y sociedad



En lo que respecta a la dimensión de cultura cibercultura y sociedad, el Gobierno ha reconocido la necesidad de dar prioridad a la seguridad cibernética en todas sus instituciones. Asimismo, se han diseñado aspectos de los procesos gubernamentales y las estructuras institucionales en respuesta a los riesgos de seguridad cibernética, pero las iniciativas se encuentran principalmente en los organismos directivos. En general, los participantes observaron que la cultura de seguridad en Brasil varía en las distintas partes del país y en los diferentes sectores del Gobierno y la economía. Una preocupación señalada por los participantes es que las estructuras gubernamentales son muy complejas. Por consiguiente, si se evalúa la madurez del sector público, pueden identificarse diversas etapas dentro de los distintos departamentos. Otra preocupación planteada por los participantes es la falta de un mecanismo de coordinación para identificar el nivel de madurez dentro del gobierno y entre los gobiernos.

Las principales empresas del sector privado han comenzado a dar mayor prioridad a la mentalidad de seguridad cibernética identificando las prácticas de alto riesgo. Los sectores de finanzas y tecnología de la información están más avanzados en materia de seguridad cibernética; al ser objetivos más frecuentes, están invirtiendo más en la seguridad cibernética. Los participantes nos informaron que, desde que los bancos nacionales comenzaron a adoptar medidas de seguridad proactivas, los delincuentes se han dirigido cada vez más a los bancos regionales y a las pequeñas y medianas empresas (PYME). Una proporción limitada, pero en aumento de usuarios de Internet en Brasil ha comenzado a dar mayor prioridad a la seguridad cibernética; por ejemplo, a través de la determinación de riesgos y amenazas. La sociedad en su conjunto sigue careciendo de una mentalidad de seguridad cibernética; los usuarios pueden ser conscientes de los riesgos de la seguridad cibernética, pero a menudo no actúan en consecuencia en sus prácticas cotidianas. Se mencionó que es común, incluso para los expertos en tecnología de la información, que son conscientes de los riesgos, abrir los correos electrónicos de phishing o compartir información sensible en sitios de las redes sociales, como Facebook.

En general, las partes interesadas participantes consideran que sólo una pequeña proporción de los usuarios de Internet evalúan críticamente lo que ven o reciben en línea. Del mismo modo, pocos creen que los usuarios finales tengan las aptitudes necesarias para utilizar el Internet de manera segura y para protegerse en línea.

En general, se insta a las empresas a prestar servicios en línea. La prestación de servicios de comercio electrónico ha aumentado desde 2017. En 2017, Brasil (la Policía Federal Brasileña) y Europol firmaron un acuerdo estratégico para aumentar la cooperación en la lucha contra las actividades delictivas transfronterizas, lo cual podría considerarse una cooperación oficial. Una proporción cada vez mayor de usuarios confía en el uso seguro de los servicios de comercio electrónico. El Ministerio de Justicia cuenta con una secretaría que se encarga de los derechos del consumidor y del comercio electrónico.



Los servicios de gobierno electrónico también se han ido desarrollando y una proporción cada vez mayor de usuarios confía en el uso seguro de estos servicios. Desde 1998 se dispone de servicios como los de envío de declaraciones de impuestos a la renta y el suministro de información sobre la seguridad social y las adquisiciones gubernamentales a través de Internet.

Se considera que un número cada vez mayor de usuarios y partes interesadas de los sectores público y privado tienen conocimientos generales sobre la forma en que se maneja la información personal en línea y emplean buenas prácticas de seguridad cibernética (proactivas) para proteger su información personal en línea. Las regulaciones de datos personales que se están discutiendo en la UE no están de acuerdo con las que se están discutiendo en el Brasil. Se han iniciado debates sobre el enfoque de Brasil en materia de protección de la información personal y sobre el equilibrio entre la seguridad y la privacidad, pero esto todavía no ha dado lugar a medidas o políticas concretas.

En Brasil, tanto el sector público como el privado cuentan con algunos canales para informar sobre incidentes en línea, pero esos canales no están bien coordinados y, por lo general, se utilizan de manera ad hoc. Se establecieron mecanismos de denuncia para que los usuarios informen sobre los delitos relacionados con Internet, los cuales se utilizan con frecuencia. SaferNet Brasil<sup>6</sup> proporciona información sobre la seguridad en Internet y los medios para registrar las quejas a través de su sitio web. SaferNet Brasil es una organización sin fines de lucro creada en 2005. Además, la Policía Federal<sup>7</sup> tiene una página dedicada para registrar las denuncias en su sitio web que también se pueden enviar a una dirección de correo electrónico exclusivamente para ese tipo de denuncias. El contenido ilegal en línea puede denunciarse a la línea de asistencia sobre pornografía infantil y adolescente<sup>8</sup> establecida por el Gobierno.

Todos los incidentes pueden ser denunciados a la policía, mientras que los que no están claramente clasificados se envían al Centro de Tratamiento y Respuesta a Incidentes Cibernéticos del Gobierno (CTIR Gov) y luego se categorizan antes de ser enviados a las instituciones correspondientes. En general, los participantes indicaron que los ciudadanos de Brasil no tienen una cultura de denuncia. Además, no fue posible determinar con qué frecuencia o rutina se utilizan los mecanismos de presentación de informes establecidos por los sectores público y privado.

En Brasil hay una cobertura mediática ad hoc de la seguridad cibernética, en la que se suministra información limitada y con poca frecuencia se informa sobre cuestiones concretas a las que se enfrentan las personas en línea, como la pornografía infantil en línea o el acoso cibernético. Además, los participantes mencionaron que el debate sobre la seguridad cibernética en los medios de comunicación social es limitado. Por lo general, los medios de comunicación hacen caso omiso a los detalles técnicos de los incidentes de seguridad cibernética y con frecuencia ofrecen una orientación y un asesoramiento posiblemente incorrectos sobre el comportamiento seguro en línea.



# Educación, capacitación y habilidades en ciberseguridad

Aún no se ha establecido un programa nacional de sensibilización sobre la seguridad cibernética dirigido por una organización designada (de cualquier sector) que aborde una amplia gama de cuestiones demográficas.

Debido a la falta de participantes de la sociedad civil, no fue posible obtener una idea clara de las iniciativas existentes destinadas a aumentar la conciencia sobre la seguridad cibernética.

Durante el proceso de revisión, el organismo de sensibilización más importante reconocido por los participantes fue SaferNet Brasil, una ONG creada en 2005. Tiene conexiones especiales con el Ministerio de Justicia, la Policía Federal y la Secretaría de Derechos Humanos de la Presidencia de la República y existe para “proteger los derechos humanos y servir de línea telefónica de ayuda y nodo de sensibilización en Brasil”.<sup>9 10</sup>

El Comité Directivo de Internet en Brasil ([www.cgi.br](http://www.cgi.br)), un consejo de múltiples partes interesadas creado por la Ordenanza Interministerial 147, del 31 de mayo de 1995, es la principal institución encargada de promover las normas de seguridad de las tecnologías de la información y las comunicaciones (TIC) y las mejores prácticas de Internet, y lleva a cabo sus actividades a través del Centro Brasileño de Información en Red (NIC.br) (<http://nic.br/quem-somos/>).<sup>11</sup> Basándose en la investigación documental, el NIC.br puso en práctica varias iniciativas como Antispam.br<sup>12</sup> (<http://www.antispam.br/>) e InternetSegura.br<sup>13</sup> (<https://www.Internetsegura.br/>), dos portales que tienen por objeto sensibilizar a los niños y padres sobre los correos electrónicos no solicitados y que difunden material sobre seguridad en Internet.<sup>14</sup>

En lo que respecta a la sensibilización de los ejecutivos sobre la seguridad cibernética, los participantes reconocieron que el nivel suele ser bajo entre los miembros de los cargos directivos de las empresas y que es necesario educarlos sobre la forma en que los riesgos de la seguridad cibernética afectan a la organización. Además, no existe la obligación de que los ejecutivos reciban capacitación en materia de seguridad cibernética, aunque se considera una práctica óptima.

Debido a la falta de participación del mundo académico, no fue posible obtener una imagen clara sobre la educación en materia de seguridad cibernética en Brasil. Por lo tanto, la información proporcionada se basa en una investigación documental.

Los principales interesados gubernamentales y de la industria señalaron la necesidad de mejorar la educación en materia de seguridad cibernética en las escuelas y universidades.

El Ministerio de Educación establece el plan nacional de estudios sobre cursos, requisitos y normas relacionados con la seguridad cibernética, pero el nivel de desarrollo se deja a decisión de las universidades. No está regulado por un organismo central. En el estudio no se informó si hay un

presupuesto nacional distinto reservado para la educación en materia de seguridad cibernética. Del mismo modo, en los debates de los grupos de discusión no quedó claro en qué medida existe cooperación entre el sector privado y las universidades.

Es fácil conseguir educadores con los títulos exigidos en seguridad cibernética. En Brasil, se ofrecen cursos especializados en informática a nivel universitario.

La necesidad de formar profesionales en ciberseguridad ha sido reconocida por el Gobierno. Basándose en la investigación documental, el Comité Gestor de Internet de Brasil (CGI.br) (véase D 3.1) coordina la labor de capacitación a través del CERT.br, el Portal de Mejores Prácticas (BCP.nic.br) y el CGSIC. Los participantes declararon que la mayoría de los profesionales del sector público obtienen sus títulos profesionales en materia de tecnología de la información en el extranjero y reciben certificados en materia de tecnología de la información y las comunicaciones, como el título de Profesional Certificado en Seguridad de los Sistemas de Información (CISSP) y el título de Gestor Certificado en Seguridad de la Información (CISM), autorizados por instituciones internacionales (International Information System Certification Consortium (ISC)2 and ISACA ®).

La red de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT) ha sido aceptada como “una norma de facto para las buenas prácticas en todo Brasil, en organizaciones privadas, públicas y gubernamentales”.<sup>15</sup>

# Marcos jurídicos y reglamentarios

Brasil no tiene un marco regulatorio completo que se haga cargo explícitamente de la seguridad cibernética. A pesar de los esfuerzos por introducir una reglamentación mediante un marco legislativo vinculante, la legislación sobre seguridad cibernética en Brasil sigue en proceso de evolución. Sin embargo, se han adoptado varias directrices oficiales o “leyes blandas” que se refieren a cuestiones de seguridad cibernética.

La Ley de Delitos Cibernéticos (Ley N° 12.737/2012),<sup>16</sup> también conocida como la “Ley Carolina Dieckmann”, y el Marco Civil de Internet de Brasil (Ley N° 12.965/2014)<sup>17</sup> se consideran los instrumentos legislativos vigentes más pertinentes y sustantivos y tienen por objeto manejar formalmente los delitos cibernéticos y otorgar facultades procesales al manejar pruebas electrónicas.

El Marco Civil de Internet de Brasil (Ley N° 12.965/2014) (Marco Civil da Internet) se elaboró mediante un proceso de consulta con múltiples interesados a fin de regular el uso de Internet en Brasil mediante el establecimiento de principios, garantías, derechos y deberes para los usuarios de Internet.

En el momento de los estudios, en marzo de 2018 y marzo de 2019, Brasil no contaba con una ley específica de protección de datos o privacidad, sino que se basaba en diversas disposiciones establecidas en la Constitución Federal,<sup>18</sup> el Código Penal del Brasil,<sup>19</sup> el Código de Protección del Consumidor<sup>20</sup> y el Marco Civil de Internet de Brasil para proteger la privacidad en Internet.

Se aprobó y aplicó una amplia legislación para la protección de los niños en línea. El artículo 241-D del Estatuto de los Niños y Adolescentes (ECA) define la captación de menores de edad en línea y establece la pena de uno a tres años de prisión.<sup>21</sup> Algunos participantes criticaron esta pena por ser demasiado indulgente y expresaron su preocupación por la falta de una legislación comparable que tipifique como delito el ciberacoso, el sexting y el acceso o la descarga de imágenes de pornografía infantil.

En la actualidad, Brasil también carece de una legislación que trate explícitamente las amenazas cibernéticas a la propiedad intelectual (PI). Una excepción es la Ley de Derecho de Autor (Ley 9.610/1998),<sup>22</sup> que garantiza la protección de cualquier tipo de producto intelectual, independientemente de su registro o publicación.<sup>23</sup>

En diciembre de 2019, Brasil inició su proceso de adhesión al Convenio de Budapest, en calidad de observador.<sup>24</sup>

La autoridad reguladora de los delitos cibernéticos es el Ministerio de Justicia y Seguridad Pública.<sup>25</sup> De acuerdo con el artículo 10, inciso V de la Ley N° 13.844/2019, la Oficina de Seguridad Institucional de la Presidencia de la República se encarga de otros asuntos de seguridad cibernética.<sup>26</sup>

La Unidad de Lucha contra el Delito Cibernético (URCC) de la Policía Federal, con sede en Brasilia, es el principal organismo de aplicación de la ley encargado de la lucha contra el delito cibernético y, por lo tanto, desempeña un papel operacional fundamental en la persecución de los delincuentes cibernéticos tanto dentro como fuera de Brasil.<sup>27</sup>

Sobre la base de las entrevistas de seguimiento, los participantes consideraron que la capacidad de los fiscales y jueces para tramitar los casos de delitos cibernéticos y los casos en que se utilizan pruebas digitales era demasiado ad hoc y no estaba institucionalizada. Por ejemplo, no hay tribunales especiales para tratar los casos de ciberdelincuencia, ni formación especializada para los jueces en materia de ciberdelincuencia. Sin embargo, los jueces reciben capacitación como parte de la formación que se imparte a los fiscales federales.

Las autoridades de Brasil han reconocido la necesidad de mejorar los mecanismos de cooperación informal y formal, tanto a nivel nacional como transfronterizo, pero estos mecanismos siguen siendo ad hoc. En particular, los entrevistados mencionaron que la cooperación en la lucha contra el delito cibernético es un área con muchas dificultades, especialmente a nivel internacional.

Entre los diversos canales de cooperación internacional disponibles, el compromiso con INTERPOL, Ameripol y Europol se describieron como las vías más importantes para facilitar la cooperación transfronteriza y el intercambio de información.



# Estándares, organizaciones y tecnologías

El diseño, la adopción y la auditoría de las normas de seguridad cibernética varían considerablemente entre los sectores público y privado. En lo que respecta al sector público, existen normas estrictas que se han convertido en estándares desde 2001 y se aplican a la Administración Federal. Existe un sistema de auditoría y todos los organismos federales deben designar a una unidad para llevar a cabo la auditoría. Además, existe una oficina de controles generales que se encarga de diseñar normas y supervisar el progreso de todos los departamentos en la aplicación de esas normas. Con respecto al sector privado, los participantes dijeron que el ritmo de adopción varía según los sectores, siendo las empresas financieras y de comunicaciones electrónicas las precursoras en esta área. Ciertos sectores, como las comunicaciones electrónicas y las finanzas, tienen algunos requisitos de seguridad obligatorios; sin embargo, en la mayoría de los casos, la fuerza motriz de adhesión a las normas es la demanda del mercado y las necesidades de las empresas. La norma ISO 27001 es el marco más frecuentemente adoptado, considerándose también el marco de seguridad cibernética del Instituto Nacional de Normas y Tecnología (NIST). Con respecto a las normas de desarrollo y adquisición de programas informáticos, existen directrices específicas para el sector público, pero no está claro hasta qué punto esas directrices están relacionadas con la seguridad cibernética. Los participantes reconocieron la necesidad de que una autoridad relacionada con la seguridad establezca normas en todos los sectores (no sólo en la Administración Federal) y promueva la adhesión a esas normas.

Los participantes en el estudio señalaron que la infraestructura de Internet en Brasil es muy resistente. En Brasil existe una amplia gama de proveedores de servicios de Internet (ISP) públicos y privados, con distintos grados de calidad, servicios y precios. La Asociación Brasileña de Internet (Abranet) ha impuesto una reglamentación, pero no hemos podido entrevistar a personas del sector de telecomunicaciones en nuestro estudio. Basándonos en nuestra investigación documental, existen más de 25 Puntos de Intercambio de Internet (IXP), que son mantenidos por un proyecto global llamado IX.br. El número de IXP garantiza un entorno atractivo para la innovación y la conectividad a Internet, a la vez que aumenta la resistencia de la infraestructura de Internet.

La calidad del software varía significativamente en el sector público dependiendo de si las organizaciones forman parte de la Administración Federal o no. Hay un inventario de software seguro para la Administración Federal y las redes son monitoreadas en busca de malware. El parcheo de los programas informáticos obsoletos se realiza automáticamente y existen Indicadores Clave de Desempeño (KPI) para evaluar la eficacia de los mecanismos de parcheo. Los gobiernos estatales no disponen de un catálogo de programas informáticos seguros y la aplicación de parches no se realiza

de forma sistemática. En cuanto al sector privado, la calidad de los programas informáticos depende del tamaño de la organización, siendo más maduras las empresas del sector financiero y de las telecomunicaciones.

La adopción de controles técnicos de seguridad en Brasil varía según los sectores y las organizaciones. Los participantes señalaron que la adopción y aplicación de controles en los órganos gubernamentales está muy avanzada en la Administración Federal, pero en los gobiernos estatales es elemental y su promoción irregular debido a las restricciones financieras, las limitaciones en materia de recursos humanos y la falta de una estructura organizativa apropiada. Existe una estrategia para la implementación de controles en el Gobierno Federal que incluye un modelo detallado para evaluar la madurez de las organizaciones, pero el Gobierno Federal no tiene control sobre los estados y municipios. En el sector privado, se entiende que las organizaciones bien establecidas adoptan controles técnicos adecuados y adaptados a sus redes. Los controles de la segmentación de la red y los instrumentos de vigilancia son evidentes en este sector, así como el uso de sistemas de detección de intrusos (IDS) y otras herramientas de gestión de información y eventos de seguridad (SIEM). Algunas organizaciones establecieron un CERT para monitorear sus redes. Sin embargo, es motivo de especial preocupación el hecho de que las organizaciones del sector privado no están obligadas a compartir información sobre incidentes con el CERT.br y pueden no recibir información sobre amenazas.

Brasil ha establecido normas técnicas para la acreditación de las autoridades de certificación (AC) y las autoridades de registro (AR), y realiza auditorías para la entidad emisora de certificados raíz y sus proveedores de servicios. Los participantes observaron que existen requisitos muy estrictos tanto para las autoridades emisoras de certificados raíz (nivel 5) como para las autoridades de certificación manejan la infraestructura de clave pública (PKI). En el Gobierno Federal, la Agencia Brasileña de Inteligencia (ABIN) es el centro de acreditación para la codificación y proporciona normas específicas sobre la forma en que debe transmitirse la información clasificada, cómo se utiliza el protocolo de comunicación para información sensible (PGP) y la forma en que deben almacenarse y manejarse los datos. En cuanto al sector privado, se pueden hacer observaciones similares. La codificación se considera principalmente para los sistemas críticos, tanto para los datos en tránsito como para los datos en reposo. No pudimos obtener una imagen clara de si los proveedores de servicios web ofrecen conexiones Secure Shell (SSH) entre los servidores y los navegadores web.

Existe una amplia gama de productos informáticos de seguridad cibernética desarrollados internamente por el sector público, así como por empresas privadas, que también exportan estas tecnologías a otros países. Asimismo, hay menos dependencia de tecnologías extranjeras de seguridad cibernética. Según los participantes, la prevalencia de los piratas informáticos en Brasil ha dado lugar a una demanda cada vez mayor de productos de seguridad cibernética. Para cumplir con esta demanda, las empresas locales desarrollan y ofrecen soluciones y software de seguridad nacional. Un factor importante para el mercado nacional establecido es la falta de legislación para proteger la propiedad intelectual. Debido a la amenaza de robo de la propiedad intelectual las organizaciones extranjeras se muestran reacias a vender sus soluciones de software. El mercado de los seguros cibernéticos ofrece una gama de pólizas, cuya demanda por parte de las organizaciones está aumentando. Generalmente, las pólizas detallan las situaciones en las que el seguro es válido y, como nota positiva, especifican las normas con las que las organizaciones deben cumplir para ser asegurables.

Se estableció un marco de divulgación de la vulnerabilidad para el Gobierno Federal. Las organizaciones establecieron procesos formales para difundir información automáticamente y el CERT.br recibe esta información y presenta informes completos sobre cómo abordar los incidentes. Por el contrario, las organizaciones privadas están excluidas del intercambio de inteligencia de amenazas del Gobierno. Además, no están obligadas a informar acerca de los incidentes, por lo que tienden a ocultar cualquier problema que detecten. Dado que Brasil ha comenzado a privatizar partes fundamentales de la infraestructura nacional, los participantes instaron al Gobierno a que reconociera el importante papel que desempeñan las organizaciones privadas en la estrategia nacional de seguridad cibernética y les otorgue acceso a la información de inteligencia sobre amenazas. Existen varios medios para que los ciudadanos denuncien los incidentes, ya sea a través de la Policía Estatal o de los sitios web. En lo que respecta al sector financiero, los bancos en particular ofrecen canales de comunicación específicos para que los clientes denuncien el fraude en línea.



## Reflexiones adicionales

Este fue el estudio No. 23° de país, apoyado directamente por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC) en Oxford. El presente estudio tiene por objeto ayudar al Gobierno del Brasil a comprender la amplitud y profundidad de la capacidad de seguridad cibernética del país. En el presente informe se sugieren varias medidas concretas mediante las cuales la capacidad de seguridad cibernética de Brasil podría alcanzar un mayor grado de madurez y que podrían contribuir a fomentar la colaboración entre las organizaciones de propiedad privada y las organizaciones estatales que forman parte de la infraestructura crítica.



Revisión de capacidades de

# Ciberseguridad

República Federativa de Brasil

# INTRODUCCIÓN

Por invitación de la OEA, el GCSCC realizó un estudio sobre la capacidad de seguridad cibernética de Brasil. El objetivo del estudio fue permitir que Brasil determinara las esferas de capacidad en las que el Gobierno podría invertir estratégicamente, a fin de mejorar su posición nacional en materia de seguridad cibernética.

Durante los días 19 y 20 de marzo de 2018, las partes interesadas de los diferentes sectores participaron en un proceso de consulta de tres días. Además, llevamos a cabo entrevistas en una etapa posterior. Los datos recogidos en el 2018 se validaron por medio de un proceso similar realizado en marzo de 2019.

- **Entidades del sector público**

- Gabinete de Seguridad Institucional de la Presidencia (GSI)
- (CTIR Gov) Centro de Tratamiento y Respuesta a Incidentes Cibernéticos del Gobierno
- Ministerio de Defensa
- Agencia Brasileña de Inteligencia (ABIN)
- Agencia Nacional de Telecomunicaciones (ANATEL)
- Ministerio de Transporte, Puertos y Aviación Civil
- Ministerio de Hacienda
- Servicio Federal de Procesamiento de Datos (SERPRO)
- Compañía de Tecnología de la Información de la Seguridad Social (DATAPREV)
- Centro de Defensa Cibernética (CDCiber)
- Armada Brasileña
- Red Nacional de Investigación y Educación de Brasil (RNP)

- **Sector de la justicia penal**

- Policía Federal
- Ministerio Público

- **Sector financiero**

- Caixa Econômica Federal
- Propietarios de infraestructuras críticas
- Confederación Nacional de Industrias (CNI)
- Asociación Brasileña de Empresas de Tecnología de la Información y las Comunicaciones

• **Sector Privado**

- Opice Blum Advogados Associados (bufete de abogados)
- Bialer Falsetti Associados (bufete de abogados)
- IBM
- Estrategias de Asuntos Públicos Concordia
- Apura Cybersecurity Intelligence

## DIMENSIONES DE LA CAPACIDAD DE SEGURIDAD CIBERNÉTICA

Las consultas se basaron en el Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CCM, por sus siglas en inglés)<sup>28</sup> del Centro Global de Capacidad en Seguridad Cibernética (GCSCC), que incluye cinco dimensiones distintas de la capacidad de ciberseguridad.

Cada dimensión está compuesta por un número de factores que describen y definen lo que significa que cada factor cuente con capacidad de ciberseguridad. El cuadro siguiente presenta las cinco dimensiones, junto con los factores que las componen:

<b>Dimensión 1</b> <b>Política y Estrategia de Ciberseguridad</b>	<b>D1.1</b> Estrategia nacional de seguridad cibernética <b>D1.2</b> Repuesta a incidentes <b>D1.3</b> Protección de Infraestructura Crítica (IC) <b>D1.4</b> Gestión de Crisis <b>D1.5</b> Defensa Cibernética <b>D1.6</b> Redundancia de comunicaciones
--	--

<p>Dimensión 2 <b>Cultura cibernética y sociedad</b></p>	<p><b>D2.1</b> Mentalidad de Ciberseguridad</p> <p><b>D2.2</b> Confianza y seguridad en Internet</p> <p><b>D2.3</b> Comprensión del usuario de la protección de la información personal en línea</p> <p><b>D2.4</b> Mecanismos de información</p> <p><b>D2.5</b> Medios y redes sociales</p>
<p>Dimensión 3 <b>Educación, Capacitación y Habilidades en Seguridad Cibernética</b></p>	<p><b>D3.1</b> Sensibilización</p> <p><b>D3.2</b> Marco para la educación</p> <p><b>D3.3</b> Marco para la formación profesional</p>
<p>Dimensión 4 <b>Marcos jurídicos y regulatorios</b></p>	<p><b>D4.1</b> Marcos jurídicos</p> <p><b>D4.2</b> Sistema de justicia penal</p> <p><b>D4.3</b> Marcos de cooperación formal e informal para combatir el delito cibernético</p>
<p>Dimensión 5 <b>Estándares, organizaciones y tecnologías</b></p>	<p><b>D5.1</b> Adhesión a los estándares</p> <p><b>D5.2</b> Resiliencia de la infraestructura de Internet</p> <p><b>D5.3</b> Calidad del Software</p> <p><b>D5.4</b> Controles técnicos de seguridad</p> <p><b>D5.5</b> Controles criptográficos</p> <p><b>D5.6</b> Mercado de la ciberseguridad</p> <p><b>D5.7</b> Divulgación responsable</p>

# ETAPAS DE MADUREZ DE LA CAPACIDAD DE SEGURIDAD CIBERNÉTICA

Cada dimensión está compuesta por un número de factores que describen lo que significa poseer capacidad de seguridad cibernética. Cada factor presenta un número de aspectos y para cada aspecto hay indicadores que describen los pasos y acciones que, una vez observados, definen el estado de madurez del aspecto. Existen cinco etapas de madurez, que oscilan desde la etapa inicial hasta la etapa dinámica. La etapa inicial implica un enfoque ad hoc de la capacidad, mientras que la etapa dinámica representa un enfoque estratégico y la capacidad de adaptarse dinámicamente o de cambiar en respuesta a consideraciones ambientales. Las cinco etapas se definen a continuación:

- **Inicial:** en esta etapa no existe madurez en ciberseguridad, o bien se encuentra en un estado muy embrionario. Puede haber debates iniciales sobre la creación de capacidad en materia de seguridad cibernética, pero no se han adoptado medidas concretas. En esta etapa no hay pruebas observables de la capacidad en materia de seguridad cibernética;
- **Formativa:** algunos aspectos han comenzado a crecer y a ser formulados, pero pueden ser ad-hoc, desorganizados, mal definidos o simplemente nuevos. Sin embargo, la evidencia de este aspecto puede ser claramente demostrada.
- **Establecida:** los indicadores del aspecto están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero esta etapa es funcional y está definida.
- **Estratégica:** En esta etapa, se han tomado decisiones sobre qué indicadores del aspecto son importantes y cuáles son menos importantes para la organización o el Estado en particular. La etapa estratégica refleja el hecho de que estas elecciones se han realizado condicionadas por las circunstancias particulares del Estado o de las organizaciones, y
- **Dinámica:** En esta etapa existen mecanismos claros para modificar la estrategia en función de las circunstancias imperantes, como la sofisticación tecnológica del entorno de amenaza, el conflicto mundial o un cambio significativo en una esfera de interés (por ejemplo, el delito cibernético o la privacidad). Las organizaciones dinámicas han desarrollado métodos para modificar las estrategias cambiantes a la mitad del camino. La toma rápida de decisiones, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.

La asignación de las etapas de madurez se basa en las pruebas reunidas, incluida la visión general o media de las cuentas presentadas por los interesados, las investigaciones documentales realizadas y el juicio profesional del personal de investigación del GCSCC. Utilizando la metodología del GCSCC que se expone a continuación, en este estudio se presentan los resultados del examen de la capacidad de seguridad cibernética de Brasil y se concluye con recomendaciones sobre las próximas medidas que podrían considerarse para mejorar la capacidad del país en seguridad cibernética.

# METODOLOGÍA - MEDICIÓN DE LA MADUREZ

Durante el estudio en el país, se examinan las dimensiones específicas con los grupos de interesados pertinentes. Se espera que cada grupo de interesados responda a una o dos dimensiones del CMM, dependiendo de su experiencia. Por ejemplo, se invitaría al mundo académico, a la sociedad civil y a los grupos de gobernanza de Internet a debatir tanto la dimensión 2 como la dimensión 3 del CMM.

A fin de determinar el nivel de madurez, cada aspecto reúne un conjunto de indicadores correspondientes a las cinco etapas de madurez. Para que los interesados aporten pruebas sobre cuántos indicadores ha aplicado una nación y para determinar el nivel de madurez de cada aspecto del modelo, se utiliza un método de consenso para impulsar los debates en las sesiones. Durante los grupos de enfoque, los investigadores utilizan preguntas semiestructuradas para orientar las discusiones sobre los indicadores. Durante estas discusiones, los interesados deberían poder aportar o indicar pruebas relativas a la aplicación de los indicadores, a fin de reducir al mínimo las respuestas subjetivas. Si no se pueden proporcionar pruebas de todos los indicadores en una etapa, esa nación no ha alcanzado todavía esa etapa de madurez.

El Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM) utiliza la metodología de grupos de discusión ya que ofrece un conjunto de datos más rico en comparación con otros enfoques cualitativos.<sup>29</sup> Al igual que las entrevistas, los grupos de enfoque son una metodología interactiva con la ventaja de que durante el proceso de recopilación de datos e información pueden surgir diversos puntos de vista y planteamientos. Una parte fundamental del método consiste en que en lugar de formular preguntas a cada entrevistado el investigador o investigadores deben facilitar un debate entre los participantes, alentándolos a adoptar, defender o criticar diferentes perspectivas.<sup>30</sup> Esta interacción y tensión es lo que ofrece una ventaja sobre otras metodologías, ya que permite alcanzar un nivel de consenso entre los participantes y obtener una mejor comprensión de las prácticas y capacidades de seguridad cibernética.<sup>31</sup>

Con el consentimiento previo de los participantes, se graban y transcriben todas las sesiones. El análisis de contenido es una metodología de investigación sistemática que se utiliza para analizar datos cualitativos y se aplica a los datos generados por los grupos de discusión.<sup>32</sup> El propósito del análisis de contenido es diseñar “inferencias reproducibles y válidas de los textos al contexto de su uso”.<sup>33</sup>

Hay tres enfoques para el análisis del contenido. El primero es el enfoque inductivo, que se basa en la “codificación abierta”, lo que significa que el investigador crea libremente las categorías o temas. En la codificación abierta, los encabezamientos y las notas se escriben en las transcripciones mientras se leen y se crean diferentes categorías para incluir notas similares que capten el mismo aspecto del fenómeno que se estudia.<sup>34</sup> El proceso se repite y las notas y los encabezamientos se leen nuevamente. El siguiente paso es clasificar las categorías en grupos. El objetivo es fusionar las posibles categorías que comparten el mismo significado.<sup>35</sup> Dey explica que este proceso categoriza los datos como “que están hechos los unos para los otros”.<sup>36</sup>

El segundo enfoque es el “análisis de contenido deductivo”, que requiere la existencia previa de una teoría que sustente el proceso de clasificación. Este enfoque es más estructurado que el método



inductivo y la codificación inicial está conformada por las características y variables clave del marco teórico.

En el proceso de codificación, los extractos se atribuyen a categorías y los hallazgos son dictados por la teoría o por investigaciones previas. Sin embargo, pueden existir categorías novedosas que contradigan o enriquezcan una teoría específica. Por lo tanto, si se siguen estrictamente los enfoques deductivos, es posible que se descuiden estas categorías novedosas que ofrecen una perspectiva refinada. Esta es la razón por la que el equipo de investigación del GCSCC opta por un enfoque mixto en el análisis de nuestros datos, que es una combinación de enfoques deductivos e inductivos.

Después de realizar un estudio de país, los datos reunidos durante las consultas con los interesados y las notas tomadas durante las sesiones se utilizan para definir las etapas de madurez de cada factor del CMM. El GCSCC adopta un enfoque mixto para analizar los datos de los grupos focales y utiliza los indicadores del CMM como nuestro criterio para un análisis deductivo. Los extractos que no encajan en los temas se analizan más a fondo para identificar cuestiones adicionales que los participantes podrían haber planteado o para adaptar nuestras recomendaciones.

En algunos casos, mientras se redacta un informe, es necesario realizar una investigación documental para validar y verificar los resultados. Por ejemplo, es posible que los interesados no siempre estén al tanto de los acontecimientos recientes en su país, por ejemplo, si el país firmó una convención sobre la protección de los datos personales. Las fuentes que pueden suministrar más información pueden ser los sitios web oficiales del Gobierno o del ministerio, los informes anuales de las organizaciones internacionales, los sitios web de las universidades, etc.

Para cada dimensión se ofrecen recomendaciones sobre las próximas medidas que se deben adoptar para que el país aumente su capacidad. Si la capacidad de un país para un determinado aspecto se encuentra en una etapa de madurez formativa, entonces al observar el CMM se pueden identificar fácilmente los indicadores que ayudarán al país a pasar a la siguiente etapa. Las recomendaciones también podrían surgir a través de las conversaciones con las partes interesadas y las discusiones entre ellas.

Utilizando la metodología del Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones del Centro Global de Capacidad en Seguridad Cibernética (GCSCC) este informe presenta los resultados del estudio de la capacidad de ciberseguridad de Brasil realizado en marzo de 2018 y marzo de 2019. Los datos recogidos en 2019 y 2020 están marcados en azul. Cada sección del informe concluye con recomendaciones sobre las próximas medidas que podrían considerarse para mejorar la capacidad de seguridad cibernética del país. Las recomendaciones se revisaron y editaron ligeramente, teniendo en cuenta los resultados del taller de validación de 2019.



Revisión de capacidades de

# Ciberseguridad

República Federativa de Brasil

# CONTEXTO DE SEGURIDAD CIBERNÉTICA EN BRASIL

El porcentaje de personas que utilizan Internet en Brasil ha aumentado rápidamente en el último decenio. Específicamente, en 2017, el 67% de la población usaba Internet.<sup>37</sup>

Ese aumento ha llevado a Brasil a ocupar el sexagésimo sexto lugar en la clasificación del Índice Mundial de Desarrollo de las TIC de la Unión Internacional de Telecomunicaciones (UIT).<sup>38</sup> Además, según el informe del Foro Económico Mundial (2017-2018),<sup>39</sup> Brasil mejoró mucho en el desarrollo de la infraestructura de las TIC. Después de dos años de caída del crecimiento del PIB y de empeoramiento de las condiciones macroeconómicas, Brasil ha mejorado ligeramente este año, volviendo a controlar la inflación y el déficit gubernamental. El mayor progreso de Brasil se produce en el pilar de la innovación, con repuntes en muchos de los indicadores, que indican una mayor capacidad de innovación, mayor colaboración entre la industria, la universidad y la empresa, mayor calidad de la investigación, así como científicos e ingenieros mejor capacitados.

Brasil tiene una de las principales economías de América Latina, representando el 40 por ciento del PIB de América Latina.<sup>40</sup> Según el “Panorama del mercado digital: Brasil” del Gobierno de Su Majestad,<sup>41</sup> la ciberseguridad se está convirtiendo en uno de los mayores mercados en el ámbito de las TIC debido al aumento de las amenazas cibernéticas en el país.

Las inversiones en banda ancha son importantes, con el objetivo de proporcionar cobertura de banda ancha en el 95 por ciento de los municipios para 2018. También hay oportunidades de 4,5G y 5G con las empresas de telecomunicaciones.

Durante el decenio pasado, se observó en Brasil un importante aumento del acceso a Internet y de las suscripciones a teléfonos móviles, con más de la mitad de su población de 200 millones de personas en línea en 2018. Varios factores relacionados con las mejoras del desarrollo social y económico de Brasil están impulsando estas tendencias. No es sorprendente que el empoderamiento digital también vaya acompañado de desafíos adicionales que van desde las protestas masivas hasta el crimen organizado. La naturaleza compleja y multifacética de la “ciberamenaza”, y la forma en que se interpreta en Brasil, ha desempeñado un papel importante en la configuración de la cibergobernanza y la arquitectura de la ciberseguridad del país.<sup>42</sup>



# INFORME DEL ESTUDIO

# VISIÓN GENERAL

En esta sección ofrecemos una representación general de la capacidad de seguridad cibernética en Brasil. La Figura 2, a continuación, presenta las estimaciones de madurez en cada dimensión. Cada dimensión representa una quinta parte del gráfico, con las cinco etapas de madurez de cada factor extendiéndose hacia afuera desde el centro del gráfico; el “inicio” está más cerca del centro del gráfico y la “dinámica” está situada en el perímetro.

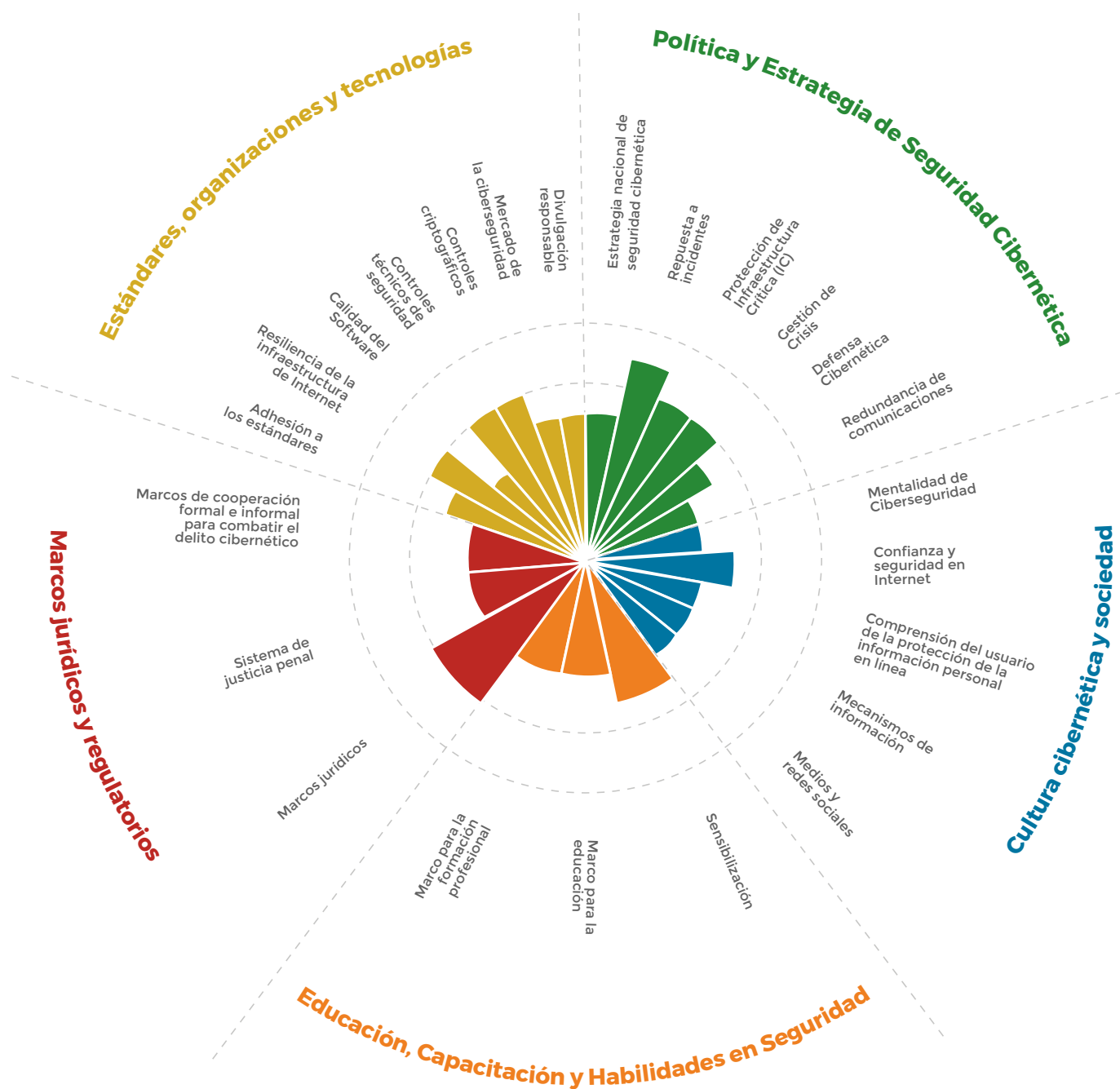


Figura 2: Representación general de la capacidad de seguridad cibernética en Brasil



Dimensión 1

# POLÍTICA Y ESTRATEGIA DE SEGURIDAD CIBERNÉTICA

Los factores de la dimensión 1 miden la capacidad de Brasil para elaborar y aplicar una política y una estrategia de seguridad cibernética y aumentar la resiliencia de la seguridad cibernética mediante mejoras en la respuesta a los incidentes, la gestión de las crisis, la redundancia y la capacidad de protección de las infraestructuras críticas. Esta dimensión también incluye consideraciones para la alerta temprana, la disuasión, la defensa y la recuperación. Se consideran algunas políticas eficaces para fomentar la capacidad nacional de ciberdefensa y resiliencia, al tiempo que se facilita el acceso efectivo al ciberespacio, lo cual es cada vez más importante para el gobierno, las empresas internacionales y la sociedad en general.

# D 1.1 - Estrategia Nacional de Seguridad Cibernética



*La estrategia de seguridad cibernética es esencial para incorporar un programa de seguridad cibernética en todo el gobierno, dado que ayuda a dar prioridad a la seguridad cibernética como una importante área normativa, determina las responsabilidades y los mandatos de los principales agentes gubernamentales y no gubernamentales de la seguridad cibernética, y dirige la asignación de recursos a los problemas y prioridades de seguridad cibernética nuevos y existentes.*

Stage: **Formative - Established**

En 2010 Brasil inició procesos para apoyar la elaboración de una estrategia de seguridad cibernética con el “Plano Brasil 2022”<sup>43</sup> [El Plan Brasil 2022], un documento en el que se detalla el plan estratégico para Brasil hasta 2022. La digitalización de la economía, la libertad de expresión en Internet y la protección del derecho de acceso público a Internet eran objetivos fundamentales del plan, cuyo éxito dependía de la elaboración de una estrategia de seguridad cibernética. El primer intento de estrategia fue el Libro Verde de Seguridad Cibernética en Brasil,<sup>44</sup> un documento aprobado por el Gobierno que proporciona orientación sobre cuestiones relacionadas con la seguridad cibernética para el Estado. La necesidad de una estrategia de seguridad cibernética también se puso de relieve en la Estrategia Nacional de Defensa del Ministerio de Defensa,<sup>45</sup> en la que se reconoce que el ciberespacio es un elemento fundamental de la función militar brasileña. A pesar de la importancia del ciberespacio, en la estrategia de defensa no se explicó en detalle cómo se puede integrar la seguridad cibernética en una estrategia nacional. La culminación de estas dos iniciativas fue la Estrategia,<sup>46</sup> un marco más amplio de planificación estratégica para el

Gobierno del Brasil. En el momento del estudio, en marzo de 2018, no existía ningún documento oficial sobre seguridad cibernética nacional, aprobado por el Congreso Nacional, en el que se detallara cómo establecer la coordinación entre los principales agentes gubernamentales y no gubernamentales de seguridad cibernética.

La falta de colaboración entre las instituciones gubernamentales y el sector privado, así como la “fragmentación de las respuestas”, se abordaron potencialmente con la Estrategia (2015-2018). El objetivo de la Estrategia fue proporcionar directrices estratégicas para la seguridad de la información y las comunicaciones, así como coordinar esa labor entre los diversos actores involucrados a fin de mitigar los riesgos a los que están expuestas las organizaciones y la sociedad.<sup>47</sup> En dicha Estrategia se establecieron los principios fundamentales que debían seguirse, objetivos estratégicos claros (tales como la educación del personal y la sensibilización sobre cuestiones de ciberseguridad, la institucionalización de las políticas de ciberseguridad, la investigación e innovación en materia de tecnologías de ciberseguridad y controles de seguridad estrictos para las partes interesadas en la



ciberdelincuencia), las medidas para lograr esos objetivos y las instituciones encargadas de aplicar esas medidas en plazos predeterminados. La estrategia se centró en la Administración Pública Federal (FPA) de Brasil, que abarca 29 Ministerios, 6.000 organismos públicos, más de 1.000.000 de empleados, 320 redes digitales y 12.000.000 de sitios web.<sup>48</sup> Los críticos de la estrategia destacaron la ausencia de una autoridad central para aplicar ese enfoque sistemático y de múltiples interesados.<sup>49</sup>

En el momento del estudio, en marzo de 2018, los participantes explicaron que la comunidad cibernética bajo el Ministerio de Defensa y Seguridad de la Información, era una entidad encargada de la seguridad cibernética en la Administración Pública Federal (FPA). Por lo tanto, se encargó a un grupo interministerial interno de más de 15 ministerios de la FPA, con la asistencia de un comité técnico compuesto por miembros del Gabinete de Seguridad Institucional, la redacción del documento de Estrategia. El documento se remitió a 98 organizaciones, entre ellas miembros del mundo académico, confederaciones nacionales, entidades del sector financiero, partes interesadas de la infraestructura crítica, empresas de ingeniería informática y proveedores privados de servicios de Internet. Como señalaron los participantes, hasta el momento se han celebrado más de 200 reuniones y eventos para seguir perfeccionando el documento antes de que se remitiera al Parlamento para su aprobación. Cabe señalar que en nuestro estudio no pudimos corroborar la participación de organizaciones privadas con personas que trabajan en el sector privado.

Sin embargo, los críticos señalaron la ausencia de organizaciones de la sociedad civil, de partes interesadas en Internet y del público en general en este grupo de múltiples partes interesadas. Durante nuestro estudio, los participantes destacaron además la ausencia de organizaciones del sector privado que deberían considerarse parte de la infraestructura crítica (IC) pero que, por el momento, están desatendidas por

la FPA. La rápida evolución de la gobernanza electrónica, las ciudades inteligentes y las soluciones innovadoras en materia de tecnología de la información y las comunicaciones en Brasil han sentado las bases para un debate y una colaboración fructíferos entre una amplia gama de interesados, tales como organizaciones de derechos civiles, sector privado y Gobierno. En la actualidad, el debate sobre las cuestiones relacionadas con la seguridad cibernética incluye funcionarios gubernamentales, las fuerzas armadas, las fuerzas del orden, un grupo de instituciones privadas, las entidades públicas de información y comunicación y un pequeño número de instituciones académicas. Los participantes sugirieron que la ampliación de la gama de partes interesadas que participan en la configuración de la estrategia nacional de seguridad cibernética, mediante la inclusión de la sociedad civil y las organizaciones privadas, tranquilizará a la comunidad en el sentido de que la estrategia ofrece un enfoque equilibrado de la seguridad cibernética y contribuirá a aliviar los temores de que no se mencionen y se protejan los derechos humanos y civiles.

En cuanto a la organización del programa de seguridad cibernética, los participantes expresaron su preferencia por un modelo descentralizado, en el que los sectores comerciales serán supervisados por los organismos de reglamentación existentes, con un organismo nacional de reciente creación para coordinar los esfuerzos. Los participantes sugirieron que el modelo propuesto se inspire en el enfoque de la Unión Europea, en el que la Agencia de Ciberseguridad de la Unión Europea (ENISA) desempeña el papel central en la unificación y coordinación de la labor entre los países. La opinión de los participantes se basó en la estructura actual del Brasil, donde existen múltiples estados autónomos, pero la FPA tiene la responsabilidad de los procesos críticos en todos los estados. Los participantes indicaron que el tamaño del país dificulta la coordinación entre los estados y que la clave del éxito de la estrategia es mejorar la colaboración entre todas las partes interesadas pertinentes de los sectores

público, federal y privado sin centralizar las responsabilidades e iniciativas.

Por último, la estrategia nacional de seguridad cibernética describe un marco genérico de medidas críticas para poner en prácticalos principales objetivos. Sin embargo, como explicaron los participantes, este marco otorga a las autoridades el mandato de diseñar acciones y detalla los plazos para los objetivos principales. Esto se debe a que la estrategia en sí misma debe ser concisa, votada por el Congreso y no se actualizará regularmente. Una estrategia más elaborada con acciones específicas requeriría una mayor coordinación política.

### **Resultados del proceso de validación llevado a cabo en marzo de 2019:**

Durante las entrevistas del grupo focal de validación de marzo de 2019, los participantes suministraron información a los investigadores de la Política Nacional de Seguridad de la Información (Política Nacional de Segurança da Informação) publicada en forma de decreto presidencial (N° 9.637) en diciembre de 2018.<sup>50</sup> La política sirvió de base para la Estrategia Nacional de Ciberseguridad que se publicó en 2020.<sup>51</sup> El esquema de la Estrategia Nacional de Seguridad Cibernética se elaboró en la Política Nacional de Seguridad de la Información.<sup>52</sup> Esta política prometía un proceso de redacción inclusivo que implicaba la participación de la multitud de interesados;<sup>53</sup> al parecer, ya se ha consultado al sector privado.

### **La información proporcionada por los gobiernos en 2020:**

Tras la validación de las entrevistas de los grupos de enfoque realizadas en marzo de 2019, se aprobó finalmente la Estrategia Nacional de Ciberseguridad (Decreto Federal N° 10.222) en febrero de 2020.<sup>54</sup> El Decreto “crea un modelo de gobernanza centralizado a nivel nacional para promover la coordinación entre los diferentes actores relacionados con la ciberseguridad, establecer un consejo nacional de ciberseguridad y fomentar los controles internos de cumplimiento de la seguridad cibernética en las entidades públicas y privadas”.<sup>55</sup> Además, “exige la notificación de los incidentes de seguridad cibernética contra infraestructuras críticas al Equipo de Respuesta a Incidentes de Seguridad Informática del Gobierno brasileño”.<sup>56</sup> Según las fuentes gubernamentales se centra en diez acciones estratégicas que deben guiar al FPA para crear sus propias acciones hacia la seguridad cibernética. Las novedades (desde 2018) con respecto a la estrategia de seguridad cibernética de Brasil indican una etapa de madurez de “formativa a establecida”.

Asimismo, se aclaró que, según el artículo 10 de la Ley N° 13.844 (junio de 2019), la coordinación y supervisión de la actividad de seguridad de la información en el ámbito de la FPA es responsabilidad de la Oficina de Seguridad Institucional de la Presidencia de la República,<sup>57</sup> mientras que las acciones de ciberdefensa son competencia del Ministerio de Defensa.

## D1.2 - Respuesta a Incidentes

Este factor se refiere a la capacidad del Gobierno de identificar y determinar las características de los incidentes a nivel nacional de manera sistemática. También examina la capacidad del Gobierno de organizar, coordinar y hacer operativa la respuesta a los incidentes.

### Etapa: Establecida - Estratégica

Hay una multitud de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), que incluyen desde entidades gubernamentales hasta el sector privado e instituciones académicas. La Figura 3: El número de CERT en Brasil muestra donde están ubicados geográficamente los CERT en Brasil. Según la función que desempeñe un CERT, esas entidades pueden participar exclusivamente en la gestión de la seguridad de los sistemas, hacer cumplir las directrices de seguridad cibernética o encargarse de coordinar la laborentre las autoridades nacionales y los niveles locales. Las iniciativas de servicios de Internet están coordinadas por el CGI.br y su rama ejecutiva, NIC.br. Estas dos autoridades supervisan las operaciones del CERT.br nacional, que está certificado por FIRST y se encarga de tramitar los informes de incidentes para el sector privado. Otra institución, CTIR Gov, también actúa como CSIRT a nivel nacional proporcionando respuesta a incidentes para la FPA, mientras que hay CERT dedicados a sectores específicos e interesados en la infraestructura crítica. Por último, existe un CERT militar que protege las redes militares.

Todas estas instituciones tienen directrices y funciones claras en cuanto a la respuesta a los incidentes y su madurez en este factor se encuentra en el nivel establecido, con la presencia de ciertos indicadores del nivel estratégico. El CERT.br mantiene el registro de incidentes nacionales y publica anualmente datos estadísticos de amenazas e incidentes.

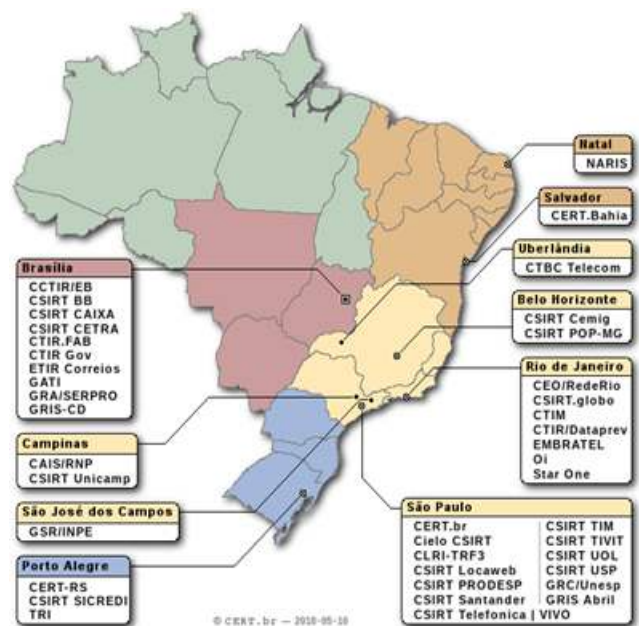


Figura 3: Número de CERT en Brasil<sup>58</sup>

Igualmente, el Gobierno del CTIR lleva a cabo las mismas actividades para la FPA y también proporciona alertas y recomendaciones en su sitio web (<https://www.ctir.gov.br/>). Los esquemas de clasificación utilizados para la gestión de incidentes se actualizan constantemente para captar los nuevos ataques y compartir los conocimientos obtenidos de esos ataques

de manera más eficiente. Además, todos los incidentes se incorporan automáticamente a una base de datos que es compatible con el software de inteligencia empresarial (BI). Como sugirieron los participantes, este software utiliza visualizaciones para permitir que los funcionarios de alto rango tengan acceso a la información pertinente “con un solo clic”. Los participantes mencionaron que, cuando se produce un incidente nacional, tanto el sector público como el privado participan en los procedimientos de respuesta. También hay apoyo de ABIN, que es la agencia de inteligencia, así como de la Policía Federal.

Todos los CERT proporcionan informes al CERT.br a través de canales oficiales. Los sistemas automatizados que siguen las normas internacionales, como la expresión estructurada de información sobre amenazas (STIX) y los Protocolos Semáforo (TLP, por sus siglas en inglés), garantizan que la información sobre amenazas se comparta con los CERT que colaboran con los CERT nacionales. Estos sistemas también facilitan las comunicaciones con los CERT internacionales. Sin embargo, los participantes mencionaron que, por razones burocráticas, se prefiere el uso del correo electrónico para los intercambios extraoficiales de información sobre amenazas con los socios internacionales. El CERT.br es miembro de la comunidad de FIRST y participa frecuentemente en eventos organizados por FIRST y la OEA.

A pesar de los sistemas automatizados existentes, los participantes sugirieron que el tiempo de respuesta para recibir la información, comprenderla y actuar en consecuencia podría mejorarse si los empleados del CERT asistieran a los eventos y colaboraran más estrechamente para fomentar la confianza. La labor actual en materia legislativa se centra en la racionalización del intercambio de información sobre amenazas entre todos los CERT, ya que no todos los interesados en la infraestructura crítica privada tienen derecho a recibir información sobre amenazas. Dado que la gama de interesados en la infraestructura crítica se está ampliando

y el intercambio de información fiable es más complejo, se necesita una mayor participación de las instituciones de investigación. Hay iniciativas destinadas a proporcionar a los CERT un mejor conocimiento de la situación, y con inteligencia artificial utilizada por diversos instrumentos para proporcionar conocimientos basados en la correlación de los acontecimientos.

En cuanto a los CERT públicos, cada uno de ellos debe crear un equipo técnico que se ocupe de los incidentes y que tenga instrucciones y políticas claras sobre cómo responder a las diferentes situaciones. También existen puntos de conducta establecidos y procedimientos específicos para preservar y almacenar pruebas. Existen sistemas innovadores para identificar las actividades de piratería informática, buscar conversaciones en la web oscura, prevenir los ataques de las páginas web y capturar, en tiempo real en los medios sociales, contenidos relevantes para los ataques en evolución. Por último, dos importantes proyectos financiados por el CERT nacional tienen por objeto aumentar la capacidad de detección de incidentes, la correlación de eventos y el análisis de tendencias (un proyecto de “honeypots distribuidos”), y obtener detalles de la actividad de envío de correos no solicitados (“SpamPots”). Para las necesidades de estos proyectos, el CERT.br ha establecido honeypots en más de 10 países y produce frecuentemente informes y publicaciones académicas con análisis de los datos.

SERPRO, una de las mayores empresas gubernamentales de servicios de tecnología de la información en Brasil, opera un CERT que ha institucionalizado los procedimientos de respuesta a incidentes. Estos procedimientos incluyen un equipo responsable de la coordinación a nivel de red, un equipo encargado de realizar pruebas de penetración y otro que realiza el refuerzo en la seguridad de la red. Existen laboratorios de última generación para el análisis de programas informáticos maliciosos y sistemas para sanear las redes, actuar de manera proactiva anticipándose a los acontecimientos y prevenir las vulnerabilidades. Además, existen procesos

internos de análisis de riesgos y modelos de madurez para indicar la eficacia con que se está manejando un incidente. SERPRO también mantiene una línea telefónica directa que conecta varios organismos gubernamentales. Además, existe un grupo de correo electrónico para las autoridades de la administración pública y un grupo de discusión donde se analizan los incidentes. Por último, la inteligencia sobre las actividades de hacking es recopilada por los expertos de SERPRO que se han infiltrado en los foros de hackers de todo el mundo.

En lo que respecta a la educación, existe una amplia gama de cursos ofrecidos por los CERT, así como varias campañas de sensibilización destinadas a informar a los ciudadanos. El CERT.br ofrece programas de formación profesional certificados por el CMU CERT, y metodologías propuestas por FIRST. También hay un portal para promover las mejores prácticas para los administradores de sistemas<sup>59</sup> y una guía sobre cómo los usuarios de Internet pueden protegerse en línea.<sup>60</sup> SERPRO también ofrece seminarios de mejores prácticas, cursos técnicos para analistas de CERT y celebra eventos semanales para educar a los usuarios sobre las amenazas contemporáneas y las noticias falsas.

### **Resultados del proceso de validación realizado en marzo de 2019:**

Brasil ha optado por una estructura descentralizada de la capacidad de respuesta a incidentes. El papel de coordinación entre los 42 CERT<sup>61</sup> de Brasil fue encomendado al CERT.br.<sup>62</sup> Este último también está encargado de coordinar las actividades internacionales de respuesta a incidentes.<sup>63</sup>

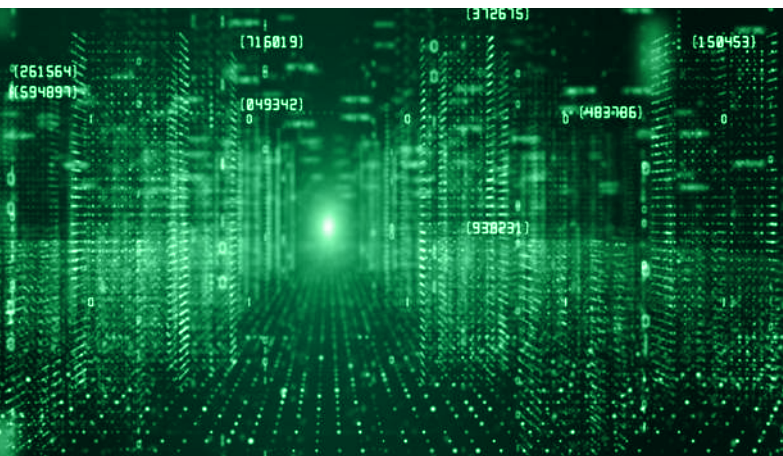
Además, CERT.br tiene la responsabilidad de fomentar la cooperación entre los integrantes de la red nacional de los CERT. En consecuencia, el CERT.br ayuda a los CERT recién establecidos a desarrollar su capacidad de manejo de incidentes mediante reuniones, capacitación y presentaciones en conferencias. También

organiza el Foro anual de los CSIRT (Fórum Brasileiro de CSIRT) y cursos especializados (por ejemplo, “Panorama general de la creación y gestión de los CSIRT”, “Fundamentos de la gestión de incidentes”, “Gestión avanzada de incidentes para el personal técnico”, etc.) en Brasil<sup>64</sup> y en el extranjero.<sup>65</sup> El compromiso internacional de CERT.br también incluye su asociación con el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon (CMI CERT) y el Grupo de Trabajo de Lucha contra el Phishing, así como su función de coordinador del proyecto SpamPots, que consiste en reunir y analizar datos sobre el uso indebido de la infraestructura de Internet por parte de los emisores de spam a partir de sensores de honeypot de baja interacción en 11 países.<sup>66</sup>

### **Información suministrada por el Gobierno en 2020:**

Luego de las entrevistas de validación del grupo de discusión, realizadas en marzo de 2019, se aclaró que Brasil cuenta con más de un CSIRT para sus operaciones nacionales: el CTIR Gov y el CERT.br. El CTIR Gov [Centro de Tratamiento y Respuesta a Incidentes Cibernéticos del Gobierno de Brasil] se encarga de coordinar las actividades relacionadas con la prevención, el manejo y la respuesta a los incidentes cibernéticos relacionados con los CSIRT de la Administración Pública Federal. Además, cada entidad de la Administración Pública Federal debe tener su propio CSIRT y su organismo de tecnologías de la información encargado de dicha interferencia. El CTIR Gov, al ser un CSIRT de responsabilidad nacional, también maneja las solicitudes de cooperación internacional en incidentes cibernéticos. Por otra parte, el CERT.br es un organismo certificado por FIRST [Foro de Equipos de Respuesta a Incidentes y Seguridad] y se hace cargo del sector privado. Cabe señalar que, debido al carácter colaborativo de la labor, en la práctica, los límites de competencia entre los CSIRT no son estrictos a fin de no poner en peligro la prevención, el tratamiento y la respuesta a los incidentes cibernéticos.

## D 1.3 - Protección De Infraestructura Crítica (Ic)



*Este factor estudia la capacidad del Gobierno para identificar los activos de infraestructura crítica y los riesgos asociados a ellos, participar en la planificación de la respuesta y la protección de los activos críticos, facilitar la interacción de calidad con los propietarios de los activos de infraestructura crítica y permitir una práctica general integral de gestión de riesgos, incluida la planificación de la respuesta.*

### Etapa: Establecida

La madurez de la capacidad de Brasil para proteger la infraestructura crítica varía entre los grupos de interés de infraestructura pública (IC) públicos y privados. Los participantes señalaron que para los segmentos de la infraestructura crítica que funcionan con fondos públicos, el Gabinete de Seguridad Institucional de la Presidencia (GSI), en colaboración con el Ministerio de Defensa, dispone de una lista detallada de los activos de IC y realiza auditorías con regularidad. En las evaluaciones de los riesgos se considera el impacto de los ataques a los bienes de la IC para la defensa nacional. Todas las instituciones federales deben realizar evaluaciones del riesgo cibernético, que se actualizan anualmente sobre la base de las lecciones aprendidas de los principales incidentes.<sup>67</sup> Se señaló que el sitio web del Departamento de Seguridad de la Información (DSI) de la GSI (<http://dsic.planalto.gov.br>) también reúne toda la legislación nacional relativa a la seguridad de la información. Entre las partes interesadas de la infraestructura crítica pública se incluyen empresas de telecomunicaciones, transporte, energía e instituciones financieras, todas las cuales cooperan y se coordinan a través de canales formales de comunicación con el Ministerio de Defensa. Existen políticas y procedimientos claramente definidos que todas

las instituciones públicas deben seguir sobre la base de la información proporcionada por el instrumento de conocimiento de la situación del CERT nacional. Se facilita el acceso a dicha información a la Policía Federal y a los servicios de inteligencia para aumentar la cooperación y el manejo de incidentes entre las partes interesadas de la IC. Todos los protocolos, procedimientos y evaluaciones de riesgos son evaluados anualmente por un grupo de trabajo de defensa cibernética. Este grupo, integrado por miembros de los jefes de información de nivel directivo, así como por miembros técnicos, determinó procesos sobre cómo incorporar las lecciones aprendidas para mejorar los protocolos y sistemas actualmente en vigor. Los participantes señalaron la contradicción de que las lecciones aprendidas se basan en incidentes importantes que ayudaron a perfeccionar considerablemente los protocolos actuales: la falta de un incidente importante en los últimos dos años ha obstaculizado el constante perfeccionamiento de esos protocolos.

Los participantes informaron que, por el momento, el sector privado no se considera parte de la infraestructura crítica del país. Dado que Brasil ha respaldado la privatización en sectores críticos como el financiero, es imperativo que se

vuelva a revisar la lista de las partes interesadas en la IC, para considerar las instituciones privadas. Las instituciones privadas no tienen ninguna obligación de informar al Gobierno sobre un incidente importante, se les restringe el acceso a la información de inteligencia sobre amenazas y no tienen en cuenta las evaluaciones de riesgos y los procesos que el Gobierno tiene en funcionamiento para los operadores públicos de infraestructura crítica. Por consiguiente, ellas deben elaborar sus propias evaluaciones de riesgo y políticas de seguridad internas, cuya eficacia dependerá de su grado de madurez. Las organizaciones bien establecidas tienen los recursos para desarrollar sus políticas internas de ciberseguridad, pero los participantes expresaron su preocupación por la capacidad de las PYMES y de la mayoría de las organizaciones del sector privado en general.

Un ejemplo característico de una parte interesada importante que se pasa por alto es el SERPRO [Servicio Federal de Procesamiento de Datos], que actualmente no se considera parte de la infraestructura crítica. Como señalaron los participantes, todas las evaluaciones de riesgos se realizan desde una perspectiva comercial y no tienen en cuenta las repercusiones en la defensa nacional. Hay indicadores y medidas internas para el manejo de incidentes de SERPRO que son corporativos o relacionados con sus clientes gubernamentales. Se proporcionan a los clientes informes de incidentes con contenido confidencial. Existen indicadores de desempeño que denotan la eficacia de los procesos, como el número de incidentes tratados, el número de incidentes categorizados y los tratados fuera del plazo aceptado. Cuando SERPRO decide que las amenazas actuales pueden afectar a la empresa y si existe la posibilidad de que ese incidente afecte a los servicios o activos del Gobierno, entonces hay políticas y directrices claras sobre la forma de elevar estos acontecimientos a las autoridades gubernamentales y a la Policía Federal. En 2010, SERPRO redactó un libro que detalla las estrategias y políticas de protección de infraestructura crítica, pero éstas no se siguen en la práctica. A pesar de que SERPRO

tiene procesos claros sobre cómo reportar incidentes y protocolos para tratar las situaciones y proporciona asistencia a las organizaciones privadas que deben considerarse como parte de la infraestructura crítica (como las instituciones financieras), los participantes enfatizaron que la seguridad de la información es como la higiene y no puede implementarse de manera aislada. Las infraestructuras públicas, aunque avanzadas en su madurez, se verán afectadas por ataques dirigidos a instituciones privadas más débiles. Por lo tanto, a pesar de las claras diferencias de competencia y capacidad cibernética entre el sector público y el privado, es importante que las instituciones mejoren su coordinación para aumentar la madurez del sector privado.

La mayoría de los participantes instaron al Gobierno a que creara un mecanismo para determinar el grado de madurez de la gobernanza de la tecnología de la información tanto en el sector público como en el privado, un protocolo de comunicación para distribuir alertas en los sectores público y privado, y una iniciativa para evaluar las normas y los estándares que poseen las organizaciones privadas y públicas. No obstante, se reconoció que estos aspectos podrían estar siendo abordados en la versión preliminar de la estrategia nacional. Se adoptaron medidas concretas para identificar los activos de la infraestructura crítica en el sector privado y crear canales oficiales de comunicación entre todas las partes interesadas de la infraestructura crítica. Por último, los participantes agradecerían la oportunidad de colaborar estrechamente con otros países e imponer la responsabilidad a los Gobiernos extranjeros por los daños que sus piratas informáticos causan a Brasil. Es por esta razón que los CERT brasileños se esfuerzan por determinar vulnerabilidades a nivel mundial. En nuestras discusiones de revisión se insistió en que el siguiente paso debería ser la cooperación más estrecha con la OEA, a través del establecimiento de una plataforma de información sobre amenazas entre los países de la OEA. El mayor obstáculo para contar con mayor información sobre amenazas entre los países es la falta de confianza

entre ellos. La revelación de las vulnerabilidades de las redes nacionales a otros países se convierte en información que podría ser objeto de medidas. Por lo tanto, es necesario acordar un protocolo de intercambio de información que no cree incomodidad a los países, a fin de fomentar confianza en la comunidad de la OEA.

### **Resultados del proceso de validación llevado a cabo en marzo de 2019:**

En noviembre de 2018, Brasil publicó su Política Nacional de Seguridad de Infraestructuras Críticas, la cual sienta las bases de la Estrategia Nacional de Infraestructuras Críticas y del Plan Nacional de Infraestructuras Críticas.<sup>68</sup> Los participantes en las entrevistas del grupo de debate sobre el estudio-validación del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM) de 2019 observaron que la presidencia de la federación estableció algunas prioridades dentro de la infraestructura nacional crítica en función de su vulnerabilidad e impacto, aunque esto no parece reflejarse en la documentación oficial. No obstante, se entiende que esos documentos, en los que se describe una orientación estratégica de ámbito nacional para la protección de las infraestructuras críticas, permitirán adoptar un enfoque más inclusivo y, por consiguiente, abordar las cuestiones relativas

a la exclusión de los operadores privados de infraestructuras críticas observada durante el análisis del CMM en 2018.

De hecho, ya se han observado algunos avances hacia el enfoque inclusivo de la protección de la infraestructura crítica. En los ejercicios de Cyber Guardian mencionados en la siguiente sección del presente informe, participaron no sólo el Gobierno y el ejército, sino también varios operadores privados de infraestructura crítica. Los participantes en las entrevistas de estudio y validación del CMM destacaron el “inmenso valor” de esas oportunidades de creación de redes entre el Gobierno y los operadores privados de infraestructura crítica.



## D 1.4 - Gestión de Crisis



*This factor addresses crisis management planning, addresses the conducting of specialised needs assessments, training exercises and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation as well as inform budgetary allocations.*

### Etapa: Establecida

Durante el último decenio, Brasil fue sede de una serie de importantes eventos, tales como los Juegos Panamericanos de 2007, la visita del Papa en 2013, la Copa Mundial de la FIFA en 2014 y los Juegos Olímpicos de 2016. La ciberseguridad fue un elemento crítico para la gestión de crisis durante dichos eventos y más de 40 organizaciones (con inclusión de Rio CERT, SERPRO, el CERT nacional y el CTIR Gov) se encargaron de manejar y mitigar los incidentes. El Centro de Ciberdefensa (CDCiber), una unidad encargada de coordinar los aspectos estratégicos y operativos de la arquitectura de ciberdefensa de Brasil, supervisó los procedimientos de gestión de crisis durante esos importantes eventos y estuvo a cargo de la coordinación con el Ministerio de Defensa y la Oficina de Seguridad Institucional de la Presidencia de la República (GSI, por sus siglas en portugués).

Como era de esperar, Brasil experimentó varios problemas de seguridad cibernética durante estos grandes eventos. Dos de los incidentes más significativos fueron los múltiples ataques DDOS que oscilaron entre 300 GB por segundo y 1 TB por segundo, así como un incidente de sabotaje

que destruyó el cable que proporcionaba el acceso a Internet a la red de la Copa Mundial de la FIFA. Todos los eventos se manejaron de manera eficiente y se logró el retorno a la actividad normal dentro del acuerdo de nivel de servicios aprobado. Los participantes explicaron que los procesos de manejo de incidentes durante estos eventos demostraron que las organizaciones críticas para la defensa cibernética son capaces de colaborar y mitigar eficazmente el efecto de esos ataques. Las organizaciones que participaron en la gestión de crisis tenían funciones claras, contaban con protocolos transparentes sobre la forma de difundir la información y cómo frenar la escalada del incidente, así como con orientaciones específicas sobre la forma de proteger los sistemas. Sin embargo, los procesos de gestión de crisis se adaptaron a esos eventos específicos.

Los participantes expresaron la opinión de que los grandes eventos obligaban a las organizaciones a cooperar y ayudaban a fomentar la confianza dentro de la comunidad de seguridad cibernética de Brasil. Como ejemplo de cómo la confianza es un elemento importante en el intercambio de

información sobre amenazas, los participantes mencionaron el ataque de “wannacry”, que tuvo un efecto mínimo en la mayoría de las organizaciones de Brasil. Esto se debió al hecho de que las organizaciones compartieron información con sus pares de confianza rápidamente, emitiendo alertas y proporcionando detalles sobre cómo responder que fueron considerados confiables y procesables por todos.

Durante el estudio se sugirió que la experiencia y las lecciones aprendidas a través de esos eventos deberían servir de base para la labor actual en materia de gestión de crisis. Es necesario diseñar protocolos de gestión de crisis y crear una red de organizaciones públicas y privadas para manejar eventos importantes. Se sugirió que la capacitación y los ejercicios de simulación de eventos de crisis eran la forma óptima de validar los protocolos de comunicación a fin de aumentar la conciencia sobre la seguridad cibernética y poner a prueba los procesos de manejo de incidentes. Con ese propósito, los participantes mencionaron el ejercicio Cyber Guardian, el cual utiliza la planificación de alto nivel para concebir escenarios y plataformas de simulación de operaciones cibernéticas que pueden emular los sistemas críticos de los sectores financiero, nuclear y público. Los ejercicios de situaciones de crisis se realizan con frecuencia y en ellos participan principalmente sistemas militares y gubernamentales. Estos ejercicios

también se combinan con simulaciones físicas. Los participantes mencionaron que pronto se llevará a cabo un ejercicio que incluirá al sector financiero y a los sistemas nucleares. Señalaron, además, que es necesario que un mayor número de organizaciones participen en estos ejercicios, incluida la sociedad civil.

### **Resultados del proceso de validación llevado a cabo en marzo de 2019:**

En 2019, el taller de validación confirmó en gran medida los resultados del informe del MMC de 2018.

## D1.5 - Defensa Cibernética



*Este factor explora si el Gobierno tiene la capacidad de diseñar e implementar una estrategia de defensa cibernética y dirigir su implementación, incluso a través de una organización de defensa cibernética específica. También se estudia el nivel de coordinación entre los diversos agentes de los sectores público y privado en respuesta a los ataques malintencionados contra los sistemas de información estratégica y la infraestructura crítica nacional.*

### Etapa: Formativa - Establecida

En cuanto a la gobernanza de la seguridad cibernética, el Gobierno del Brasil asignó el nivel político y estratégico a la Oficina de Seguridad Institucional de la Presidencia de la República (GSI) y los procedimientos estratégicos, operacionales y de ciberdefensa al Ministerio de Defensa. En los últimos años las fuerzas armadas se reestructuraron para adaptarse a las necesidades de un sistema democrático en evolución, centrándose en las nuevas amenazas transfronterizas y los acontecimientos de seguridad interna. Según fuentes secundarias, las fuerzas armadas son consideradas como la institución nacional de mayor confianza y se les ha encomendado la gestión de crisis para los grandes eventos civiles.<sup>69</sup> Por lo tanto, han adquirido financiación gubernamental para dirigir el desarrollo de las capacidades de ciberdefensa de la nación.

Un documento oficial de ciberdefensa publicado en 2012 establece directrices sobre políticas de ciberseguridad. El ejército opera un CERT y proporciona formación para gestión de riesgos y respuesta a incidentes. Hay una unidad dedicada que se especializa en la planificación y realización de operaciones cibernéticas.<sup>70</sup> La misma unidad se hace cargo de la coordinación con el Ministerio del Interior, así como con los servicios de inteligencia, la Policía Federal y el SERPRO, a través de canales de comunicación formales y bien establecidos.

Los participantes señalaron que el ejército posee capacidad tanto ofensiva como defensiva y

se enfocan en mejorarlas medidas defensivas. Indicaron que los militares despliegan sistemas que aportan un conocimiento de la situación y defienden proactivamente contra ataques (DDoS) y la desfiguración de la web. Existen laboratorios de análisis de programas informáticos maliciosos y un número importante de personal está recibiendo capacitación para ejecutar esas tareas. Existen algunas herramientas, tal como el Business Intelligence (BI) para facilitar la evaluación de los riesgos cibernéticos y analizar los resultados. Por último, hay ejercicios cibernéticos que se realizan con frecuencia y para el próximo evento los militares invitarán a organizaciones privadas a participar.

### Resultados del proceso de validación llevado a cabo en marzo de 2019:

En 2019 Brasil no contaba aún con una estrategia de ciberdefensa específica. Cuando se adopte una estrategia uno de los principales elementos de la Estrategia Nacional de Seguridad de la Información será la ciberdefensa.<sup>71</sup> El Ministerio de Defensa ya está redactando las directrices estratégicas para la ciberdefensa y, según se informa, las futuras consultas incluirán al sector privado. Las orientaciones estratégicas pertinentes están actualmente brevemente descritas en la Estrategia Nacional de Defensa (Estrategia Nacional De Defensa).<sup>72</sup>

## D 1.6 - Redundancia de Comunicaciones



*En este factor se examina la capacidad del Gobierno para identificar y mapear la redundancia digital y las comunicaciones redundantes entre las partes interesadas. La redundancia digital prevé un sistema de ciberseguridad en el que la duplicación y el fallo de cualquier componente está salvaguardado por una copia de seguridad adecuada. La mayoría de estos respaldos adoptarán la forma de redes digitales aisladas (de los sistemas de línea principal) pero fácilmente disponibles, pero algunos pueden ser no digitales (por ejemplo, respaldar una red de comunicación digital con una red de radiocomunicaciones).*

### Etapa: **Formativa**

No fue posible obtener una visión completa con respecto a la redundancia de comunicaciones en el curso del estudio del CMM. Los participantes señalaron que el sector público tiene activos de respuesta a emergencias conectados por cable a la red de comunicaciones de emergencia de la estrategia nacional. Se dispone de recursos apropiados para evaluar la redundancia de los protocolos actuales vigentes, para probar los sistemas redundantes, realizar ejercicios y llevar a cabo simulacros de comunicación. Existen múltiples centros de crisis designados en lugares geográficos dispersos para garantizar la participación de todos los interesados en el caso de una emergencia. En marcado contraste, el sector privado está descuidado y excluido de estos planes, con la excepción de un número pequeño de CERT privados.

Como explicaron los participantes, existen sistemas telefónicos seguros entre el CERT nacional y los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), y se siguen las normas internacionales para el uso del correo electrónico y otros métodos como procedimientos

de redundancia para la comunicación. Sin embargo, la ausencia del sector privado en la red de comunicaciones de emergencia sigue siendo problemática. Es importante obtener una imagen holística de la madurez de las partes interesadas de la infraestructura crítica privada que apoyan los procesos críticos de las redes de comunicación nacionales. Es necesario promulgar leyes sobre los requisitos para que los proveedores de servicios de internet (ISP) dispongan de activos redundantes de respuesta a emergencias y realicen con frecuencia pruebas de capacidad para comprobar la disponibilidad de la red.

### **Resultados del proceso de validación llevado a cabo en marzo de 2019:**

Desde 2018, la situación en Brasil no ha cambiado de manera drástica. Según un participante del taller de revisión-validación del CMM de 2019, "Brasil todavía necesita hacer más para establecer medidas adecuadas de redundancia de comunicaciones".

# Recomendaciones

A raíz de la información presentada durante el estudio de la madurez de la política y la estrategia de seguridad cibernética, el Centro Global de Capacidad en Seguridad Cibernética (GCSCC) formuló el siguiente conjunto de recomendaciones para su consideración por el Gobierno del Brasil. Estas recomendaciones proporcionan asesoramiento y medidas destinadas a aumentar la capacidad de la seguridad cibernética existente, de acuerdo con las consideraciones del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones del Centro. Las recomendaciones se proporcionan específicamente para cada factor.

## ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA

### R1.1

Diseñar un documento complementario a la estrategia que se ajuste a los objetivos nacionales y a las prioridades de riesgo, a fin de aportar directrices factibles con la correspondiente métrica para supervisar el avance de la aplicación de la estrategia;

### R1.2

garantizar que entre las partes interesadas que participan en la formulación de la estrategia nacional de seguridad cibernética figuren organizaciones del sector privado que deberían formar parte de la infraestructura crítica (especialmente finanzas, energía, telecomunicaciones, transporte, SERPRO, Empresa de Tecnología e Informações da Previdência Social (Dataprev), PYMES), la sociedad civil, el mundo académico y los socios internacionales;

### R1.3

mejorar la colaboración con la OEA y desarrollar una taxonomía común para la seguridad cibernética; y

### R1.4

garantizar que los estándares de seguridad de la información elaborados por la Administración Pública Federal constituyan los estándares mínimos a ser adoptados por las autoridades públicas estatales y que su aplicación se incluya en los programas de la estrategia nacional de seguridad cibernética.

## Respuesta a incidentes

### R1.5

Establecer una base de datos central de materia de inteligencia de incidentes a nivel nacional que incluya información sobre incidentes de todos los sectores. Asignar a los CERT para cada sector crítico (es decir, finanzas, telecomunicaciones, gobierno, ejército, petróleo y gas, etc.) con la responsabilidad de difundir información adaptada a las necesidades del sector correspondiente;

### R1.6

identificar las organizaciones del sector privado que son de importancia clave para la ciberseguridad nacional y proporcionarles acceso a la información compartida por el CERT nacional;

### R1.7

Obtener un consenso entre las partes interesadas (especialmente del sector privado) sobre la arquitectura, las interfaces y las normas para el intercambio de información. Las normas comunes

promovidas, por ejemplo, por la UE y los EE.UU., son STIX y TAXII. Entre las partes interesadas deberían figurar los sectores público y privado, así como la comunidad de seguridad cibernética en los planos nacional, regional e internacional;

#### **R1.8**

establecer parámetros para monitorear y evaluar la efectividad de todos los CERT. Además, mejorar la colaboración entre la OEA, los CERT regionales y otros organismos internacionales;

#### **R1.9**

establecer capacitación en forma regular para los empleados de todos los CERT y diseñar parámetros para evaluar los resultados de dicha capacitación. Los cursos ofrecidos por el CERT nacional, el CERT militar y el SERPRO pueden servir de base para el entrenamiento de los demás CERT.

#### **R1.10**

determinar y documentar los procesos clave de respuesta a los incidentes destacando cuándo y cómo deben participar los diferentes ministerios, el gobierno estatal y las organizaciones privadas.

### **Protección de infraestructura crítica**

#### **R1.11**

Desarrollar y llevar a cabo una evaluación nacional de riesgos con el objetivo de identificar a las partes interesadas de la infraestructura crítica, así como las amenazas nacionales, con especial atención a las organizaciones del sector privado;

#### **R1.12**

Elaborar y difundir una lista de activos de infraestructura crítica con prioridades determinadas en función de los riesgos, que incluya activos del sector privado;

#### **R1.13**

establecer un mecanismo para la divulgación periódica de la vulnerabilidad y el intercambio de información entre los propietarios de activos de infraestructura crítica privados y públicos y el Gobierno. Establecer un diálogo regular entre los niveles táctico, ejecutivo y estratégico en relación con las prácticas de riesgo cibernético y fomentar la comunicación entre los operadores de la infraestructura crítica;

#### **R1.14**

Identificar las estrategias de comunicación interna y externa de la infraestructura crítica con puntos de contacto claros que incluyan al sector privado;

#### **R1.15**

establecer procedimientos y procesos de protección de la información y de gestión de riesgos dentro de la infraestructura crítica, apoyados por soluciones técnicas de seguridad adecuadas, que sirvan de base para la elaboración de un plan de respuesta a incidentes cibernéticos;

#### **R1.16**

establecer procedimientos comunes para medir y evaluar la capacidad de los propietarios de los activos de la infraestructura crítica para detectar, identificar, responder y recuperarse de las amenazas cibernéticas;

### **R 1.17**

ordenar el diseño y la aplicación de evaluaciones periódicas apropiadas de los riesgos cibernéticos para todas las partes interesadas de la infraestructura crítica y determinar la información que debe compartirse. Diseñar evaluaciones de riesgo cibernético para todas las partes interesadas de la infraestructura crítica, basadas en el enfoque de evaluación de riesgos nacionales, y

### **R 1.18**

encargar a los reguladores de cada sector que ordenen la divulgación de los incidentes. Fijar umbrales para la divulgación de incidentes tras consultar con organizaciones públicas y privadas de los respectivos sectores.

## **Gestión en crisis**

### **R 1.19**

Un escenario realista de crisis de alto nivel debería servir de base a un plan para poner a prueba las corrientes de información, la adopción de decisiones y la inversión de recursos a nivel nacional;

### **R 1.20**

desarrollar objetivos específicos, medibles, alcanzables, pertinentes y de duración determinada (SMART) e indicadores clave de desempeño (PKI) para orientar las decisiones en la gestión de crisis;

### **R 1.21**

garantizar que los resultados de la evaluación de los dos ejercicios anteriores del Cyber Guardian sirvan de base para la inversión futura en la capacidad nacional en materia de ciberseguridad y que las conclusiones se evalúen en relación con las buenas prácticas internacionales de gestión de crisis; y

### **R 1.22**

deben prepararse informes específicos para cada sector sobre los ejercicios de gestión de crisis para cada parte interesada.

## **Defensa cibernética**

### **R 1.23**

Asegurar que se desarrolle un componente de defensa cibernética en la estrategia de seguridad nacional. Este componente debería tener en cuenta las amenazas a la seguridad nacional que podrían surgir del espacio cibernético;

### **R 1.24**

evaluar y determinar los requisitos de capacidad de defensa cibernética y hacer participar a las partes interesadas de los sectores público y privado. Realizar estudios continuos de la evolución del panorama de las amenazas a la seguridad cibernética para garantizar que las políticas de defensa cibernética sigan cumpliendo los objetivos de seguridad nacional; y

### **R 1.25**

diseñar ejercicios cibernéticos nacionales en los que participarán diversas organizaciones del sector privado.

## Redundancia de comunicaciones

### R 1.26

Poner a prueba la interoperabilidad y la función de los activos de respuesta a emergencias en situaciones de comunicaciones comprometidas para fundamentar la inversión estratégica en futuros activos de respuesta a emergencias. Asegurarse de que el sector privado sea considerado como una parte interesada clave en el plan de respuesta de emergencia;

### R 1.27

establecer un proceso, en el que participen todas las partes interesadas pertinentes, para determinar las lagunas y superposiciones en las comunicaciones de los activos de respuesta a emergencias las responsabilidades de las autoridades;

### R 1.28

conectar todos los activos de respuesta a emergencias a una red nacional de comunicaciones de emergencia con sistemas de respaldo aislados pero accesibles en situaciones de emergencia;

### R 1.29

establecer canales de comunicación entre las funciones de respuesta a emergencias, las áreas geográficas de responsabilidad, los gestores públicos y privados encargados de responder y las autoridades de mando. Crear actividades de divulgación y educación para protocolos de comunicación redundantes adaptados a las funciones y responsabilidades de cada organización en el plan de respuesta a la emergencia; y

### R 1.30

incluir elementos cibernéticos en los ejercicios de emergencia y crisis existentes y establecer procesos de medición para evaluar el éxito del ejercicio. Evaluar los ejercicios e incorporar los resultados en el proceso de toma de decisiones.





## Dimensión 2

# CULTURA CIBERNÉTICA Y SOCIEDAD

Las estrategias y políticas de seguridad cibernética con visión de futuro implican una amplia gama de actores, incluidos los usuarios de Internet. Con el auge de Internet, la seguridad cibernética ya no se deja en manos de los expertos que se encargaban oficialmente de aplicarla. Todos aquellos que participan en Internet y en tecnologías relacionadas, como las redes sociales, deben comprender el papel que pueden desempeñar para salvaguardar los datos sensibles y personales al utilizar los medios y recursos digitales. Esta dimensión subraya el papel central de los usuarios en el logro de la ciberseguridad, pero trata de evitar las tendencias convencionales de culpar a los usuarios por los problemas de la ciberseguridad. En cambio, un aspecto importante de la cultura y la sociedad de la seguridad cibernética es la conciencia de los expertos en seguridad cibernética de que deben crear sistemas y programas para los usuarios, sistemas que puedan utilizarse fácilmente y puedan incorporarse a las prácticas cotidianas en línea.

En esta dimensión se estudian elementos importantes de una cultura y una sociedad responsables en materia de seguridad cibernética, como la comprensión de los riesgos relacionados con la delincuencia cibernética por parte de todos aquellos involucrados, el desarrollo de un nivel aprendido de confianza en los servicios de Internet, el gobierno electrónico y los servicios de comercio electrónico, y la comprensión por parte de los usuarios de cómo proteger la información personal en línea. Esta dimensión también entraña la existencia de mecanismos de rendición de cuentas, como los canales para que los usuarios informen acerca de las amenazas a la seguridad cibernética. Además, esta dimensión examina el papel de los medios de comunicación y los medios sociales para ayudar a dar forma a los valores, las actitudes y el comportamiento de la ciberseguridad.

## D 2.1 - Mentalidad de Ciberseguridad



*Este factor evalúa el grado en que se da prioridad a la seguridad cibernética y se la incorpora a los valores, actitudes y prácticas gubernamentales, el sector privado y los usuarios de toda la sociedad en general. Una mentalidad de seguridad cibernética consiste en valores, actitudes y prácticas, incluidos los hábitos, de los usuarios individuales, los expertos y otros agentes del ecosistema de seguridad cibernética que aumentan la resistencia de los usuarios a las amenazas de su seguridad en línea.*

### Etapa: **Formativa**

El Gobierno ha reconocido la necesidad de dar prioridad a la seguridad cibernética en todas sus instituciones. Asimismo, se han diseñado aspectos de los procesos gubernamentales y las estructuras institucionales en respuesta a los riesgos de la seguridad cibernética, pero se encuentran principalmente alojadas en organismos particulares destacados.

En general, los participantes señalaron que la cultura de seguridad en Brasil varía en las distintas partes del país y en los diferentes sectores del Gobierno, las empresas y la industria. Todos los ministerios cuentan con empleados certificados por el CISSP [Profesional Certificado en Seguridad de Sistemas de Información] y, además, existen organismos que se ocupan de las necesidades de gestión de las TIC y establecen requisitos relativos a los programas informáticos.

La Oficina del Presidente de la República tiene su propia oficina de tecnología de la información que proporciona todo, desde software hasta computadoras personales, por lo que el apoyo administrativo está centralizado. Como mencionaron los participantes, en el Gobierno federal se asignan recursos para la capacitación de los empleados que se ocupan de las cuestiones de seguridad para las actividades de cumplimiento de la ley ISACA y de marcos, tal como la norma ISO 270001, y para el cumplimiento de las

prácticas óptimas relacionadas con la seguridad de la información que fueron determinadas por el Gobierno. Además, se está aplicando un sistema de auditoría dentro del gobierno federal. Todos los organismos tienen un departamento que se encarga de la auditoría. En 2017 se llevó a cabo un programa de visitas de auditoría para evaluar el nivel de madurez en 40 organismos diferentes.

Los participantes se mostraron preocupados por la complejidad de la estructura gubernamental de Brasil. Como se evalúa actualmente la madurez del sector público, se reconoce que habrá diversas etapas de madurez dentro de los distintos departamentos y entre los mismos. Sin embargo, el control y la influencia del Gobierno federal sobre los gobiernos estatales y los municipios es limitada.

Otra preocupación planteada por los participantes es la falta de un mecanismo de coordinación para identificar y abordar insuficiencias de madurez en el Gobierno. Como se ha señalado falta un protocolo de distribución de alertas, similar a los utilizados por un CERT y también se necesita un canal de comunicación integrado para evaluar las normas y los estándares que se están siguiendo.

La DSI es el Departamento de Seguridad de la Información y puede administrar la seguridad de la información para el sector público en general. Sin

embargo, hay departamentos gubernamentales independientes y conjuntos de directrices independientes. Como ejemplos, los participantes mencionaron, entre otros, el Servicio Federal de Procesamiento de Datos y el SERPRO,<sup>73</sup> que es una dependencia de la administración pública encargada de prestar servicios de tecnología de la información al Ministerio de Hacienda. Los reglamentos y normas son obligatorios para SERPRO porque pertenece al Gobierno. Sin embargo, los organismos estatales no están obligados a cumplir esas normas, lo cual crea la necesidad de que el Gobierno federal convenza a los organismos estatales y locales de que adopten iniciativas de seguridad cibernética.

Las principales empresas del sector privado han comenzado a dar mayor prioridad a la mentalidad de seguridad cibernética, determinando prácticas de alto riesgo. Los participantes observaron que entre los obstáculos que se oponen al desarrollo de una esfera digital figuran el alto costo de la aplicación y la falta de claridad con respecto a la recuperación de la inversión, así como la falta de normas y reglamentos bien entendidos, la falta de normas técnicas y la necesidad de educación y capacitación en esta área.

Los sectores financieros y de tecnología de la información están relativamente más avanzados en materia de seguridad cibernética, debido a que son objetivos ataques frecuentes. Por consiguiente, invierten más en seguridad cibernética y podrían mostrar a otros organismos cómo adoptar prácticas más seguras. Los participantes nos informaron que, desde que los bancos nacionales han empezado a adoptar medidas de seguridad proactivas, los delincuentes cibernéticos se han centrado cada vez más en los bancos regionales y en las PYME. Un número limitado pero cada vez mayor de usuarios de Internet ha comenzado a dar mayor prioridad a la seguridad cibernética, tomando conciencia de los riesgos y amenazas. La sociedad en su conjunto todavía carece de una mentalidad de ciberseguridad. Es posible que los usuarios de Internet estén cada vez más conscientes de

los riesgos de la seguridad cibernética, pero rara vez actúan de manera consecuente en sus prácticas cotidianas. Se mencionó que es común, incluso para los expertos en tecnología de la información, que son conscientes de los riesgos, hacer clic en los correos electrónicos de phishing o compartir información sensible en sitios de medios sociales como Facebook. Además, en los distritos de bajos ingresos, los ciudadanos tienden a depender del uso de teléfonos móviles para conectarse a Internet, a pesar de que el Gobierno les proporciona satélites para la conexión a Internet. La sensibilización sobre los riesgos es una necesidad importante para estas comunidades.

En general, los participantes destacaron la necesidad de una mayor sensibilización y educación a todos los niveles y en todos los sectores.

### **Resultados del proceso de validación llevado a cabo en marzo de 2019:**

En 2019 los entrevistados señalaron que se habían producido algunos avances en la madurez de la mentalidad de la seguridad cibernética durante el último año. A pesar de ello, algunos sostuvieron que persisten problemas con el phishing y otros incidentes cibernéticos similares, lo que indica que las buenas prácticas de seguridad cibernética no son ampliamente utilizadas por los funcionarios gubernamentales.

Los representantes del sector privado informaron de que el principal problema de sus empleados es la falta de conocimiento de la seguridad cibernética, especialmente en relación con la protección de los datos personales. “La gente comparte todo en línea”, escucharon los investigadores durante una de las entrevistas del grupo en marzo de 2019. No obstante, la mentalidad de seguridad cibernética en el sector privado sigue aumentando y existe un número cada vez mayor de empresas consideran que una mentalidad de seguridad cibernética es una prioridad.

Se pueden hacer observaciones similares sobre la mentalidad de seguridad cibernética de los usuarios de Internet. Aunque la mentalidad de la sociedad brasileña en materia de seguridad cibernética sigue siendo limitada y la gente suele hacer caso omiso de las buenas prácticas, especialmente cuando se trata de compartir contenidos personales en línea, algunas fuentes secundarias indican que una proporción limitada de usuarios de Internet da prioridad a la seguridad cibernética en su vida cotidiana. Por ejemplo,

casi la mitad de los usuarios de Internet de Brasil evitan hacer clic en los enlaces no solicitados de los mensajes y más de un tercio de ellos utilizan los parámetros de privacidad que ofrecen diversas plataformas en línea. Además, casi la mitad de los usuarios brasileños de Internet utilizan software antivirus, aunque sólo una cuarta parte de ellos cambia sus contraseñas con regularidad.<sup>74</sup>

## D 2.2 - Confianza y Seguridad en Internet



*Este factor estudia el nivel de confianza de los usuarios en la utilización de los servicios en línea en general, y de los servicios de gobierno electrónico y de comercio electrónico en particular.*

### Etapa: Formativa - Establecida

En general, las partes interesadas participantes creen que una pequeña proporción de los usuarios de Internet evalúa críticamente lo que ve o recibe en línea. Del mismo modo, pocos creen que tienen las aptitudes necesarias para utilizar el Internet y protegerse en línea. Además, un limitado número de usuarios confía en la seguridad de Internet y no conoce las formas de determinar la legitimidad de un sitio web.

Los servicios de gobierno electrónico se han desarrollando y una proporción cada vez mayor de usuarios confía en el uso seguro de dichos servicios. Sin embargo, se están identificando, reconociendo y divulgando las posibles infracciones en los servicios de gobierno electrónico de una manera ad hoc.

Actualmente, el gobierno brasileño ofrece varios servicios gubernamentales a los ciudadanos. Entre los principales se encuentran<sup>75</sup>:

- Ingresos Federales - servicios para la recaudación del impuesto sobre la renta, la situación fiscal del contribuyente, el registro del Catastro de Pessoas Físicas (CPF) y el Catastro Nacional da Pessoa Jurídica (CNPJ), el registro y las declaraciones, entre otros;
- Policía Federal - servicios tales como solicitudes de pasaporte, declaraciones de antecedentes penales, apoyo a las adopciones internacionales, entre otros;
- Sistema Integrado de Administración Financiera del Gobierno Federal (SIAFI) - intereses vinculados al Tesoro Nacional, como la provisión del gasto público;
- Poupa Tempo (Estado de São Paulo) - acceso a la información sobre los servicios públicos, como la solicitud de documentos y el inicio y cierre de negocios;

- Proyecto OntoJuris - suministro de información sobre la legislación en el ámbito de los derechos de propiedad intelectual, los derechos de los consumidores y el derecho electrónico, y
- Sistema Público de Contabilidad Digital (SPED) - presenta la promoción de la presentación de información tributaria, la racionalización y la estandarización de las obligaciones accesorias de los contribuyentes.

Desde 1998 se dispone de servicios como los de envío de declaraciones de impuestos sobre la renta, información sobre la seguridad social y las adquisiciones gubernamentales a través de Internet, pero se trata en gran medida de suministro de información frente a la prestación de servicios. En el año 2000 se definió e instituyó la Política de Gobierno Electrónico y se puso en marcha el Programa de la Sociedad de la Información, con lo que se consolidaron y difundieron las estrategias de gobierno electrónico, la importancia social de la inclusión digital, así como las acciones relacionadas con la tecnología de la información en el país, como la creación de directrices y estructuras jurídicas en el país para los servicios de gobierno electrónico (Scartezini, 2004).

Una proporción cada vez mayor de usuarios confía en el uso seguro de los servicios de comercio electrónico. El Ministerio de Justicia es una secretaría que se centra en los derechos del consumidor y el comercio electrónico. La legislación brasileña incluye disposiciones sobre el comercio electrónico (Código de Protección al Consumidor - Ley N° 8.078/1990, el Decreto N° 8.771/2016, que regula el Marco de Derechos Civiles del Brasil y la Ley del Marco de Derechos Civiles del Brasil para la Internet o Ley de Internet (Ley N° 12.965/2012 - Ley del Marco Civil de la Internet N° 12.965/2012), véase D 4.1). Por lo tanto, dentro de esta área, las tasas impositivas más altas sobre el comercio electrónico no son para el comercio nacional sino para el comercio transfronterizo.

En general, se alienta a las empresas a prestar servicios en línea. El servicio de comercio

electrónico está creciendo y ha aumentado desde 2017, cuando Brasil (la Policía Federal Brasileña) y la Europol firmaron un acuerdo estratégico para aumentar la cooperación en la lucha contra las actividades delictivas transfronterizas, que podría considerarse una cooperación oficial. Las empresas tienden cada vez más a invertir en servicios de comercio electrónico plenamente establecidos. Las soluciones de seguridad se actualizaron y se pusieron a disposición sistemas de pago fiables. Sin embargo, los participantes indicaron que aún quedan problemas por resolver en lo que respecta a la seguridad cibernética y la protección de los datos de los usuarios; por ejemplo, en lo que respecta a la fuga de datos de tarjetas de crédito a causa de los ataques cibernéticos.

El sector bancario organiza campañas de sensibilización y proporciona información en línea a los usuarios sobre su seguridad. Por ejemplo, el Banco do Brazil<sup>76</sup> y el Banco Itaú<sup>77</sup> dan consejos de seguridad para sus clientes. Aunque se están haciendo inversiones en servicios de comercio electrónico y los participantes creen que habrá un aumento en el uso de los servicios de comercio electrónico, se percibe que los piratas informáticos están llevando a cabo sus propósitos.

### **Resultados del proceso de validación llevado a cabo en marzo de 2019:**

En mayo de 2018, el Gobierno publicó la versión revisada de la Estrategia de Gobernanza Digital: Transformación digital - Ciudadanía y gobierno,<sup>78</sup> que, entre otras cosas, cubre asuntos de seguridad cibernética en el contexto de los servicios de gobierno electrónico. La estrategia incluye varios principios de gobernanza digital aplicables (la ciberseguridad es uno de ellos) que son promovidos por diversas entidades gubernamentales e incluso tiene una página web dedicada al tema.<sup>79</sup> Es probable que la promoción de los principios haya contribuido a que, según la investigación de 2018 de la OCDE, el 94% de las organizaciones del sector público conozcan la Estrategia de Gobernanza Digital.<sup>80</sup>

Tanto los usuarios como el Gobierno son conscientes de la importancia de los servicios


seguros de gobierno electrónico.<sup>81</sup> La identificación, el anuncio y el análisis de las infracciones están comprendidos en el mandato del Equipo de respuesta del gobierno brasileño para incidentes de seguridad informática (CTIR Gov) y se pueden consultar en línea ejemplos de alertas públicas relacionadas con la inseguridad de los servicios electrónicos del Gobierno.<sup>82</sup> Según el estudio oficial más reciente, publicado en 2018, el 64% (y sigue aumentando) de todos los brasileños mayores de 16 años utilizan los servicios electrónicos del Gobierno. La mitad de ellos no mencionan la preocupación por la privacidad y la seguridad como la principal razón de su abstinencia.<sup>83</sup>

En 2019 la mayoría de los sitios web de comercio electrónico ofrecían términos y condiciones de uso de fácil acceso.<sup>84</sup> La mayoría de ellos también utilizaban una conexión cifrada entre el usuario y sus servidores, y ofrecían una amplia gama de

opciones de pago seguro.<sup>85</sup> Los proveedores de comercio electrónico promovieron la seguridad y la confianza a través de protocolos de seguridad claramente visibles a disposición de los usuarios. El Gobierno también se dedicó activamente a fomentar la confianza mediante la publicación de consejos de seguridad para los compradores en línea.<sup>86</sup>

Un número cada vez mayor de brasileños utiliza los servicios de comercio electrónico. En 2018, el 33% de los encuestados en el estudio del Centro para la Innovación de la Gobernanza Internacional indicaron que compraban en línea al menos dos veces al mes, frente al 23% en 2017. Una cuarta parte de los que no compran en línea señalaron que se debía a que no confían en las compras en línea (aunque esto no sólo se debe a la falta de confianza en la seguridad de las plataformas de compras en línea).<sup>87</sup>

## D 2.3 - Comprensión del Usuario de la Protección de la Información Personal en Línea



*Este factor analiza si los usuarios de Internet y las partes interesadas de los sectores público y privado reconocen y comprenden la importancia de la protección de la información personal en línea y si están conscientes de sus derechos de privacidad.*

### Etapa: Formativa

Los usuarios y las partes interesadas de los sectores público y privado tienen conocimientos generales sobre la forma en que se maneja la información personal en línea y emplean buenas prácticas de seguridad cibernética (proactivas) para proteger su información personal en línea.

En julio de 2018 Brasil aprobó el proyecto de ley general de protección de datos.<sup>88</sup> Además, muchos

bufetes de abogados en Brasil comenzaron a crear divisiones especializadas en la protección de datos y las empresas privadas y organizaciones sin fines de lucro están organizando eventos sobre la protección de datos.

Además, existen disposiciones en otros marcos legislativos que abordan esta cuestión (véase D 4.1). Por ejemplo, las partes interesadas

mencionaron que en Brasil es común que se pida a las personas que presenten su información personal tanto en línea como fuera de línea. Según los participantes, los brasileños están acostumbrados a renunciar a su privacidad, aunque se tiene conocimiento de grandes bases de datos que sufrieron importantes fugas y un mal uso de los datos.

Además de un recibo, un consumidor en Brasil recibirá una factura con un número y un código de barras que deben escanear por medio de su teléfono móvil. Esta práctica ha causado algunos incidentes en el pasado, como, por ejemplo, cuando el malware llamado “boware” fue dirigido a usuarios del comercio electrónico, cambiaba el código de barras de la factura de manera que permitía el fraude.

En cuanto a las PYME, las partes interesadas mencionaron que era necesario prepararlas para esas actividades fraudulentas. Al respecto, el Gobierno adoptó medidas de sensibilización sobre la privacidad de los datos y la protección de la información personal en línea (véase D 3.1).

El año pasado se realizaron ejercicios internos de phishing y se realizó un análisis interno sobre

el grado de conocimiento con el propósito de comprender cómo aumentar el grado de conocimiento a nivel nacional. Se sigue trabajando en la sensibilización, mediante la difusión de folletos sobre la protección con contraseña y la necesidad de copias de seguridad, por ejemplo, así como el establecimiento del mes de octubre como mes de la seguridad, la celebración de conferencias y otros eventos, y la generación de una serie de videos, audios y material escrito informativos. Estas iniciativas se están desarrollando basándose en la idea de que el usuario debe ser capaz de seguir las instrucciones impartidas.

### **Resultados del proceso de validación llevado a cabo en marzo de 2019:**

Aunque es difícil decir que la madurez del factor cambió desde el estudio del CMM en 2018, cabe señalar que, en agosto de 2018, Brasil promulgó la Ley General de Protección de Datos de Brasil (Ley Federal N° 13.709/2018). Los participantes en las entrevistas de los grupos de discusión de 2019 expresaron su descontento por el hecho de que esta ley no entraría en vigor sino hasta agosto de 2020.

## D 2.4 - Mecanismos de Presentación De Informes



*Este factor explora la existencia de mecanismos de denuncia que funcionan como canales para que los usuarios denuncien los delitos relacionados con Internet, como el fraude, el ciberacoso, el abuso de niños, el robo de identidad, las violaciones de la privacidad y la seguridad y otros incidentes.*

### Etapa: Formativa

Se establecieron mecanismos de denuncia, los cuales se utilizan con frecuencia, para que los usuarios informen sobre los delitos relacionados con Internet. SaferNet Brasil<sup>89</sup> suministra información sobre la seguridad en Internet y el espacio para quejas a través de su sitio web. SaferNet Brasil es una organización sin fines de lucro que fue creada en 2005. La organización es un órgano de la sociedad civil único en Brasil, con acuerdos formales con el Ministerio de Justicia, la Policía Federal y la Secretaría de Derechos Humanos de la Oficina de la Presidencia de la República, que le permiten recibir y procesar informes del público. Su servicio de línea directa sólo en línea puede ser usado para denunciar contenido de forma anónima.

La Policía Federal<sup>90</sup> también tiene una página en su sitio web para las denuncias que también se pueden hacer a través de su dirección de correo electrónico (denuncia.ddh@dpf.gov.br) La pornografía infantil y adolescente<sup>91</sup> puede denunciarse a través de la línea telefónica de asistencia establecida por el Gobierno.

En general, en Brasil existen diferentes canales para denunciar incidentes. Para incidentes tales como pornografía infantil, se debe enviar un correo electrónico a la policía, mientras que para incidentes de fraude la denuncia debe pasar por el respectivo banco. Todos los incidentes se notifican a la policía, mientras que los que no están claramente clasificados se envían al CTIR Gov Brasil antes de ser enviados a las instituciones

pertinentes. Por ejemplo, si se comete un delito cibernético contra un ciudadano, el incidente lo maneja la policía civil en el estado de dicho ciudadano. Para los delitos que llegan a las empresas públicas federales, como la Caixa<sup>92</sup> o Banco Central del Brasil,<sup>93</sup> el organismo competente es la policía federal.

En general, los participantes indicaron que en Brasil los ciudadanos no tienen una cultura de denuncia. Además, no fue posible determinar si hay programas que promueven el uso de mecanismos existentes establecidos por los sectores público y privado.

Los incidentes más comunes que los usuarios enfrentan son delitos financieros tales como el fraude en línea. Para dichos incidentes, le corresponde a la Federación de Bancos encargarse de ellos. El CTIR Gov de Brasil participa en las reuniones mensuales y también en el intercambio de información en el sector financiero. El Gobierno también está buscando la manera de que la notificación de incidentes sea obligatoria para el sector privado.

### Resultados del proceso de validación llevado a cabo en marzo de 2019:

En 2019, el taller de validación confirmó en gran medida los resultados del informe del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM) de 2018.



## D 2.5 - Medios de Comunicación y Redes Sociales

*Este factor explora si la ciberseguridad es un tema común en los principales medios de comunicación, y un tema de amplio debate en los medios sociales. Además, este aspecto habla del papel de los medios de comunicación en la transmisión de información sobre la seguridad cibernética al público, dando así forma a sus valores, actitudes y comportamiento en línea en materia de seguridad cibernética.*

### Etapa: **Formativa**

En Brasil hay una cobertura mediática ad hoc de la seguridad cibernética, en la que se presenta información limitada y se informa sobre cuestiones concretas a las que se enfrentan las personas en línea, como la protección infantil en línea. Un ejemplo de la labor informativa sobre seguridad cibernética en las redes sociales es Facebook.<sup>94</sup> Facebook creó un “Centro” para prevenir el ciberacoso en Brasil en 2016, en asociación con UNICEF y Safernet. Los participantes mencionaron también que el debate sobre la seguridad cibernética en los medios sociales es limitado. Existen grupos sin fines de lucro que discuten el tema en los medios sociales brasileños. Sin embargo, alguien debe estar interesado en el tema para recibir la información. Normalmente, en caso de un incidente cibernético, esto se comunica a través de la prensa, la televisión, los medios de audio y digitales, y también se proporciona orientación.

Sin embargo, las partes interesadas indicaron que ningún incidente importante ha afectado la infraestructura nacional crítica de Brasil como para dar lugar a una cobertura más amplia por parte de los medios de comunicación y las redes sociales.

### **Resultados del proceso de validación llevado a cabo en marzo de 2019:**

En 2019, el taller de validación confirmó en gran medida los resultados del informe del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM) de 2018.

# Recomendaciones

Sobre la base de las consultas, se formulan las siguientes recomendaciones para su consideración en relación con la madurez de la cultura cibernética y la sociedad. Las recomendaciones tienen el propósito de ofrecer posibles pasos a seguir para mejorar la capacidad de ciberseguridad actual, de acuerdo con las consideraciones del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM) del Centro.

## Mentalidad de ciberseguridad

### R 2.1

Intensificar la labor en todos los ámbitos del Gobierno, especialmente los funcionarios y en el sector privado para emplear buenas prácticas de seguridad cibernética (proactivas). Crear sistemas que permitan a los usuarios de toda la sociedad incorporar más fácilmente prácticas seguras en su uso cotidiano de Internet y los servicios en línea;

### R 2.2

desarrollar programas de formación coordinados para los empleados del sector público;

### R 2.3

hacer que la cooperación intersectorial y el intercambio de información sobre los riesgos de la ciberseguridad y las prácticas óptimas se conviertan en algo habitual entre las organizaciones de los sectores público y privado, y

### R 2.4

reconocer los grupos vulnerables y los comportamientos de alto riesgo en toda la sociedad para suministrar información a las campañas de sensibilización específicas y coordinadas.

## Confianza y seguridad en internet

### R 2.5

Establecer programas de proveedores de servicios de Internet (ISP) para promover la confianza en sus servicios, basándose en medidas de eficacia de esos programas;

### R 2.6

aplicar mecanismos de retroalimentación para asegurar que los servicios electrónicos se mejoren continuamente y que se fortalezca la confianza entre los usuarios; y

### R 2.7

emplear procesos para recoger las opiniones de los usuarios en los organismos gubernamentales, a fin de garantizar una gestión eficiente del contenido en línea.

## Comprensión del usuario de la protección de información personal en línea

### R 2.8

Promover la comprensión de la protección de la información personal en línea entre los usuarios y fomentar el desarrollo de sus habilidades para gestionar su privacidad en línea;

### **R 2.9**

fomentar un debate público sobre la protección de la información personal y sobre el equilibrio entre la seguridad y la privacidad para aportar información para la elaboración de políticas;

### **R 2.10**

promover el cumplimiento de las normas de la web que protegen el anonimato de los usuarios; y

### **R 2.11**

formular políticas de consentimiento del usuario destinadas a notificar las prácticas de recopilación, utilización o divulgación de información personal confidencial.

## **Mecanismos de presentación de informes**

### **R 2.12**

Elaborar programas para promover el uso de los mecanismos de denuncia existentes por los sectores público y privado para denunciar el fraude en línea, el ciberacoso, el abuso de niños en línea, el robo de identidad, las violaciones de la privacidad y la seguridad y otros incidentes;

### **R 2.13**

instar a las diferentes partes interesadas (sectores público y privado, policía, CERT) a que coordinen los mecanismos de presentación de informes y sus funciones y responsabilidades, y colaboren y compartan buenas prácticas para mejorar los mecanismos; y

### **R 2.14**

emplear medidas de eficacia para todos los mecanismos vigentes y asegurarse de que contribuyan a su mejora.

## **Medios de comunicación y redes sociales**

### **R 2.15**

Instar a los proveedores de los medios de comunicación y las redes sociales a que amplíen aún más su cobertura más allá de la información sobre amenazas y se centren en informar al público sobre las medidas de seguridad cibernética proactivas y factibles, así como sobre las repercusiones económicas y sociales;

### **R 2.16**

fomentar un debate frecuente sobre la seguridad cibernética en las redes sociales; y

### **R2.17**

asegurar que el debate en los medios de comunicación masivos y redes sociales, así como las actitudes expresadas, aporten información para la formulación de políticas.

## Dimensión 3

# EDUCACIÓN, CAPACITACIÓN Y HABILIDADES EN CIBERSEGURIDAD

Esta dimensión analiza la disponibilidad de programas de sensibilización sobre seguridad cibernética tanto para el público como para los ejecutivos. Además, evalúa la disponibilidad, calidad y aceptación de las ofertas educativas y de capacitación para varios actores gubernamentales en el sector privado y la población en general.

## D 3.1 - Sensibilización

*Este factor se concentra en la preeminencia y concepción de los programas que despiertan el discernimiento acerca de los riesgos y las amenazas de materia de seguridad cibernética, al igual que la forma de abordar un problema, tanto para el público en general como para la dirección ejecutiva.*

Etapa: **Formativa - Establecida**

Se establece un programa nacional de sensibilización de seguridad cibernética dirigido por una organización determinada (de cualquier sector) y se orienta a una amplia gama demográfica..

Debido a la participación limitada de la sociedad civil no fue posible obtener una perspectiva

clara de las iniciativas sobre los programas de sensibilización de seguridad cibernética.

Durante el estudio, el organismo más importante de sensibilización reconocido por los participantes fue SaferNet Brasil, una organización no gubernamental creada en 2005<sup>95</sup>. En exclusiva asociación con el

Ministerio de Justicia, la Policía Federal y el Secretariado de Derechos Humanos de la Oficina del Presidente de la República que la habilitan para “proteger los derechos humanos y actuar como línea de acceso directo, línea de asistencia y nódulo de sensibilización en Brasil<sup>96</sup>. Funciona como un servicio de línea de acceso directo que recibe reclamos anónimos sobre delitos y violaciones contra los derechos humanos en Internet.<sup>97</sup> Además, SaferNet participa en la organización de campañas de sensibilización a través de instituciones educativas en todo el país.<sup>98</sup> En el 2008, SaferNet aumentó la cooperación a fin de incluir compañías tecnológicas tales como Google por medio de la firma de un contrato de cooperación que permite el monitoreo y filtración de los delitos de pornografía de menores.<sup>99</sup>

El Comité Gestor de Internet en Brasil ([www.cgi.br](http://www.cgi.br)), un consejo formado por múltiples partes interesadas creado por medio de la Orden interministerial 147 del 31 de mayo de 1995, es la principal institución encargada de promover los estándares de seguridad de las tecnologías de la información y la comunicación (TIC) y las mejores prácticas de internet,<sup>100</sup> y realiza sus actividades a través del Centro de Información de Redes de Brasil (Brazilian Network Information Centre (NIC.br) (<http://nic.br/quem-somos/>)).<sup>101</sup> Basándose en un trabajo de investigación, el NIC.br implementó varias iniciativas tales como el Antispam.br<sup>102</sup> (<http://www.antispam.br/>) e InternetSegura.br<sup>103</sup> ([https://www.Internetsegura.br/;](https://www.Internetsegura.br/)). Ambos portales tienen como objetivo la concienciación de padres y niños sobre el spam y difunden materiales sobre seguridad en internet. Además, CERT.br en colaboración con CGI.br and NIC.br ha promovido y difundido materiales de sensibilización (libros electrónicos, diapositivas) al público (<https://cartilha.cert.br/>), los cuales están especialmente diseñados para profesores y niños, y cubren temas tales como redes sociales, contraseñas, dispositivos móviles y comercio electrónico.<sup>104</sup> (Para mayor información sobre los proyectos del NIC.br relacionados con capacitación profesional, véase D 3.3). Uno de los participantes mencionó que existen algunas

actividades de sensibilización interna para el equipo administrativo dentro de las instituciones federales, pero que no se encuentran a disposición del público.

Algunos participantes señalaron que las actividades de sensibilización llevadas a cabo entre 2009 y 2013, se centraron en el uso seguro de Internet y estuvieron dirigidas a las escuelas públicas y privadas. Añadieron que en 2015 el Servicio de la Fiscalía Federal lanzó un proyecto llamado Servicio de la Fiscalía Federal para la Educación digital en los Colegios (Ministério Público pela Educação Digital nas Escolas) con el fin de organizar talleres en las universidades (para 200 profesores y estudiantes) y entregar folletos y materiales.<sup>105</sup> Después del taller, se incentivó a los maestros para que tomaran los materiales que entregaba el Servicio de la Fiscalía Federal y se les solicitó que suministraran retroalimentación a través de la página web de SaferNet. En 2018, esos mismos talleres se llevaron a cabo en universidades, pero estuvieron dirigidos a profesionales y psicólogos.

En lo que respecta a la sensibilización en materia de seguridad cibernética para ejecutivos, los participantes reconocieron que el personal directivo no siempre está consciente del tema de la seguridad cibernética y debe educarse acerca de los riesgos de seguridad cibernética que pueden afectar a sus organizaciones. Por ejemplo, dentro de la Federación de Industria del Estado de Sao Paulo (FIESP) existe un departamento de seguridad que encabeza el debate sobre la seguridad cibernética.<sup>106</sup> Asimismo, Brasscom (Asociación Brasileña de Compañías de Tecnología de la Información y la Comunicación) organiza eventos cibernéticos para promover el sector TIC ante las autoridades públicas y los clientes públicos y privados.<sup>107</sup> Ello no supone la participación de importantes organizaciones internacionales, instituciones financieras y compañías de telecomunicación, para las cuales las repercusiones estratégicas de la seguridad cibernética constituyen una prioridad. Existen algunas iniciativas sobre la sensibilización que están disponibles para las juntas directivas, pero no hay programas específicos. Además, los ejecutivos no están obligados a asistir a cursos de

capacitación sobre seguridad cibernética, aunque se considera una buena práctica. De acuerdo con el modelo para las compañías públicas o estatales, el Gobierno designa a los directores y es un requisito obligatorio que dos de los ejecutivos nombrados sean del Gobierno. Un participante declaró que, generalmente, en las compañías de tecnología, los líderes seleccionados carecen de conocimiento previo sobre el funcionamiento de la compañía, lo cual generalmente deriva en una administración deficiente dado que el ejecutivo es nombrado teniendo en cuenta afiliaciones políticas. Sin embargo, una de las compañías públicas de tecnología está planeando establecer reglas internas para rectificar este procedimiento y nombrar a los integrantes de la junta directiva basándose en sus conocimientos y experiencia en seguridad cibernética. Se agregó que las políticas de seguridad de las compañías estatales están directamente vinculadas a la oficina de la Presidencia de la República con el fin de prestar apoyo y pautas a los principales líderes.

Además, los participantes resaltaron la importancia de diferenciar entre compañías de tecnología de la información (TI) y las compañías de seguridad de información en Brasil, dado que, en su opinión, las compañías no hablan el mismo idioma. Una compañía TI está mucho más comprometida con la satisfacción del cliente y la precisión, pero en el caso de una compañía de seguridad de la información sucede lo contrario; por consiguiente, se toman distintas medidas para disminuir la brecha entre las metas comerciales y la seguridad de la tecnología de la información. A menudo, cuando llega una nueva administración, el equipo TI tiene

que acomodarse a la “tecnología de vanguardia” de la compañía. Esto significa que se imparten cursos de capacitación a la nueva administración ejecutiva (por ejemplo, para explicar la importancia de la seguridad cibernética y las normas de seguridad de la información). Un participante reveló que en su compañía tienen 24 normas de seguridad y cuatro procedimientos que guían estos procesos.

Uno de los avances que tuvo lugar después de la evaluación realizada en marzo de 2018 fue la introducción de la Política Nacional de Seguridad de la Información (Decreto Presidencial número 9.637) de diciembre de 2018, la cual establece que es responsabilidad de la Oficina de Seguridad Institucional de la Presidencia de la República “desarrollar e implementar programas sobre seguridad de la información con el objeto de sensibilizar y capacitar a los funcionarios públicos federales y a la sociedad”.<sup>108</sup> Por consiguiente, no está claro hasta qué punto las actividades de sensibilización encabezadas por la Oficina de Seguridad Institucional de la Presidencia de la República se superponen a las actividades de sensibilización de NIC.br.<sup>109</sup>

### **Resultados del proceso de validación realizado en marzo del 2019:**

En 2019, el taller de validación confirmó en gran medida los resultados del Informe del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM) de 2018.

## D 3.2 - Marco para la Educación



*Este factor aborda la importancia de las ofertas de educación de alta calidad en seguridad cibernética y la existencia de educadores titulados. Más aun, este factor examina la necesidad de mejorar la educación en seguridad cibernética a nivel nacional e institucional y la colaboración entre el Gobierno y la industria para garantizar que las inversiones educativas cumplan con las necesidades del entorno de seguridad cibernética en todos los sectores.*

### Etapa: **Formativa**

Debido a la falta de participación de los círculos académicos no fue posible obtener un panorama claro sobre la educación en seguridad cibernética en Brasil. Por consiguiente, la información suministrada a continuación se basa en un trabajo de investigación. Algunos representantes del Gobierno y la industria señalaron la necesidad de fomentar la educación en seguridad cibernética en los colegios y universidades.

El Ministerio de Educación (MEC) determina los cursos del currículum nacional sobre seguridad cibernética, así como los requisitos y las normas, pero el nivel de desarrollo es decisión de las universidades. No está regulado por organismo central. El Ministerio de Educación tiene un Catálogo Nacional de Programas de Educación Superior en Tecnología, donde se presentan los requisitos para crear programas relacionados con la seguridad cibernética, tales como defensa cibernética y seguridad de la información.<sup>110</sup> Esto presenta la carga mínima y la infraestructura recomendada para cada uno de los cursos.<sup>111</sup> El presente estudio no menciona si existe un presupuesto nacional específico para la educación en ciberseguridad. De forma similar, desde el punto de vista de las discusiones de grupo no está claro en qué medida existe cooperación entre el sector privado y las universidades.

Ya se encuentran disponibles los títulos y la oferta de educadores en seguridad cibernética. En Brasil se ofrecen cursos especializados de posgrado en seguridad cibernética. Un participante mencionó que la mayoría de las universidades que ofrecen cursos en computación tienen laboratorios. La Universidad de Sao Paulo ofrece un diploma en Ciencias Informáticas, Física Informática e Ingeniería Informática al igual que el diploma de maestría y doctorado en Ciencias Informáticas.<sup>112</sup> La Universidad Federal de ABC ofrece también programas de maestría y doctorado en Ciencias Informáticas dentro del Programa de Postgrado en Ciencias Informáticas.<sup>113</sup> Las áreas de investigación incluyen Informática Científica y Aplicada, Fundamentos de la Informática y Sistemas Informáticos.<sup>114</sup>

Además de las universidades privadas, también se ofrecen cursos de seguridad cibernética a nivel de posgrado en la Red Nacional de Investigación y Educación de Brasil (Rede Nacional de Ensino e Pesquisa - RNP).<sup>115</sup> Además, todos los años la RNP organiza el día de la seguridad internacional del computador (DISI), un evento gratuito, abierto al público y que se transmite en vivo.<sup>116</sup> El Servicio Nacional para la Educación Comercial (SENAC) es una institución privada sin fines de lucro que ofrece cursos a nivel de posgrado sobre defensa cibernética con el fin de apoyar a dicho sector en particular.<sup>117</sup>

Asimismo, de acuerdo con el informe de Trend Micro sobre la ciberdelincuencia clandestina en Brasil, se demuestra que existe una tendencia preocupante de hackers que “ofrecen clases tutoriales y cursos para aspirantes a la ciberdelincuencia por un precio determinado (por ejemplo, videos de capacitación y explicativos en Skype).”<sup>118</sup>

En la actualidad existe un debate nacional acerca de cuáles aspectos de la seguridad cibernética debe enseñarse a los alumnos de primaria y secundaria. El currículum actual presenta una pequeña referencia a los sistemas de tecnología de la información, pero en su mayor parte en el contexto de cómo utilizar los medios digitales y las tecnologías de la información para ampliar el conocimiento adquirido.<sup>119</sup>

No se presentó información sobre la participación de las partes interesadas en cuanto al desarrollo de prioridades para los programas de educación en seguridad cibernética. Dado que este tema es todavía muy incipiente no existen debates sobre las prioridades, pero si hay uno sobre los procedimientos de implementación.

#### Resultados del proceso de validación realizado en marzo del 2019:

En 2019, los representantes del mundo académico participaron en el taller de validación y confirman en gran parte los resultados del Informe CMM para las Naciones del 2018.

## D 3.3 - Marco para la Formación Profesional



*Este factor aborda la disponibilidad y el suministro de programas de capacitación en seguridad cibernética para crear un equipo de profesionales en ciberseguridad. Además, este factor examina la asimilación de la capacitación en seguridad cibernética y la transferencia horizontal y vertical de conocimientos en seguridad cibernética dentro de las organizaciones y cómo ello se traduce en el desarrollo continuo de las habilidades.*

### Etapas: **Formativa**

El Gobierno ha reconocido la necesidad de capacitar a profesionales en el campo de la seguridad cibernética.

Basándose en investigación documental, el CGI.br (véase D 3.1) coordina la labor de capacitación a través de CERT.br., el Portal de Mejores Prácticas (BCP.nic.br) y el Comité Gestor de Seguridad de la Información y Comunicaciones (CGSIC). Por ejemplo, CERT.br, siendo socio

de CME CERT, tiene la licencia para ofrecer programas de capacitación profesional como los “Fundamentos de manejo de Incidentes”, “Manejo avanzado de Incidentes para el Personal Técnico” y “Información General para la Creación y Gestión de Equipos ante Incidentes de Seguridad Informática”.<sup>120</sup> Además, el BCP.nic.br reúne un conjunto de buenas prácticas operativas para administradores de sistemas.<sup>121</sup> El portal nacional lo mantienen profesionales



de varias áreas de NIC.br, como CERT.br, el Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (CEPTRO.br) y Registro.br, en colaboración con especialistas externos a NIC.br.<sup>122</sup> Además, el CGSIC ofrece un curso sobre “Gestión de la seguridad de la información y las comunicaciones.”<sup>123</sup>

Los participantes afirmaron que la mayoría de los profesionales dentro del sector público poseen títulos profesionales extranjeros en tecnología de la información y reciben certificados en Tecnología de la Información y las Comunicaciones, tales como el título de Profesional Certificado en Seguridad de Sistemas de Información (CISSP, por sus siglas en inglés) y el de Gerente Certificado de Seguridad de la Información (CISM, por sus siglas en inglés). En cuanto a las acreditaciones técnicas, un participante mencionó que el curso informático forense ofrecido por CERT.br, es costoso, pero vale la pena.<sup>124</sup>

Basándose en trabajos de investigación documental, el Comando de Defensa Cibernético (ComDCiber), dentro del ejército brasileño y en cooperación con la Escuela Nacional de Defensa Cibernética ofrecen capacitación para los ejecutivos civiles y militares que requieran enfrentarse de manera eficaz a los ataques cibernéticos.<sup>125</sup> Las instituciones financieras tales como Fundação Bradesco (un banco nacional) ofrecen cursos en seguridad informática.<sup>126</sup>

El COBIT [Objetivos de Control para la Información y Tecnologías Relacionadas] fue aceptado como “una norma de facto para las buenas prácticas en Brasil dentro de las organizaciones privadas,

públicas y gubernamentales”.<sup>127</sup> El Tribunal de Cuentas de la Unión (TCU) realizó encuestas, informes e iniciativas de auditoría sobre el uso y aceptación del marco y existe un gran número de cursos y certificaciones relacionados con la tecnología de la información (TI) tanto para los profesionales como funcionarios públicos.<sup>128</sup> Para complementar el COBIT, también se utiliza como referencia la norma ISO 27000. El Gobierno Federal ofrece cursos relacionados con la gestión de la información: cuatro cursos durante un período de dos años. El título CISSP de Profesional Certificado en Seguridad de Sistemas de Información (Certified Information Systems Security Professional) es el certificado más reconocido junto con la capacitación de respuesta a incidentes ofrecido por el Instituto SANS.

Los participantes sugieren que existe una alta demanda de un mayor número de profesionales en seguridad cibernética en Brasil. La mayoría de los participantes confirmaron que existe una gran necesidad de cursos en seguridad cibernética y las empresas privadas generalmente capacitan a su propio personal de forma interna.

### **Resultados del proceso de validación realizado en marzo del 2019:**

En 2019, los participantes en las entrevistas de grupo nos informaron acerca de proveedores adicionales de educación profesional (por ejemplo, Febraban, una federación de Bancos Brasileños)<sup>129</sup>, pero se ha registrado un cambio en la madurez de la capacidad en seguridad cibernética en Brasil.

# Recomendaciones

De acuerdo a la información presentada en el presente estudio sobre la madurez de la educación, la capacitación y las habilidades en materia de ciberseguridad, formularemos el siguiente conjunto de recomendaciones para Brasil. Estas recomendaciones tienen como objetivo asesorar e indicar los pasos a seguir para mejorar la capacidad existente en seguridad cibernética, de conformidad con las consideraciones del Modelo de Madurez de la Capacidad de Seguridad Cibernética (CMM) del Centro Global de Capacidad en Seguridad Cibernética.

## Sensibilización

### R 3.1

Nombrar a una organización asignada (por ejemplo, RNP) con un mandato para desarrollar e implementar programas de sensibilización nacional en ciberseguridad. Coordinar y cooperar con las partes interesadas de todos los sectores;

### R 3.2

desarrollar un programa de sensibilización dirigido a los gerentes ejecutivos dentro de los sectores público y privado dado que este grupo es generalmente el árbitro final de las inversiones en seguridad. El programa podría enfocarse en hacer hincapié en la responsabilidad y la rendición de cuentas por parte de los líderes ejecutivos y los miembros de las juntas para la seguridad cibernética;

### R 3.3

promover una labor de sensibilización para el manejo de la crisis de ciberseguridad a nivel ejecutivo;

### R 3.4

promover la toma de conciencia sobre riesgos y amenazas en todos los niveles del Gobierno;

### R 3.5

adoptar medidas de evaluación para estudiar la efectividad de los programas de sensibilización en un nivel en el que se informe a las futuras campañas, teniendo en cuenta las brechas o incumplimientos; y

### R 3.6

promover debates que hagan hincapié en los fundamentos y el papel preponderante de la información y la seguridad cibernética en todas las compañías y operaciones en materia de tecnología de la información (TI) teniendo en cuenta los futuros riesgos.

## Marco para la educación

### R 3.7

crear programas de educación en ciberseguridad para instructores de seguridad cibernética a fin de garantizar que el equipo capacitado se encuentre disponible para enseñar nuevos cursos de seguridad cibernética;

### R 3.8

crear cursos con títulos reconocidos oficialmente en ciberseguridad para niveles universitarios y de posgrado, además de los otros cursos existentes relacionados con ciberseguridad en las diversas universidades en Brasil;

### **R 3.9**

promover esfuerzos por parte de las universidades y otros organismos para llevar a cabo seminarios y conferencias sobre asuntos de seguridad cibernética, dirigidos a profesionales no especializados;

### **R 3.10**

integrar cursos especializados en ciberseguridad en las carreras de ciencia informática en universidades y ofrecer cursos especializados en seguridad cibernética en universidades y otros organismos de educación superior;

### **R 3.11**

recopilar y evaluar la retroalimentación de los estudiantes actuales para desarrollar y mejorar aún más las ofertas de cursos en ciberseguridad;

### **R 3.12**

crear iniciativas para promover una educación en seguridad cibernética en currículos para niveles primario y secundario;

### **R 3.13**

establecer asociaciones para el desarrollo de interfaces para la investigación, innovación e interacción entre universidades y el sector privado;

**R 3.14** asegurar la sustentabilidad de los programas de investigación;

**R 3.15** desarrollar criterios de medición efectivos para asegurar que las inversiones en el mejoramiento en materia de educación y habilidades cumpla con las necesidades del entorno de la seguridad cibernética; y

### **R 3.16**

recopilar estadísticas sobre la oferta y la demanda de los egresados de estudios en ciberseguridad.

## **Marco para la formación profesional**

### **R 3.17**

Establecer programas de capacitación en seguridad cibernética más accesibles y estructurados con el fin de desarrollar habilidades para crear un equipo de profesionales dedicados a la ciberseguridad;

### **R 3.18**

establecer una capacitación continua para los empleados en tecnologías de la información y empleados en general con relación a asuntos relacionados con seguridad cibernética en todos los sectores;

### **R 3.19**

desarrollar criterios de medición para evaluar la demanda y el éxito de los cursos capacitación en ciberseguridad;

### **R 3.20**

crear un programa de intercambio de conocimientos orientado a mejorar la cooperación entre los proveedores de capacitación y el mundo académico;

**R 3.21**

garantizar que se ofrezcan certificaciones asequibles para profesionales en seguridad en los distintos sectores dentro del país;

**R 3.22**

desarrollar una plataforma central para intercambiar información sobre capacitación entre expertos y crear un registro de expertos en seguridad cibernética a nivel nacional;

**R 3.23**

establecer requisitos para la capacitación conjunta en ciberseguridad de los sectores público y privado, y desarrollar plataformas de capacitación colaborativas;

**R 3.24**

crear iniciativas para desarrollar un enfoque expedito para la construcción de la capacidad cibernética;

**R 3.25**

establecer iniciativas para promover el atractivo de la profesión de seguridad cibernética con el fin de instar a los empleadores a capacitar a su equipo de personal a fin de que se conviertan en profesionales de seguridad cibernética; y

**R 3.26**

desarrollar un marco de habilidades en seguridad cibernética o utilizar un marco de habilidades ya existente en el país a fin de definir claramente la trayectoria profesional para los expertos en ciberseguridad.



**Revisión de capacidades de**  
**Ciberseguridad**

**República Federativa de Brasil**



Dimensión 4

# MARCOS LEGALES Y REGULATORIOS

Esta dimensión examina la capacidad del Gobierno de diseñar y promulgar legislación nacional, directa e indirectamente relacionada con la seguridad cibernética, con especial énfasis en los temas de seguridad de las TIC, privacidad y asuntos de protección de datos, así como otros asuntos relacionados con el delito cibernético. La capacidad para hacer cumplir dichas leyes se examina a través de la capacidad de aplicación de la ley, de iniciar procedimientos judiciales y capacidad de los tribunales. Además, esta dimensión analiza asuntos tales como los marcos formales e informales de cooperación para combatir el delito cibernético.

# D 4.1 - Marcos Legales

*Este factor aborda los marcos legislativos y regulatorios relacionados con la seguridad cibernética, con inclusión de: marcos legislativos de seguridad de las TIC, privacidad, libertad de expresión y otros derechos humanos en línea, protección de datos, protección de niños, protección del consumidor, propiedad intelectual y legislación sustantiva y procesal sobre el delito cibernético.*

**Etapas:** Establecida

En Brasil no existe una normativa global que trate de manera explícita la seguridad cibernética. A pesar de los esfuerzos por introducir un marco legislativo vinculante, la legislación sobre seguridad cibernética en Brasil todavía se encuentra en desarrollo. Sin embargo, se adoptaron varias pautas oficiales o de “cumplimiento no obligatorio” que hacen referencia a temas de seguridad cibernética.

Los marcos legislativos y las directrices más pertinentes y relacionados con el sector de Internet en Brasil son:

- Ley de Delitos Cibernéticos (Ley No. 12.737/2012) (2012) también conocida como la “Lay Carolina Dieckmann” <sup>130</sup>
- El marco de los Derechos Civiles de Brasil para Internet (Ley número 12.965) (2014), Ley conocida también como el “Marco Civil da Internet” [Marco Civil de Internet] <sup>131</sup>
- El Libro Verde (Livro Verde) sobre Seguridad Cibernética en Brasil (2010) <sup>132</sup>
- La Política de defensa cibernética (2012) Regla Normativa Administrativa No. 3.389 <sup>133</sup>
- El Documento Blanco sobre Defensa Nacional (2012) <sup>134</sup>
- Estrategia de Defensa Nacional (Estratégia Nacional De Defensa) (2008) <sup>135</sup>

- Información Crítica y Protección a la Infraestructura de de las Comunicaciones (2010) <sup>136</sup>

- Anatel- Consulta Pública No. 21 <sup>137</sup>

## Legislación penal

Otras legislaciones sobre delito cibernético se encuentran en los siguientes instrumentos:

- [Ley 8,137/1990, Art. 2](#)
- [Ley 9,296/1996, Art. 10](#)
- [Ley 11,829/2008](#)
- [Ley 8,069/1990, Art. 241](#)
- [Ley 9,504/1997](#)
- [Ley 12,735/2012, Art.4](#)
- [Ley 9,100/1995, Art. 67](#)
- [Ley 9,983/2000](#)

## Regulación y cumplimiento

Otras legislaciones relacionadas con seguridad cibernética se encuentran en los siguientes instrumentos:

- [Norma Administrativa no. 35/2009](#)
- [Decreto 3,505/2000](#)
- [Resolución No. 614/2013, Art. 53](#)
- [Norma Administrativa No. 45/2009](#)
- [Norma Administrativa No. 34/2009](#)
- [Decreto 7,845/2012](#)
- [Resolución No. 617/2013, Art. 47](#)

*(Adaptado de la UIT, Perfil de Bienestar Cibernético, Brasil) <sup>138</sup>*

La introducción de leyes penales de “emergencia” no es algo nuevo en la historia del sistema jurídico de Brasil, especialmente cuando los legisladores aprueban precipitadamente estas leyes con el fin de satisfacer la demanda pública de justicia.<sup>139</sup> Asimismo, en 2012, la Ley de Delito Cibernético<sup>86</sup> (Ley No. 12.737/ 2012), también conocida oficialmente como la “Ley Carolina Dieckmann<sup>140</sup>”, fue aprobada rápidamente por el Congreso y agregada al Código Penal<sup>141</sup> con el fin de manejar el uso indebido de computadores. Los dos artículos 154-A y 154- B que se introdujeron hacen referencia a delitos cibernéticos tales como la intromisión cibernética, el uso indebido de los datos del usuario o el retiro de páginas web.

### Invasión del Dispositivo de Informática

#### **Artículo 154-A**

*Invasión de otro dispositivo informático, conectado o no a la red de computadores a través de una vulneración indebida del mecanismo de seguridad y con el propósito de obtener, falsificar o destruir datos o información sin la autorización expresa o tácita del propietario del dispositivo o instalar vulnerabilidades para obtener una ventaja ilícita:*

*Pena- Detención de tres (3) meses a un (1) año y una multa.*

### Acción penal

#### **Artículo 154-B.**

*En los delitos estipulados en el artículo 154-A solamente se procederá por medio de representación, a menos que el delito sea cometido contra la administración pública, de forma directa o indirecta, de cualquiera de los poderes de la Unión, los Estados, el Distrito Federal o las municipalidades, o contra las empresas de servicios públicos.*

El Artículo 154-A tipifica como delito la intromisión informática y estipula un incremento de las sanciones en caso de resultar en una pérdida económica o en una violación de datos.<sup>142</sup> Durante el estudio, algunos participantes señalaron su preocupación en el sentido de

que las sanciones eran demasiado leves (tres meses a un año de prisión, además de la multa). Esto se considera que crea una actividad de bajo riesgo para los delincuentes y promueve el comportamiento malicioso en línea.

El Artículo 154-B le permite a la víctima decidir si procede con los cargos penales, a menos que el ataque sea contra el Gobierno o un organismo público.<sup>143</sup>

El Marco Civil de Internet de Brasil<sup>144</sup> (Ley número 12.965) se desarrolló por medio de un proceso de consulta con múltiples partes interesadas y con la participación de la sociedad civil durante varios años, habiendo sido finalmente aprobado en 2014. La Ley está dirigida a regular el uso de Internet en Brasil, a través de principios, garantías, derechos y deberes para los usuarios. La legislación abarca varios aspectos, tales como: neutralidad de la red, privacidad de los datos relacionados con Internet, retención de datos en relación con Internet, derechos civiles relacionados con Internet, las obligaciones para los usuarios de Internet y los proveedores de servicios de Internet (ISP), y la libertad de expresión y de comunicación.<sup>145</sup> Además, esta Ley se considera precursora en la protección de los derechos del usuario de Internet y también limita estrictamente el acceso a los datos requeridos para investigaciones.<sup>146</sup>

En julio de 2018, Brasil aprobó la Ley General de Protección de Datos (Lei Geral de Proteção de Dados, o LGPD), la cual entró en vigencia en febrero 2020.<sup>147</sup> Además, Brasil cuenta con diversas disposiciones establecidas en la Constitución Federal<sup>148</sup>, el Código Penal de Brasil,<sup>149</sup> el Código de Defensa del Consumidor<sup>150</sup> y el Marco Civil de Internet:

### Marco Civil de Internet:

#### Sección II

#### Protección de archivos de registro, datos personales y comunicaciones privadas

#### **Artículo 10.**

*El almacenamiento y la disponibilidad de la conexión y el acceso a los archivos de registro de las aplicaciones de Internet*



mencionadas en esta ley, al igual que los datos personales y el contenido de las comunicaciones privadas deben tener en cuenta la preservación de la intimidad, la privacidad, el honor y la imagen de las partes directamente implicadas.

### **Artículo 11.**

*En cualquier operación de recolección, almacenamiento, custodia y tratamiento de registros, datos personales o comunicaciones por conexión y proveedores de aplicaciones de Internet en los cuales ocurra por lo menos uno de estos actos en el territorio nacional, la Ley de Brasil y los derechos a la privacidad y protección de datos personales y la confidencialidad de las comunicaciones privadas y los registros deben respetarse de forma obligatoria.*<sup>151</sup>

Durante el estudio (marzo 2018) muchas personas expresaron la necesidad de aprobar un estatuto para regular la protección de datos, el cual fue finalmente aprobado en julio del 2018.<sup>152</sup> El Marco Civil de Internet de Brasil solamente se aplica a los asuntos relacionados con Internet.<sup>153</sup> Este marco “protege los datos personales (sin definir cuáles serían considerados datos personales), el contenido de las comunicaciones privadas y el acceso a archivos de registro en referencia tanto a la conexión como a las aplicaciones de Internet”.<sup>154</sup> Además, de acuerdo con el Código Civil de Brasil,<sup>155</sup> los directores de una organización pueden ser considerados responsables en caso de negligencia en relación a la protección de las redes y los datos de la organización.<sup>156</sup> A pesar del hecho de que la Ley de Derechos de Autor de Brasil<sup>157</sup> tiene una disposición específica sobre protección de datos, se refiere solamente a la protección del titular.

El reciente Proyecto de Ley de Protección de Datos (el “Proyecto de Ley”) - inspirado en el Reglamento General de Protección de Datos (GDPR) de la Unión Europea - requiere la creación de una autoridad nacional de protección de datos y la notificación acerca de las violaciones de datos a la autoridad de protección de datos.<sup>158</sup> Dado que no existía una autoridad nacional de protección de datos, las víctimas de dichas violaciones de datos generalmente presentaban un reclamo contra el

controlador de datos, quien podía ser sancionado, en virtud del Marco Civil de Internet de Brasil y la Ley Carolina Dieckmann, pudiendo, además, incurrir en responsabilidad civil.<sup>159</sup>

Brasil puede considerarse a la vanguardia de los derechos digitales con la aprobación del Marco Civil de Internet de Brasil (también conocido como la “Carta de Derechos de Internet” de Brasil) en 2014, el cual tiene el propósito de proteger la privacidad y la libre expresión de los derechos en línea.<sup>160</sup> Además, en 2015 Brasil “dirigió conjuntamente una iniciativa en el Consejo de Derechos Humanos de las Naciones Unidas con el fin de crear un nuevo Relator Especial de Naciones Unidas sobre el derecho a la privacidad”.<sup>161</sup> A pesar de haber implementado estos textos legislativos emblemáticos, que protegen de manera integral los derechos humanos en línea, según Human Rights Watch, han ocurrido algunas violaciones que amenazan el derecho a la privacidad en Brasil. Por ejemplo, en 2015, las compañías de telefonía móvil recibieron una orden judicial para bloquear temporalmente WhatsApp (el servicio de mensajería que es propiedad de Facebook) durante dos días.<sup>162</sup> Luego, en 2016, un ejecutivo de Facebook fue arrestado por la policía federal porque la compañía negó a las autoridades el acceso a los datos del usuario.<sup>163</sup>

Brasil ha aprobado y aplicado una amplia legislación sobre la protección de los niños en línea:

- en virtud de los artículos 240 \* y 241A - E\* de la Ley 11.829 / 2008 que modifican el Estatuto del Niño y Adolescente (Estatuto da Criança e do Adolescente - ECA) (Ley No. 8.069 / 90) en 2008.<sup>164 165</sup>
- en virtud de los artículos 218, 218A, 218B\* del Código Penal, modificados e incluidos en la Ley N° 12015/2009 en 2009<sup>166</sup>

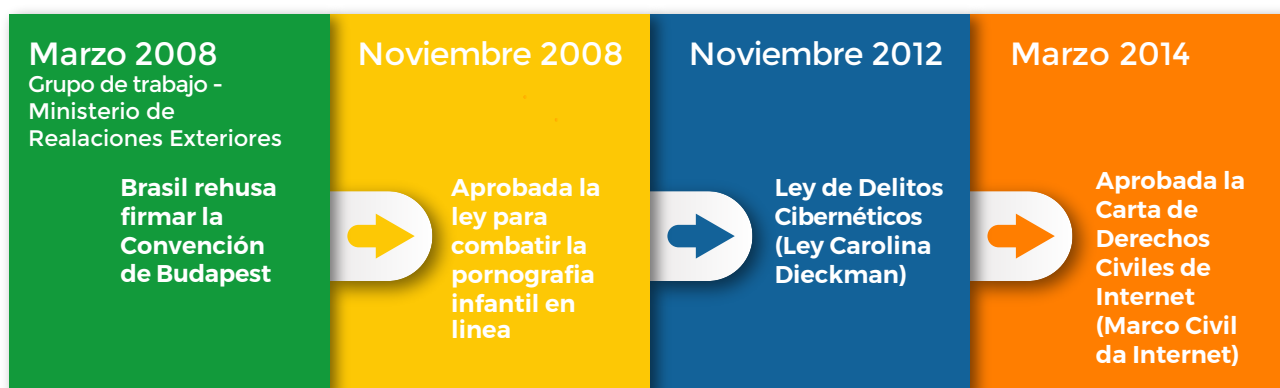
Asimismo, “los artículos 17, 18, 143 y 247 del Estatuto del Niño y del Adolescente contienen disposiciones para proteger la imagen y la reputación de los niños y adolescentes, mediante la sanción a cualquiera que los exponga de manera negativa o perjudicial”.<sup>167</sup> El artículo 241 -

del Estatuto del Niño y del Adolescente define el comportamiento de seducción de menores por Internet e impone una pena de prisión de uno a tres años.<sup>168</sup> Algunos participantes criticaron esta sanción por ser demasiado indulgente y expresaron su preocupación por la falta de legislación para tipificar el acoso cibernético, el envío de mensajes con contenido sexual (sexting) y el acceso o descarga de imágenes de pornografía infantil. Además, en la legislación brasileña, no hay denuncia obligatoria de sospecha de pornografía infantil por parte de los Proveedores de Servicios de Internet (Internet Service Provider), a menos que reciban una notificación oficial para negar el acceso a las imágenes de abuso infantil.<sup>169</sup> Por otra parte, Brasil firmó y ratificó la Convención sobre los Derechos del Niño, sin declaraciones ni reservas a los artículos 16, 17 (e) y 34 (c).<sup>170</sup> Del mismo modo, se firmó y ratificó el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía, sin declaraciones ni reservas a los artículos 2 y 3.<sup>171</sup>

Brasil carece actualmente de legislación que aborde explícitamente las amenazas cibernéticas a la propiedad intelectual. Sin embargo, la Ley de Derecho de Autor (Ley N° 9.610 /1998)<sup>172</sup> garantiza la protección de cualquier tipo de producto intelectual, independientemente de que esté registrado o publicado.<sup>173</sup> Además, la protección de la propiedad intelectual de un programa informático está regulada por la Ley sobre Protección de la Propiedad Intelectual del Software (Ley N° 9.609 / 1998).<sup>174</sup>

Las empresas en Internet están reguladas por la Ley de Internet<sup>175</sup> (Ley N° 12.965/2014), el Decreto Regulatorio<sup>176</sup> (Decreto N° 8.771 / 2016) y el Código de Defensa del Consumidor<sup>177</sup> (Ley N° 8.078 / 1990), los cuales se aplican a todos los consumidores y proveedores de servicios o bienes.<sup>178</sup> Las Oficinas de Protección al Consumidor son responsables de los derechos de los consumidores. Además, el Código de Defensa del Consumidor garantiza el derecho individual a “acceder a todos los datos almacenados sobre sí mismos y solicitar cambios, correcciones e incluso su eliminación de una base de datos”.<sup>179</sup> El hecho de no proporcionar al consumidor acceso a información sobre sí mismo está sujeto a una pena de prisión o una multa.<sup>180</sup> La Agencia Nacional de Telecomunicaciones (Anatel) regula el acceso a Internet y tiene la facultad de suprimir los abusos y establecer normas; por ejemplo, la obligación de notificar los precios a los clientes de manera oportuna.<sup>181</sup>

La Ley de Delitos Cibernéticos (Ley N° 12.737 / 2012)<sup>86</sup> y el Marco Civil de Internet de Brasil (Ley N° 12.965)<sup>182</sup> (2014) se consideran las legislaciones sustantivas actualmente vigentes de mayor pertinencia para manejar formalmente los delitos cibernéticos y otorgar facultades procesales en el manejo de pruebas electrónicas (Figura 4).



**Figura 4:** Cronología sobre la legislación del delito cibernético en Brasil

Algunos participantes señalaron que el problema no es la legislación per se sino el cumplimiento y la capacidad de respuesta. A pesar de las discusiones políticas vigentes sobre estos asuntos existen algunas brechas legislativas en el proceso de implementación que Brasil tiene que superar. Un participante señaló que:

“Por ejemplo, la Ley Carolina Dieckmann se introdujo porque los medios cuestionaban lo sucedido. Nosotros no tenemos el mismo nivel de compromiso. La legislación debe evolucionar continuamente; sin embargo, todavía se encuentra rezagada con respecto a los delincuentes cibernéticos. Los medios revelan algunas veces eventos cibernéticos, pero ¿cuál debe ser la norma y la línea de pensamiento al legislar? Todavía no hemos alcanzado el nivel deseado.”

Por consiguiente, la falta de aplicación de la legislación contra el delito cibernético y las sanciones indulgentes tienden a estimular la ciberdelincuencia.

El “Phishing (suplantación de identidad)” fue otra preocupación expresada por uno de los participantes, dado que no está penada en Brasil y no se considera una actividad delictiva. El participante sostuvo que muchas personas consideran que el “phishing” es una simple preparación, que es como si simplemente se blandiera un arma de fuego contra alguien sin usarla. La discusión técnica en la esfera legal se ve obstaculizada por la falta de conocimiento de las tecnologías de la información. Generalmente los abogados no entienden la severidad de los casos (por ejemplo, la fuga de información o el fraude en línea) y, por consiguiente, no consideran que este sea el problema.

Brasil no ha firmado el Convenio sobre la Ciberdelincuencia del Consejo de Europa (CoE); sin embargo, algunos participantes destacaron la necesidad de que Brasil acceda a esta Convención.

## **Resultados del proceso de validación realizado en marzo del 2019:**

El panorama legislativo no ha cambiado de forma significativa desde el estudio del Modelo de Madurez de la Capacidad de Ciberseguridad (CMM) de 2018. Una vez más los participantes en las entrevistas del grupo de análisis señalaron la necesidad de que Brasil firme el Convenio sobre la Ciberdelincuencia; se celebraron algunos debates internos entre diversas entidades gubernamentales. En diciembre, después de las entrevistas del grupo de análisis de marzo del 2019, Brasil tuvo acceso al proceso del Convenio de Budapest en calidad de observador.

Una adición importante al panorama legislativo brasileño lo constituye la Ley General de Protección de Datos promulgada en agosto del 2018. En diciembre de 2018, se publicó la Medida Provisional número 869 /2018, que enmienda la Ley de Protección de Datos y crea la Autoridad Nacional de Protección de Datos. De acuerdo con la enmienda mencionada anteriormente, se espera que la Ley de Protección de Datos entre en vigencia en agosto del 2020.

De manera similar, la Ley de Acoso Sexual [importunidad sexual] (No. 13.718) que entró en vigencia en septiembre del 2018 para enmendar el Código Penal (Decreto Ley No. 2.848 del 7 de diciembre de 1940) tipifica como delito la conducta libidinosa (no consensual) y la divulgación de escenas de la violación, lo cual anteriormente se consideraba solamente un delito menor.<sup>183</sup> La nueva ley prevé la pena de prisión de uno a cinco años.<sup>184</sup> Esto deroga las disposiciones de la Ley de Delitos Penales Menores (Decreto-Ley N ° 3.688, del 3 de octubre de 1941). La Ley de Acoso Sexual representa un avance importante en la lucha contra la pornografía y “cubre la divulgación de sexo, desnudos o escenas pornográficas, ya sea en forma de vídeo o fotografía, sin el consentimiento de la víctima”.<sup>185</sup>

### La Ley de Acoso Sexual (No. 13.718)

***Divulgación de la escena de violación, o escena de violación de persona vulnerable, escena de sexo o pornografía***

### **Artículo. 218-C.**

*Ofrecer, intercambiar, poner a disposición, transmitir, vender o exhibir para venta, distribución, publicación o divulgación por cualquier medio- incluidas la comunicación masiva o un computador o sistema telemático- fotografía, vídeo u otro registro audio- visual que contenga una escena de violación o violación de una persona vulnerable, o quién tolere o induzca a su práctica o, sin consentimiento de la víctima, escena de sexo, desnudez o pornografía:*

*Pena- Cárcel de uno (1) a cinco ( 5) años si el hecho no constituye un delito más serio.*

Por último, pero no por ello menos importante, los participantes en el estudio del grupo de análisis de 2019 señalaron varias iniciativas destinadas a modernizar la legislación actual (incluida la Ley sobre Delitos Cibernéticos) y asegurarse de que la seguridad cibernética se maneje de forma adecuada, aunque no se prevé ninguna legislación relacionada con ciberseguridad en 2019.

## **D 4.2 - Sistema de Justicia Penal**



*Este factor estudia la capacidad de la aplicación de la ley para investigar el delito cibernético y la capacidad de la Fiscalía de presentar casos de delitos cibernéticos y pruebas electrónicas. Finalmente, este factor aborda la capacidad de los tribunales de presidir casos de delitos cibernéticos y aquellos que implican evidencia electrónica.*

### **Etapas: Formativa**

En todo el sistema de justicia penal en Brasil, las capacidades se encuentran entre las etapas inicial y formativa de madurez.

La principal autoridad reguladora que implementa las reglas de seguridad cibernética en Brasil es el Ministerio de Justicia, a través de la Fiscalía Federal y el departamento de Policía Federal.<sup>186</sup>

La Unidad contra Delitos Cibernéticos (URCC) de la Policía Federal con sede en Brasilia, es la principal agencia de aplicación de la Ley encargada de combatir el delito cibernético y, por lo tanto, desempeña un papel operativo crítico en la persecución de los delincuentes cibernéticos dentro y fuera de Brasil.<sup>187</sup> Entre sus competencias,

la unidad está encargada de la investigación de fraudes electrónicos (estafas de banca electrónica y tarjetas de crédito), de las redes delictivas que apoyan el abuso infantil en línea, el acceso no autorizado de sistemas y redes de tecnologías de la información así como del tratamiento de delitos contra las instituciones públicas federales.<sup>188</sup> En el estudio se reconoció que la Policía Federal tiene una muy buena trayectoria de lucha contra el fraude bancario en línea y la pornografía infantil en línea.

Los participantes expresaron varias preocupaciones que enfrenta la comunidad encargada de la aplicación de la ley con respecto a la aplicación de las leyes de delitos cibernéticos:

- Carencia de un nivel adecuado de capacitación y certificaciones en muchas de las instituciones necesarias para llevar a cabo los procesos penales, ya que los oficiales de policía tienen poco conocimiento de la tecnología de la información (TI); por consiguiente, es esencial tener conocimientos básicos de TI para que la investigación sea exitosa (por ejemplo, capacitación en materia de ISP, análisis de código malicioso, atribución de delitos cibernéticos);
- falta de recursos técnicos y financieros para personal poco capacitado;
- los agentes de policía invitados a asistir a cursos de capacitación en ciberdelincuencia en Brasilia son a menudo reubicados en otros lugares; por lo tanto, es difícil retener a los oficiales en áreas específicas de ciberdelincuencia;
- diferente grado de capacidad entre las unidades de ciberdelincuencia de la Policía Federal y las de la Policía Civil (presupuesto reducido, falta de herramientas forenses avanzadas, falta de capacitación específica);
- falta de confianza entre los organismos encargados de hacer cumplir la ley y las empresas privadas para llevar a cabo investigaciones sobre delitos cibernéticos;
- falta de estandarización en la recolección de pruebas digitales y los procedimientos forenses;
- competencia limitada en la recopilación de inteligencia cibernética; y
- necesidad de aclarar las funciones y responsabilidades de los actores institucionales a fin de administrar el delito cibernético en una estructura federal compleja.

La Unidad contra Delitos Cibernéticos (URCC) tiene acuerdos principalmente informales con las

agencias de aplicación de la ley de los 26 estados de Brasil, cuando lleva a cabo investigaciones sobre delitos cibernéticos a nivel sub-nacional. Durante el estudio se destacó que, dado que los oficiales de la policía solo tienen conocimientos básicos de TI, a menudo se llama a especialistas en delincuencia cibernética extranjeros para ayudar con las investigaciones. Además, la Academia Nacional de Policía ofrece cursos y capacitación en línea sobre seguridad cibernética para oficiales de la Policía Federal.

Brasil tiene un laboratorio digital forense ubicado en el Instituto Nacional de Criminalística (Instituto Nacional de Criminalística- (INC) dentro de la Policía Federal en Brasilia.<sup>189</sup> Además, cada Estado en Brasil posee su propio laboratorio con funciones específicas tales como decodificar los datos cifrados de los teléfonos. En caso de que el laboratorio de TI, a nivel estatal, carezca de alguna capacidad, se establece contacto con la URCC o con una organización privada. Los participantes describieron la cooperación a nivel laboral y el intercambio de información entre la Policía Federal y la Policía Civil Estatal como muy eficiente. Un participante reconoció que dentro de la Policía Federal no existe ninguna restricción que pudiera impedir el intercambio de información. No existe una estructura formal para el intercambio de información entre la Policía Federal y la Policía Civil Estatal y la cooperación se basa en la confianza. En lo referente a intercambiar información de seguridad entre las agencias de aplicación de las leyes, Brasil sigue un enfoque vertical de arriba hacia abajo.

De acuerdo con las leyes de Brasil, los proveedores de servicios de Internet (ISP) deben cooperar con las autoridades gubernamentales al recibir solicitudes oficiales (por ejemplo, una orden del tribunal, una orden de registro, órdenes de comparecencia) y para divulgar los datos de los clientes.<sup>190</sup> Una vez que la autoridad competente recibe una solicitud, un juez puede emitir una orden de comparecencia, o una orden para realizar una investigación debido a la violación de la ley.<sup>191</sup> El Marco Civil de Internet de Brasil garantiza que las restricciones legales no limiten la capacidad de la autoridad competente de

llevar a cabo sus obligaciones y tener acceso a los datos personales cuando tiene la autoridad legal para hacerlo.<sup>192</sup> De acuerdo con la reglamentación de Telecomunicaciones del Brasil, en virtud de la Ley No. 9.296/96, “la interceptación de las comunicaciones telefónicas y los sistemas de tecnología de la información pueden producirse solamente con una orden del tribunal, si existe sospecha de que el perpetrador cometió un delito, y no existe ninguna otra forma de obtener pruebas.”<sup>193</sup>

Durante el estudio del 2018, no fue posible obtener un panorama claro sobre la capacidad de los jueces y fiscales para manejar los casos de delitos cibernéticos y los casos que implican pruebas digitales. Teniendo en cuenta las entrevistas de seguimiento, los participantes consideraron que la capacidad de los jueces y fiscales para manejar los casos de delitos cibernéticos y los casos que implican pruebas digitales era ad hoc y no institucionalizada. Brasil cuenta en la actualidad con 1000 fiscales federales y 2.400 fiscales. No existen tribunales especiales para manejar los casos de delitos cibernéticos, así como tampoco jueces especializados en delitos cibernéticos. Los jueces reciben capacitación solamente a través de los fiscales federales.

En 2011, se creó un grupo especial de trabajo sobre delitos cibernéticos constituido por ocho fiscales federales.<sup>194</sup> Estos nuevos fiscales y jueces federales pueden (desde el 2015) participar en este grupo de trabajo, pero el mismo solamente está disponible una vez al año. Esto tiene repercusiones negativas en la efectividad de la aplicación de la ley para manejar los casos de delitos cibernéticos. Si los casos se presentan ante el tribunal, ello podría derivar en investigaciones y procesos judiciales ineficaces y, en consecuencia, a que no se logre condenar a los culpables. Igualmente, durante el estudio se destacó que, a nivel estatal, el mayor problema es que el fiscal estatal a menudo carece del conocimiento y la capacidad para llevar a cabo la investigación de delitos cibernéticos. También existen dificultades cuando los fiscales solicitan

datos digitales de los proveedores de servicios de Internet (ISP) debido parcialmente al hecho de que Brasil no ha podido cambiar a la versión 6 del Protocolo de Internet (IPv6). En la actualidad, los proveedores de servicios de internet (ISP) están funcionando con el Protocolo de Internet versión 4 (IPv4), que es insuficiente porque no existen suficientes direcciones IP en el conjunto de direcciones de IPv4. En consecuencia, los proveedores de servicio de internet comparten las mismas direcciones IP entre muchas personas, haciendo muy difícil que se pueda identificar al verdadero delincuente. Una sugerencia fue establecer normas sobre el número de personas que pueden tener acceso a la misma dirección IP. En la actualidad, en Brasil, hasta 32 personas pueden recibir la misma dirección IP de los proveedores de servicios de internet.

Brasil participa regularmente en programas de capacitación sobre delito cibernético en el exterior, patrocinados por organismos regionales tales como el Consejo de Europa y la Organización de los Estados Americanos. Por ejemplo, el Programa sobre el delito cibernético de la Oficina del Consejo de Europa (C-PROC) presta apoyo a Brasil en materia de legislación, capacitación judicial y aplicación de las leyes y desarrollo institucional.<sup>195</sup> En julio del 2018, los fiscales federales fueron invitados a asistir a la Conferencia Octopus sobre Delitos Cibernéticos en Estrasburgo.<sup>196</sup> Un participante señaló que, los fiscales federales y estatales son invitados a participar en las reuniones sobre delitos cibernéticos con la OEA, en el Grupo de Trabajo sobre Delitos Cibernéticos de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), cada dos años en Washington D.C.<sup>197</sup>

En 2018, Microsoft Brasil firmó un acuerdo de cooperación con la oficina de la Fiscalía de Sao Paulo (MPSP) para impartir un programa de capacitación sobre delito digital para los fiscales públicos y otras iniciativas relacionadas con la lucha contra el delito en línea.<sup>198</sup>

## Resultados del proceso de validación realizado en marzo del 2019:

Además de reafirmar los resultados del estudio del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM), los participantes en las entrevistas de los grupos de análisis de 2019 señalaron la capacitación reciente impartida para el poder judicial. También informaron a los investigadores acerca de la existencia de equipos de procesamiento judicial en ciertos estados de la federación. A pesar de ello, los participantes opinaron que Brasil todavía no tiene suficientes fiscales y jueces capacitados para llevar a la justicia a un número cada vez mayor de delincuentes cibernéticos.

## Retroalimentación gubernamental presentada en 2020

Según el trabajo de investigación documental posterior a las entrevistas de los grupos de análisis de marzo al 2019, la autoridad regulatoria para los delitos cibernéticos es el Ministerio de Justicia y Seguridad Pública.<sup>199</sup> De acuerdo con el artículo 10, Punto V de la Ley No. 13.844, la Oficina de Seguridad Institucional de la Presidencia de la República, está encargada de los asuntos de seguridad cibernética.<sup>200</sup> Esto no constituye un desvío significativo de los resultados del estudio del CMM en 2018; por consiguiente, no cambia la madurez de la capacidad en seguridad cibernética de Brasil.

## D 4.3 - Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético



*Este factor aborda la existencia y el funcionamiento de mecanismos formales e informales que permiten la cooperación entre actores internos y aquellos más allá de las fronteras para impedir y combatir el delito cibernético.*

### Etapa Formative

Las autoridades de Brasil han reconocido la necesidad de mejorar los mecanismos de cooperación tanto formal como informal, a nivel nacional y transfronterizo, pero dichos mecanismos siguen siendo ad hoc. Los participantes mencionaron en particular que la cooperación en la lucha contra el delito cibernético es un área con grandes dificultades especialmente a nivel internacional.

La cooperación formal existe tanto a nivel interestatal como interinstitucional. Una asociación con CICTE es un buen ejemplo de cooperación interestatal al facilitar el intercambio

de información sobre seguridad cibernética más allá de las fronteras de Brasil.<sup>201</sup> Igualmente, el blog SegInfo sirve como programa nacional para difundir la información relacionada con seguridad cibernética (por ejemplo, advertencias de vulnerabilidad, últimos proyectos y eventos) dentro del sector público.<sup>202</sup> Brasil es un miembro de la iniciativa ITU-IMPACT y también ha participado en reuniones de los Equipos de respuesta a incidentes de seguridad informática (CSIRT) latinoamericanos y del Caribe organizadas por el Registro de Direcciones de Internet de América Latina y el Caribe (LACNIC).<sup>203</sup> Además, CERT.br es miembro de FIRST desde 2002.<sup>204</sup>

Existe cooperación informal con proveedores de servicios de internet multinacionales, a título voluntario, ya que no tienen responsabilidad legal ni están obligados a responder a las solicitudes de los organismos de aplicación de la ley a menos que reciban una solicitud oficial (por ejemplo, una orden de un tribunal o una orden de registro). En la actualidad, Brasil se encuentra en el proceso de desarrollar un acuerdo bilateral entre los proveedores de servicios internet (ISP) y los organismos encargados de la aplicación de las leyes que permite que los ISP intercambien datos directamente con las autoridades encargadas de la aplicación de la ley. Por ejemplo, en mayo de 2018, la Oficina Central Nacional (NCB) de INTERPOL en Brasilia y el Banco do Brasil S/A firmaron un contrato para cooperar e intercambiar información con el propósito de manejar los delitos cibernéticos. “Esta sociedad público-privada patrocinará un intercambio sistemático de datos relacionados con las amenazas cibernéticas.”<sup>205</sup>

Entre los diversos canales de cooperación internacional disponibles, los compromisos con INTERPOL, Ameripol y Europol fueron descritos como los canales más importantes para facilitar la cooperación trasfronteriza e intercambiar información. Teniendo en cuenta el trabajo de investigación documental, la URCC se encarga de coordinar “todas las redes internacionales de aplicación de la ley para facilitar el intercambio de información y manejar los protocolos operacionales”<sup>206</sup> A nivel operativo, el intercambio de información con las agencias encargadas del cumplimiento de las leyes y los tribunales fue descrita como efectiva, pero surgieron problemas cuando se solicitó información de los proveedores de servicios internet en el extranjero y de compañías privadas de Internet (tales como Facebook y Google en los Estados Unidos) ya que pocas veces responden y evitan cooperar con los organismos encargados de la aplicación de las leyes en Brasil. En otras palabras, si las compañías tienen sede en Brasil la solicitud de información es más fácil porque deben acatar las leyes brasileñas. Otra preocupación que se planteó durante el estudio

fue un asunto relacionado con los Tratados de Asistencia Legal Mutua (MLAT) porque son muy lentos y esto retrasa las investigaciones. Generalmente toma aproximadamente dos años obtener una respuesta a una solicitud oficial de los Estados Unidos porque solamente cuentan con unos pocos fiscales que tratan con los Tratados de Asistencia Legal Mutua alrededor del mundo.

INTERPOL Brasilia tiene acceso al enlace de comunicación seguro de INTERPOL, I- 24/7, que es un portal de Internet de acceso restringido que brinda a la policía de todo el país un acceso instantáneo y automatizado con las bases de datos criminales de la INTERPOL.<sup>207</sup> La red 24/7 es considerada como una comparación informal porque solamente se utiliza para compartir información para propósitos de inteligencia, y no para recopilar pruebas. En el 2017, la Policía Federal de Brasil y Europol firmaron un contrato estratégico para expandir la cooperación y combatir actividades delictivas a través de las fronteras, lo cual podría considerarse una cooperación formal.<sup>208</sup>

Uno de los participantes agregó que la capacitación para delitos cibernéticos y los eventos internacionales relacionados con la seguridad cibernética sirven como otra plataforma para crear confianza y conexión entre los diferentes protagonistas con el fin de permitir realizar solicitudes informales de apoyo, preservando los datos y obteniendo información para determinar la mejor forma de seguir adelante. El Gobierno se encuentra en proceso de tomar medidas para colocar a Brasil en una posición legislativa que conduzca a ratificar próximamente el Convenio de Budapest sobre la Ciberdelincuencia.

### **Resultados del proceso de validación realizado en marzo de 2019:**

Una vez más, los participantes en las entrevistas del grupo de análisis en la validación del 2019, señalaron que la colaboración entre los ISP y las autoridades encargadas del cumplimiento de las leyes está en proceso, pero todavía existen algunos ejemplos en que los ISP no están



colaborando. El problema se ve exacerbado, entre otras cosas, por el gran número de ISP en el país, muchos de los cuales no cuentan con personal de TI dedicado y dependen de consultores externos para tratar los problemas de seguridad cibernética.

Por otra parte, la cooperación entre CERT.br y CTIR Gov ha mejorado notoriamente. Lo mismo fue reconocido por los entrevistados en 2019 en lo referente a la cooperación entre los diversos

niveles de organismos de aplicación de la ley en el país; las funciones y responsabilidades entre los organismos encargados de la aplicación de la ley a nivel estatal y federal son claras y las relaciones son funcionales. Todas estas entidades tienen un punto de contacto las 24 horas, que contribuye a lo que fue evaluado por los entrevistados en el estudio-validación de 2019 como “buena comunicación”.

## Recomendaciones

De acuerdo con la información presentada en este estudio sobre los marcos legales y regulatorios de seguridad cibernética, formulamos el siguiente conjunto de recomendaciones para Brasil. Estas recomendaciones tienen como objetivo ofrecer asesoramiento y presentar los pasos a seguir para mejorar la capacidad actual en seguridad cibernética, siguiendo las consideraciones del modelo CMM del Centro

### Marcos Legales

#### R 4.1

Considerar la posibilidad de establecer un proceso periódico de revisión y ampliar de las leyes de Brasil relacionadas con el ciberespacio para abordar la dinámica de las amenazas de seguridad cibernética (por ejemplo: acoso cibernético, envío de mensajes de texto con contenido sexual (sexting) y acceso y descarga de imágenes de pornografía infantil);

#### R 4.2

desarrollar nuevas disposiciones legislativas a través de procesos de consulta de múltiples partes interesadas sobre IP en línea y derechos humanos en línea;

#### R 4.3

promulgar órdenes de entrada en vigor de la legislación existente y asignar organismos para supervisar la aplicación de la ley en la seguridad cibernética y el delito cibernético;

#### R 4.4

dedicar recursos para garantizar la plena aplicación de las leyes de seguridad cibernética existentes y nuevas y supervisar la implementación;

#### R 4.5

garantizar que, en caso de investigación transfronteriza, la ley procesal estipule las acciones que deben llevarse a cabo para investigar con éxito el delito cibernético;

#### R 4.6

considerar el desarrollo de una estrategia que cubra la seguridad cibernética y el delito cibernético y que también aclare las funciones y responsabilidades de los actores (CIRT, organismos encargados de la aplicación de la ley, ministerios) que participan en el manejo de la respuesta a incidentes de seguridad informática e investigaciones de delitos cibernéticos;

#### R 4.7

adaptar e implementar disposiciones legales sobre comercio electrónico, en relación con incidentes de delitos cibernéticos, como fraudes en línea, spam y sitios de suplantación de identidad [phishing];

#### R 4.8

considerar la creación de una plataforma para intercambiar pruebas electrónicas entre las fuerzas regionales encargadas del delito cibernético;

#### R 4.9

mejorar la cooperación existente entre los ISP y las agencias de aplicación de la ley para retirar el contenido que infringe los derechos de autor de los sitios web;

#### R 4.10

revisar y hacer cumplir las disposiciones legislativas que obligan a los ISP a brindar asistencia técnica a los organismos de aplicación de la ley cuando realizan vigilancia electrónica legal; y

#### R 4.11

considerar la posibilidad de firmar el Convenio de Budapest sobre la Ciberdelincuencia del Consejo de Europa.

### Sistema de Justicia Penal

#### R 4.12

Invertir en capacidades e investigación avanzadas para permitir la investigación de casos complejos de delitos cibernéticos, con el apoyo de pruebas periódicas y capacitación de investigadores;

#### R 4.13

asignar recursos dedicados a unidades de delitos cibernéticos completamente operativas basadas en la toma de decisiones estratégicas para apoyar las investigaciones, especialmente a nivel estatal;

#### R 4.14

establecer programas de creación de capacidad institucional para jueces, fiscales y personal policial (por ejemplo, a través de Ameripol, Interpol, Europol u otras organizaciones) con el fin de adquirir nuevas habilidades en tecnologías de la información y la comunicación, necesarias para realizar las investigaciones de delitos cibernéticos (por ejemplo: recopilación de pruebas digitales), así como formas efectivas de hacer cumplir las leyes cibernéticas;

#### R 4.15

fortalecer la capacidad nacional de investigación de delitos relacionados con la informática, con inclusión de recursos humanos, procesales y tecnológicos, medidas de investigación completas y cadena de custodia digital;

#### R 4.16

crear un equipo de fiscales y jueces especializados para manejar casos de delitos cibernéticos y casos que involucren evidencia electrónica;

#### R 4.17

considerar el establecimiento de normas para la capacitación de los agentes del orden en el delito cibernético;

#### R 4.18

dedicar suficientes recursos humanos y tecnológicos para asegurar procedimientos legales efectivos con respecto a casos de delitos cibernéticos;

#### R 4.19

considerar la posibilidad de solicitar estadísticas confiables y precisas sobre el delito cibernético a la Unidad de Represión de Delitos Cibernéticos (URCC) de la Policía Federal y al CERT.br para informar mejor a los encargados de la toma de decisiones sobre el panorama actual de amenazas del delito cibernético en Brasil al desarrollar políticas y legislaciones para abordar este asunto;

#### R 4.20

considerar la creación de un Laboratorio Nacional de Delitos Cibernéticos bajo los auspicios de la URCC de la Policía Federal para facilitar el análisis forense digital;

#### R 4.21

establecer un mecanismo formal para permitir el intercambio de información y buenas prácticas entre fiscales y jueces a fin de garantizar el enjuiciamiento eficiente y efectivo en los casos de delitos cibernéticos, y

#### R 4.22

recopilar y analizar regularmente estadísticas y tendencias sobre investigaciones de delitos cibernéticos, enjuiciamientos por delitos cibernéticos y condenas por delitos cibernéticos.

### Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético

#### R 4.23

fortalecer la cooperación internacional para combatir el delito cibernético basándose en los marcos de asistencia jurídica vigentes y celebrar nuevos acuerdos bilaterales o internacionales;

#### R 4.24

considerar el establecimiento de una Plataforma de Inteligencia de Amenazas para intercambiar información en tiempo real entre la URCC de la Policía Federal y el CERT (CERT.br);

#### R 4.25

asignar recursos para apoyar el intercambio de información entre los sectores público y privado en el ámbito nacional y para fomentar el marco legislativo y los mecanismos de comunicación;

#### R 4.26

ampliar la cooperación entre el sector público y los bancos y otras instituciones financieras en relación con el intercambio de incidentes, con el fin de aumentar el grado de conciencia sobre la seguridad cibernética en Brasil;

#### R 4.27

facilitar los mecanismos de cooperación informal dentro de los sistemas policial y de justicia penal, y entre la policía y terceros, tanto a nivel nacional como transfronterizo, en particular los proveedores de servicios de internet, y

#### R 4.28

fortalecer los mecanismos de cooperación informal dentro de los sistemas policial y de justicia penal, y entre la policía y terceros, tanto a nivel nacional como transfronterizo. Considerar los conocimientos técnicos de otras áreas, como la cooperación anticorrupción.



**Revisión de capacidades de**  
**Ciberseguridad**

**República Federativa de Brasil**




Dimensión 5

# ESTÁNDARES, ORGANIZACIONES Y TECNOLOGÍAS

Esta dimensión examina el uso efectivo y generalizado de la tecnología de seguridad cibernética para proteger a los individuos, las organizaciones y la infraestructura nacional. La dimensión examina específicamente la implementación de estándares de seguridad cibernética y buenas prácticas, el despliegue de procesos y controles, y el desarrollo de tecnologías y productos para reducir los riesgos de seguridad cibernética.

## D 5.1 - Adhesión a los Estándares



*Este factor estudia la capacidad del gobierno para diseñar, adaptar e implementar normas de seguridad cibernética y buenas prácticas especialmente aquellas relacionadas con procedimientos y desarrollo de software.*

Etapa: **Formativa- Establecida**

Brasil ha establecido un número de instituciones, a las que las organizaciones, tanto privadas como públicas, pueden dirigirse para obtener una certificación de acuerdo a los estándares, las mejores prácticas y las directrices de las TIC. Más concretamente, la Associação Brasileira de Normas Técnicas (ABNT) suministra las

versiones brasileñas de las normas ISO IEC tales como ABNT NBR ISO/IEC 270001; el CEPESC es el Centro de Investigación y Desarrollo para la Seguridad de la Comunicación, el cual se encarga del desarrollo de proyectos relacionados con la seguridad de las comunicaciones, incluida la transferencia de tecnología; el CAIS (Centro de

Atención a Incidentes de Seguridad) de la RNP (Red Nacional de Enseñanza e Investigación), a pesar de ser el equipo de respuesta a incidentes para las redes académicas brasileñas, se encarga de crear y promover prácticas de seguridad para las redes en general. De conformidad con las fuentes gubernamentales, existen instrucciones normativas y normas complementarias elaborados en el Departamento de Seguridad de la Información de la Oficina de Seguridad Institucional de la Presidencia de la República (GSI), que maneja la normalización de la seguridad de información y la seguridad cibernética en el ámbito de la Administración Pública Federal.

Los participantes señalaron que el diseño, la adopción y la auditoría de las normas de seguridad cibernética varían significativamente entre los sectores públicos y privados. En cuanto al sector público existen reglas estrictas que se han convertido en estándares desde el 2001 y que aplican a la Administración Pública Federal (FPA).<sup>209</sup> Existe un sistema de auditoría y todas las agencias federales deben designar una unidad dentro de su organización para realizar auditorías. Más aun, existe una oficina de control general encargada de crear estándares y evaluar el progreso de la implementación de dichos estándares por parte de todos los departamentos. Además, hay una herramienta de autoevaluación a disposición de los departamentos para ayudarlos a preparar auditorías futuras. Por último, los participantes mencionaron que la FPA diseñó un modelo y visitó más de 40 agencias para establecer un panorama completo del nivel general de madurez. En marcado contraste existen diferencias significativas en cuanto a la madurez en las organizaciones públicas de nivel estatal. La principal razón es la ausencia de mecanismos para implementar una aplicación uniforme de políticas lo mismo que falta de experiencia y de financiamiento. Al mismo tiempo, la falta de responsabilidad cuando los empleados no cumplen con las políticas y la ausencia de criterios para medir el cumplimiento contribuyen a la práctica deficiente en seguridad cibernética en los Estados.

Algunos casos interesantes son SERPRO y DATAPREV, dos compañías que no forman parte de la FPA pero que prestan servicios críticos para el Gobierno brasileño. Ambos se adhieren a los más altos estándares internacionales; DATAPREV obtuvo la certificación de Nivel 4 para dos de sus centros de datos, mientras que el tercero tiene una certificación de Nivel 3.

Al centrarse en el sector privado, los participantes informaron que la tasa de adopción difiere entre sectores, siendo las compañías financieras y de comunicación electrónica pioneras en esta área. Ciertos sectores, como las comunicaciones electrónicas y las finanzas, tienen algunos requisitos de seguridad obligatorios; sin embargo, en la mayoría de los casos, la fuerza que impulsa el cumplimiento de las normas es la demanda del mercado y la necesidad comercial. La norma ISO 27001 es el marco más frecuentemente adoptado y también se está considerando el marco de seguridad cibernética NIST.

Los participantes coincidieron en que el Banco Central puede imponer requisitos de seguridad, pero no existe un estándar específico promovido por el regulador. Existe una combinación de estándares internacionales, como el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)<sup>210</sup> para la seguridad de datos impuestos por MasterCard<sup>211</sup> y Visa<sup>212</sup> que las compañías se propusieron seguir estrictamente. Cabe señalar que, durante el estudio, no tuvimos la oportunidad de hablar con instituciones financieras privadas para corroborar estos datos.

Haciendo hincapié en los estándares de desarrollo y adquisición de software, existen pautas específicas para el sector público, pero no está claro en qué medida las pautas están relacionadas con la seguridad cibernética. Los participantes señalaron que existen requisitos en la FPA con respecto a la compra de equipos de seguridad cibernética y el desarrollo de software. Estos requisitos son genéricos y las organizaciones desarrollan procesos internos. En general, los participantes afirmaron que las pautas son eficaces y aportan transparencia. No pudimos obtener un panorama claro del sector privado.

Los participantes reconocieron la necesidad de contar con una autoridad relacionada con la seguridad para establecer los estándares en todos los sectores (no solamente en la FPA) y promover el cumplimiento de estos estándares. También se destacó la importancia de simplificar el proceso adquisición de software y hardware. Se sugirió, además, que las discusiones con todas las partes interesadas y reguladores pertinentes deben comenzar antes de la adopción de la estrategia nacional de seguridad cibernética.

#### **Resultados del proceso de validación realizado en marzo de 2019:**

En marzo en 2018 no existían estándares de TIC a nivel nacional prescritos en el sector bancario, lo cual se reflejó en nuestro informe.

Desde entonces la situación ha cambiado. De acuerdo con la Resolución del Consejo Monetario Nacional de Brasil, CMN 4.658 del 26 de abril de 2018,<sup>213</sup> todas las instituciones financieras bajo la sombrilla reguladora del Banco Central de Brasil debían implementar una política de seguridad cibernética a más tardar el 6 de mayo del 2019 y tomar medidas de acuerdo con los estándares de seguridad cibernética prescritos por esta resolución para finales del 2021. Fuera de esto los entrevistados en 2019 no han informado sobre nuevos estándares en seguridad cibernética.

## **D 5.2 - Resiliencia de Infraestructura de Internet**

*Este factor se refiere a la existencia de servicios e infraestructura de internet confiables en el país, al igual que rigurosos procesos de seguridad en los sectores público y privado. Este aspecto también examina el control que el gobierno puede tener sobre su infraestructura de Internet y la medida en que se subcontratan los sistemas y las redes.*

#### **Etapas: Establecida**

Los participantes del estudio señalaron que la estructura de Internet en Brasil es muy confiable. Durante los últimos cinco años ha existido un incremento constante en el número de usuarios de Internet. En la actualidad, el índice de penetración de Internet en Brasil es del 67 por ciento.<sup>214</sup>

También existe un importante mercado de internet móvil con más de 81 millones de personas que utilizan el Internet móvil.<sup>215</sup> Las ventas por comercio electrónico están aumentando y en la actualidad exceden los \$20 mil millones dado que

más de 61 millones de personas son compradores digitales, con un comercio móvil que alcanza un índice de penetración del 32%.

Estas estadísticas nos muestran las bases para comprender la madurez de la confiabilidad de infraestructura de Internet y de los estándares de seguridad en los servicios electrónicos ofrecidos por las organizaciones públicas y privadas. Los participantes sugirieron que se ofrece una amplia gama de servicios de gobierno electrónico, tales como la votación electrónica. Se pueden hacer observaciones similares con respecto al

sector privado, donde existe una abundancia de servicios electrónicos, y los participantes creen que su aceptación está aumentando.

Existe una amplia gama de proveedores de servicios de internet públicos y privados en Brasil, con distintos grados de calidad, servicios y precios. Abranet<sup>216</sup> ha impuesto regulaciones, pero no pudimos entrevistar a las personas del sector de las telecomunicaciones durante nuestro estudio. Tomando como base nuestra investigación documental existen más de 25 Puntos de Intercambio de Internet (IXP) que se mantienen gracias a un proyecto global llamado IX.br. El número de puntos de intercambio (IX) asegura un entorno atractivo para la innovación y la conectividad a Internet, al tiempo que incrementa la resiliencia de la infraestructura de Internet.<sup>217</sup> Vale la pena señalar que el proyecto IX.br logra una capacidad máxima de 5.060GB

por segundo con un promedio de 3.260GB por segundo en Brasil, ampliamente equivalente a los servicios ofrecidos por el proveedor alemán DE-CIX, que son los más altos del mundo.<sup>218</sup>

### Resultados del proceso de validación realizado en marzo de 2019:

Además de la información recopilada durante el estudio, los participantes entrevistados en el grupo de revisión y validación nos informaron sobre las actividades del NIC.br para promover la resiliencia de la infraestructura de Internet. En particular, aprendimos sobre la promoción de las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS), cuyo propósito es alentar a los operadores de redes y a los puntos de intercambio de internet a fomentar la resiliencia en la infraestructura de internet de Brasil.

## D 5.3 - Calidad del Software



*Este factor examina la calidad de la implantación de software y los requisitos funcionales en los sectores público y privado. Además, este factor estudia la existencia y mejora de las políticas y los procesos de actualización y mantenimiento de software, basándose en evaluaciones de riesgos y en la criticidad de los servicios.*

### Etapas: **Formativa**

La calidad del software varía significativamente en el sector público dependiendo de si las organizaciones forman o no parte de la Administración Pública Federal (FPA). Existe un inventario de software de seguridad para la FPA y las redes están monitoreadas en caso de programas maliciosos [malware]. La aplicación de parches de software obsoleto se logra automáticamente y existen KPI (indicadores claves de desempeño) para evaluar la efectividad de los mecanismos de parcheo. Además, todos los ministerios tienen agencias que cubren la gestión de las TIC y establecen requisitos relacionados con el software. Hay una oficina especial de TI

que ofrece soluciones de software y hardware, por lo que el apoyo de la administración está centralizado.

Los participantes señalaron que las organizaciones del gobierno estatal no tienen un catálogo de software seguro y que los parches no se implementan de manera sistemática. Con respecto al sector privado, la calidad del software depende en gran medida del tamaño de la organización, siendo más maduras las corporaciones en los sectores financiero y de telecomunicaciones.



El desarrollo de software es una práctica común tanto en el sector privado como público. Los participantes mencionaron que se desarrollan instrumentos de software internos para monitorear las redes, los incidentes y para brindar sensibilización acerca de la situación. Las organizaciones utilizan técnicas de inteligencia artificial y aprendizaje automático para disuadir, detectar y mitigar los ataques.


Como lo explicaron los participantes la transferencia de tecnología es problemática en Brasil debido a la falta de legislación para establecer y proteger la propiedad intelectual. Por lo tanto, muchas organizaciones internacionales del sector tecnológico se muestran indecisas en suministrar soluciones de software a Brasil. Esto ha llevado a un incremento en el diseño de productos de seguridad cibernética nacionales.

No pudimos obtener un panorama claro sobre si el software interno se verifica para validar las propiedades de seguridad.

#### **Resultados del proceso de validación realizado en marzo de 2019:**

Durante el taller de validación del 2019 los participantes agregaron que ni la industria de la Aviación y el sector financiero.<sup>219</sup> Tenían un catálogo de plataformas de software seguro y sus aplicaciones. Aunque ambas industrias informaron ser conscientes de la seguridad Cuando se relaciona con el Software que se está utilizando. Debido a las restricciones presupuestarias el software utilizado por las instituciones financieras no se actualiza regularmente.

## **D 5.4 - Controles Técnicos de Seguridad**



*Este factor estudia la evidencia relacionada con la implantación de controles técnicos de seguridad por parte de los usuarios y los sectores público y privado, y si el conjunto de controles técnicos de seguridad cibernética está basado en los marcos de seguridad cibernética establecidos.*

Etapa: **Establecida**

La adopción de controles técnicos de seguridad en Brasil varía entre sectores y organizaciones. Los participantes señalaron que la adopción e implementación de controles en los organismos gubernamentales se encuentran muy adelantadas en la FPA, pero es bastante elemental y su promoción irregular en los gobiernos estatales, debido a restricciones financieras, limitaciones de recursos humanos y falta de una estructura organizacional apropiada. Brasil tiene una constitución extensa que no contempla la seguridad cibernética. Existe una estrategia para la implementación de controles

en la FPA que incluye un modelo detallado para evaluar la madurez de las organizaciones, pero no tiene control sobre los estados y municipios. En consecuencia, cualquier control técnico que sea obligatorio para la FPA no se puede hacer cumplir en los Estados ni las agencias de auditoría pueden controlar su cumplimiento.

Los participantes mencionaron que hay 22 reglas complementarias que describen los controles técnicos para la FPA. Existen redes descentralizadas protegidas por un CERT, filtros, servidores de seguridad [firewall],

sistemas de detección de intrusos (IDS) que utilizan inteligencia artificial para determinar las tendencias, sistemas de respaldo, procesos de respuesta y recuperación ante incidentes, al igual que plataformas para intercambiar inteligencia sobre amenazas con otros sectores interesados. Los participantes mencionaron que el incidente “wannacry” constituye un ejemplo, donde gracias a las plataformas de intercambio de inteligencia sobre las amenazas, pudieron intercambiar información de forma automática sobre software malicioso, reajustar las redes y e intercambiar parches y actualizaciones de software. Finalmente existen criterios de medición para todos los controles y evaluaciones del riesgo que se llevan a cabo con frecuencia.

En el sector privado se entiende que las organizaciones bien establecidas adoptan controles técnicos adecuados que se ajustan a sus redes. Los controles de segmentación de la red y los instrumentos de monitoreo son evidentes en ese sector, al igual que el uso de herramientas de detección de intrusos (IDS) y otras herramientas de gestión de eventos e información de seguridad (SIEM). Algunas organizaciones en particular establecieron un CERT para monitorear sus redes. Sin embargo, es de particular preocupación el hecho de que las organizaciones en el sector privado no estén obligadas a compartir información sobre los incidentes con el CERT nacional y es posible que no recibirán la información de inteligencia sobre amenazas.

En general, los participantes consideran que el nivel de entendimiento e implantación de controles de seguridad en los sectores público y privado es adecuado. Sin embargo, no existen mecanismos para evaluar la efectividad de estos controles en organizaciones específicas, ni procesos para recomendar otras mejoras. Los participantes están de acuerdo en que una sola autoridad debería ser responsable de las decisiones estratégicas sobre controles técnicos y debería promover la adopción de un marco unificado como un conjunto mínimo de controles de seguridad.

### **Resultados del proceso de validación realizado en marzo de 2019:**

La investigación realizada en 2019 confirma ampliamente la evidencia obtenida durante el estudio del CMM de 2018, el cual fue corroborado por los resultados de la investigación documental. Los datos del NIC.br<sup>220</sup> indican que el 93% de las organizaciones del sector público en Brasil realizan copias de respaldo regularmente y el 85% de ellas realizan controles físicos para impedir que personal no autorizado acceda a las instalaciones informáticas.

## D 5.5 - Controles Criptográficos

*Este factor examina el despliegue de técnicas criptográficas en todos los sectores y usuarios para la protección de datos en reposo o en tránsito, y la medida en que estos controles criptográficos cumplen con los estándares y directrices internacionales y se mantienen actualizados.*

### Etapa: **Establecida**

La Infraestructura de Clave Pública de Brasil (ICP-Brasil) es la entidad responsable de garantizar la autenticidad, integridad y validez legal de los documentos en formato electrónico, apoyar aplicaciones y aplicaciones acreditadas mediante certificados digitales y garantizar transacciones electrónicas seguras.<sup>221</sup> ICP-Brasil comprende una serie de autoridades de certificación que prestan diferentes servicios, tales como una autoridad de certificación raíz (Root CA), autoridades de certificación (CA) y autoridades de registro (RA). ICP Brasil ha establecido estándares técnicos para la acreditación de las autoridades de certificación y autoridades de registro, realiza auditorías y supervisa la entidad emisora de certificados raíz (Root CA) y sus proveedores de servicios. Los participantes señalaron que existen requisitos muy estrictos tanto para las entidades emisoras de certificados raíz [Root CA](Nivel 5) como para las autoridades de certificación que proporcionan la Infraestructura de Clave Pública (PKI).

En el gobierno federal, ABIN es el centro de acreditación para el cifrado y proporciona reglas específicas sobre cómo se debe transmitir la información clasificada, define el protocolo de comunicación para la información confidencial (se utiliza PGP) e indica cómo se deben almacenar los datos. Al centrarnos en DATAPREV, ellos utilizan SSH para sus servicios y cifran datos en tránsito, pero no cifran los datos en las bases de información. El uso de correos electrónicos

en código de criptografía es frecuente en DATAPREV, pero esto ha creado problemas con las auditorías. Por lo tanto, para la información no confidencial, no se aconseja el uso de correos electrónicos cifrados. Los participantes mencionaron que existe una clave maestra para descifrar la información con fines de auditoría. Con respecto al sector privado, se pueden hacer observaciones similares. El cifrado se considera principalmente para sistemas críticos, tanto para datos en tránsito como para datos almacenados. No pudimos obtener una imagen clara de si los proveedores de servicios web ofrecen conexiones SSH entre servidores y navegadores web.

### **Resultados del proceso de validación realizado en marzo de 2019:**

La importancia de la criptografía ha sido reconocida por las autoridades federales y la Política Nacional para la Seguridad de la Información adoptada a fines de 2018 recomienda su uso.<sup>222</sup> Los participantes de las entrevistas grupales de validación de 2019 señalaron que esta política solo está dirigida a las instituciones públicas federales y debe expandirse a todos los sectores para tener un impacto tangible en la madurez de la capacidad de seguridad cibernética de Brasil. Se espera que esto extienda el uso de la criptografía, que según se informa, aún no se usa ampliamente en todos los sectores críticos.

## D 5.6 - Mercado de Ciberseguridad



*Este factor se refiere a la disponibilidad y el desarrollo de tecnologías y productos de seguros de seguridad cibernética competitivos.*

### Etapa: **Establecida**

El mercado interno de tecnologías de seguridad cibernética en Brasil se encuentra en un nivel establecido de madurez. Existe una amplia gama de productos software de seguridad cibernética desarrollados internamente, tanto por compañías públicas como privadas. Los participantes mencionaron que algunas de estas tecnologías se exportan y se utilizan en otros países. Asimismo, existe menor dependencia de las tecnologías de seguridad cibernética extranjeras. De acuerdo con los participantes, la prevalencia de piratas informáticos (hackers) en Brasil ha derivado en una demanda cada vez mayor de productos de ciberseguridad. Para satisfacer la demanda, las compañías locales desarrollan y ofrecen soluciones para software de seguridad nacionales. Un factor importante para el mercado interno establecido es la falta de legislación que proteja la propiedad intelectual, lo cual hace que las organizaciones extranjeras se muestren renuentes a desplegar sus soluciones de software en Brasil por temor a los robos de propiedad intelectual.

El mercado de los seguros cibernéticos en Brasil se encuentra en un nivel de madurez formativo. Hay una variedad de pólizas y la demanda de las organizaciones está aumentando. Por lo


general, las pólizas detallan las situaciones en las que el seguro es válido y, como observación positiva, especifican pautas de seguridad con las que las organizaciones deben cumplir para ser asegurables. Un pequeño número de participantes señaló que sus organizaciones están cubiertas para casos de incidentes cibernéticos específicos.

Los participantes estuvieron de acuerdo en que es beneficioso para todas las organizaciones obtener un seguro cibernético; como ellos señalaron, el costo de un solo incidente justifica el gasto. Además, destacaron el apoyo ofrecido durante incidentes y específicamente el análisis forense, el cual es muy valioso.

### **Resultados del proceso de validación realizado en marzo de 2019:**

**En 2019 el taller de validación confirmó ampliamente los resultados del informe CMM del 2018**

## D 5.7 - Divulgación Responsable



*Este factor explora el establecimiento de un marco de divulgación responsable para la recepción y difusión de información sobre la vulnerabilidad en todos los sectores y, en caso de existir la capacidad suficiente, revisar y actualizar continuamente este marco.*

### Etapa: **Establecida**

Los participantes concluyeron que la divulgación responsable varía entre los sectores, alcanzando la FPA un grado de madurez establecido con la presencia de algunos indicadores de nivel estratégico. En mercado contrate, los gobiernos estatales y el sector privado se encuentran en la etapa formativa de madurez.

Más específicamente, la PFA cuenta con un marco de divulgación de vulnerabilidades. Las organizaciones han establecido procesos formales para difundir información automáticamente y el CERT nacional recibe esta información y realiza informes completos sobre cómo abordar los incidentes. Se presentaron casos, como el evento “wannacry”, donde los detalles técnicos y los parches se compartieron de manera oportuna con todas las partes interesadas pertinentes, las cuales pudieron analizar automáticamente la información y actuar para proteger sus redes.

Por el contrario, las organizaciones privadas están excluidas del intercambio de información de inteligencia sobre amenaza del Gobierno.

Además, no están obligadas a informar sobre incidentes, por lo que tienden a ocultar cualquier problema que detecten. Teniendo en cuenta el hecho de que Brasil ha comenzado a privatizar áreas críticas de la infraestructura nacional, los participantes instaron al Gobierno a reconocer el importante papel desempeñado por las organizaciones privadas en la estrategia nacional de seguridad cibernética y a darles acceso a los sistemas de inteligencia de amenazas.

Finalmente, existen varios medios para que los ciudadanos denuncien incidentes, ya sea a través de la policía estatal (cuya madurez, sin embargo, no es comparable a la de la Policía Federal) o a través de sitios web. Existen canales de comunicación dedicados en el sector bancario para que los clientes denuncien fraudes en línea y varias organizaciones públicas, como SERPRO, brindan orientación sobre cómo defenderse de las amenazas, a través de las redes sociales, programas de radio y periódicos.

# Recomendaciones

Luego de la información presentada sobre la revisión de la madurez de los estándares, organizaciones y tecnologías de seguridad cibernética, se presenta el siguiente conjunto de recomendaciones para Brasil. Estas recomendaciones tienen como objetivo asesorar y señalar los pasos a seguir para mejorar la capacidad de la seguridad cibernética actual, de conformidad con las consideraciones del CMM del Centro.

## Adhesión a los estándares

### R 5.1

Adoptar estándares y buenas prácticas de referencia, acordados a nivel nacional, relacionados con la seguridad cibernética en los sectores público y privado, incluidos los estándares de adquisición y desarrollo de software;

### R 5.2

establecer o asignar una institución responsable para la implementación, auditoría y medición del éxito de las normas en los sectores público y privado. Aplicar criterios de medición para controlar el cumplimiento y establecer auditorías periódicas;

### R 5.3

promover debates sobre la forma en que las organizaciones gubernamentales y privadas pueden utilizar los estándares y las buenas prácticas para abordar el riesgo dentro de las cadenas de suministro de la infraestructura crítica. Identificar y exigir estándares a los que debe adherirse la infraestructura crítica.;

### R 5.4

identificar un conjunto mínimo de controles para todos los departamentos gubernamentales (incluido el gobierno estatal) basándose en evaluaciones anuales e información de inteligencia sobre amenazas del CERT nacional, y establecer una revisión de controles para evaluar la efectividad de los controles y prácticas actuales;

### R 5.5

establecer requisitos obligatorios para el cumplimiento de los estándares mediante el nombramiento de agentes de la seguridad que se encargarán de su implementación;

### R 5.6

promulgar legislación para permitir la aplicación de medidas disciplinarias por violaciones de las políticas;

### R 5.7

agilizar una guía clara para la adquisición de hardware y software teniendo en cuenta los estándares que atienden a la ciberseguridad;

### R 5.8

promover la sensibilización e implementación de estándares entre las PYME; y

### **R 5.9**

establecer un marco para evaluar la efectividad de los estándares para la adquisición y el desarrollo de software.

## **Internet Infrastructure Resilience**

### **R 5.10**

Mejorar la coordinación y la colaboración con respecto a la resiliencia de la infraestructura de Internet en los sectores público y privado;

### **R 5.11**

realizar evaluaciones periódicas de los procesos, de conformidad con los estándares y directrices internacionales, junto con la evaluación de la seguridad de la infraestructura nacional de la información y los servicios críticos que impulsan la inversión en nuevas tecnologías;

### **R 5.12**

identificar y mapear posibles puntos de falla crítica dentro de la infraestructura de Internet; y

### **R 5.13**

identificar y mapear posibles puntos de falla crítica dentro de la infraestructura de Internet; y establish a system to formally manage the national infrastructure, with documented processes, roles and responsibilities, and adequate redundancy.

## **Calidad del software**

### **R 5.14**

Desarrollar un catálogo de plataformas y aplicaciones de software seguras dentro de los sectores público y privado;

### **R 5.15**

desarrollar un inventario de software y aplicaciones utilizados en el sector público y en la infraestructura crítica;

### **R 5.16**

desarrollar políticas y procesos sobre actualizaciones y mantenimiento de software y aplicarlos para las infraestructuras públicas en el sector público y privado;

### **R 5.17**

recopilar y evaluar pruebas de deficiencias en la calidad del software con respecto a su impacto en la utilidad y el rendimiento;

### **R 5.18**

establecer o asignar una institución para obtener, de manera estratégica, requisitos comunes para la calidad y funcionalidad del software en todos los sectores públicos y privados; y

### **R 5.19**

supervisar y evaluar la calidad del software utilizado en los sectores público y privado.

## Controles técnicos de seguridad

### R 5.20

Establecer capacitación frecuente para los empleados en tecnologías de la información (TI);

### R 5.21

instar a los ISP y a los bancos a que ofrezcan ofrecer servicios antimalware y antivirus;

### R 5.22

establecer criterios de medición para medir la efectividad de los controles técnicos en el dominio público (incluido el gobierno estatal) y aconsejar al sector privado que adopte estos criterios de medición;

### R 5.23

desarrollar procesos para razonar sobre la adopción de más controles técnicos basados en metodologías de evaluación de riesgos en todo el dominio público;

### R 5.24

promover las mejores prácticas en ciberseguridad para los usuarios;

### R 5.25

designar una autoridad responsable de las decisiones estratégicas sobre los controles técnicos que supervisará todas las redes, de extremo a extremo, y promoverá la adopción de un marco unificado para los controles de seguridad;

### R 5.26

controles técnicos de seguridad profundos actualizados dentro de los sectores público y privado, controlar su efectividad y revisarlos periódicamente; y

### R 5.27

realizar regularmente pruebas de penetración para la protección de los sectores público y privado.

## Controles criptográficos

### R 5.28

Fomentar el desarrollo y la difusión de controles criptográficos en todos los sectores y usuarios para la protección de datos almacenados y en tránsito, de acuerdo con los estándares y directrices internacionales;

### R 5.29

sensibilizar al público sobre los servicios de comunicación seguros, tales como los correos electrónicos cifrados / firmados;

### R 5.30

sensibilizar al público sobre los servicios de comunicación seguros, tales como los correos electrónicos cifrados / firmados;



### **R 5.31**

establecer o asignar una institución responsable para el el diseño de una política que evaluará el despliegue de controles criptográficos de acuerdo con sus objetivos y prioridades dentro del sector público y privado.

## **Mercado de ciberseguridad**

### **R 5.32**

Ampliar la colaboración con el sector privado y el sector académico en relación con la investigación y el desarrollo del desarrollo tecnológico de la ciberseguridad;

### **R 5.33**

Promover el intercambio de información y mejores prácticas entre las organizaciones, para explorar posibles coberturas de seguros.

## **Divulgación responsable**

### **R 5.34**

Desarrollar un marco o política responsable de divulgación de vulnerabilidades dentro del sector público y facilitar su adopción en el sector privado, con inclusión de una fecha límite de divulgación, una resolución programada y un informe de reconocimiento;

### **R 5.35**

establecer o asignar una institución responsable para supervisar el proceso de divulgación responsable y garantizar que las organizaciones no oculten información de vulnerabilidad;

### **R 5.36**

rediseñar el sistema actual que facilita el intercambio de inteligencia sobre amenazas entre los socios de infraestructura crítica para incluir el sector privado y el servicio civil. Promover el intercambio de información sobre amenazas e incentivar a las empresas privadas a participar activamente;

### **R 5.37**

promover los mecanismos de notificación de incidentes existentes en el sector público;

### **R 5.38**

definir umbrales y requisitos de notificación para todos los sectores. Estos requisitos no solo deben considerar la disponibilidad de servicios, sino también la integridad y confidencialidad de los datos, y

### **R 5.39**

acordar instrucciones claras sobre cómo intercambiar información de manera uniforme dentro de otros países de la región de América Latina y el Caribe (LAC) (y no solamente) de manera formal y estructurada.

# Reflexiones adicionales

Aunque el nivel de participación de las partes interesadas en la revisión fue más limitado de lo que hubiéramos esperado, lo que limita la integridad de la evidencia en algunas áreas, la representación y composición de los grupos de partes interesadas fue, en general, equilibrada y amplia.

La revisión del Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM) de 2018 fue el vigésimo tercer estudio de país que hemos apoyado directamente.

El taller de revisión y validación de 2019 fue el primer intento de los investigadores del Centro Global de Capacidad en Seguridad Cibernética (GCSCC) para buscar la confirmación de los resultados del estudio inicial e investigar los cambios en la madurez de la capacidad en seguridad cibernética de una nación. Aunque no se detectaron cambios importantes en la madurez, la actividad de validación se considera útil.



OEA Más derechos para más gente

### Global Cyber Security Capacity Centre

Department of Computer Science, University of Oxford  
Wolfson Building, Oxford OX1 3QD,  
United Kingdom

Teléfono: +44 (0)1865 287434

Correo electrónico: [cybercapacity@cs.ox.ac.uk](mailto:cybercapacity@cs.ox.ac.uk)

Página Web: [www.oxfordmartin.ox.ac.uk/cyber-security](http://www.oxfordmartin.ox.ac.uk/cyber-security)

Portal con capacidad de seguridad cibernética: [www.sbs.ox.ac.uk/cybersecurity-capacity](http://www.sbs.ox.ac.uk/cybersecurity-capacity)

DERECHOS DE AUTOR (2020) Organización de los Estados Americanos.

Todos los derechos reservados bajo las Convenciones Internacional y Panamericana. Ninguna parte del contenido de este material podrá reproducirse o transmitirse de ninguna forma, ni por ningún medio electrónico o mecánico, en su totalidad o en parte, sin el consentimiento expreso de la Organización.

Preparado y publicado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo ([cybersecurity@oas.org](mailto:cybersecurity@oas.org)).

Los contenidos expresados en este documento se presentan exclusivamente con fines informativos y no representan la opinión oficial o la posición de la Organización de los Estados Americanos, su Secretaría General o sus Estados Miembros.

Esta publicación ha sido posible gracias al apoyo financiero de UKFCO y su Programa de Acceso Digital.

# Referencias

1. "Cybersecurity Capacity Maturity Model for Nations" (CMM), Revised Edition, <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition> (consultado el 25 de febrero de 2018).
2. "Estrategia de seguridad de la información y las comunicaciones y seguridad cibernética de la Administración Pública Federal 2015-2018", Oficina de Seguridad Institucional de la Presidencia de la República Secretaría Ejecutiva del Departamento de Seguridad de la Información y las Comunicaciones, 2015, [http://dsic.planalto.gov.br/legislacao/4\\_Estrategia\\_de\\_SIC.pdf](http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf) (consultado el 29 de julio de 2018).
3. National Cybersecurity Strategy, 2020, Federal Decree No. 10.222, <http://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419> (consultado el 16 de abril de 2020).
4. Algunos se llaman CSIRT y otros CERT.
- 5 "Sobre CERT br, <https://www.cert.br/about/> (consultado el 1 de junio de 2020).
6. <http://www.inhope.org/gns/our-members/Brazil.aspx>; <http://new.safernet.org.br/> (consultado el 7 de mayo de 2019).
7. <http://www.pf.gov.br/> (consultado el 7 de mayo de 2019).
8. <http://www.disque100.gov.br> (consultado el 7 de mayo de 2019).
9. INHOPE Association-SaferNet Brazil, <https://www.inhope.org/EN/become-a-partner> (consultado 14 Julio 2018).
10. SaferNet Brazil, <http://new.safernet.org.br/content/o-que-fazemos> (consultado el 14 de julio de 2018).
11. Brazilian Network Information Centre (NIC.br), Available at <https://www.nic.br/who-we-are/> (consultado el 14 de julio de 2018).
12. Antispam.br, <http://www.antispam.br/> (consultado el 14 de julio de 2018).
13. InternetSegura.br, <https://www.internetsegura.br/> (consultado el 14 de julio de 2018).
14. CGI.br, <https://www.cgi.br/about/> (consultado el 14 de julio de 2018)
15. J. L. Marciano, "Applying COBIT in a Government Organization," ResearchGate, April 2015, <https://www.researchgate.net/publication/275638852> (consultado el 13 de julio de 2018).
16. Cyber Crimes Act (Law No. 12,737/2012), también conocida como la "Ley Carolina Dieckmann", [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2012/Lei/L12737.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm) (consultado el 14 de mayo de 2018).
17. Marco de Derechos Civiles Brasileños para Internet, Ley 12.965, 23 de abril de 2014, establece los principios, garantías, derechos y deberes para el uso del Internet en Brasil - Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204), [bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/brazilian\\_framework\\_%20internet.pdf?sequence=1](http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/brazilian_framework_%20internet.pdf?sequence=1) Brazilian Civil Framework of the Internet in English (consultado el 14 de abril de 2018).
18. Constitution of the Federative Republic of Brazil, 1998, <http://english.tse.jus.br/arquivos/federal-constitution> (consultado el 14 de mayo de 2018).
19. Penal Code 1940, Decree-Law No. 2.848, 7 December, 1940, [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm) (consultado el 11 de mayo de 2018).
20. Consumer Protection Code (Law 8,078/1990) (1990), [https://www.emergogroup.com/sites/default/files/file/lei\\_8.078\\_1990\\_consumer\\_protection\\_code.pdf](https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf) (consultado el 14 de mayo de 2018).
21. Janice K. Song, "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying", World Bank, 2015; License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), [https://www.icmec.org/wpcontent/uploads/2015/10/Protecting\\_Children\\_from\\_Cybercrime\\_\\_Legislative\\_Responses\\_in\\_Asia\\_to\\_Fight\\_Child\\_Pornography\\_\\_Online\\_Grooming\\_\\_and\\_Cyberbullying\\_2015.pdf](https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf) (consultado el 16 de junio de 2018).
22. Law on Copyright and Neighbouring Rights, 1998, (Law No. 9.610), [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=125393](http://www.wipo.int/wipolex/en/text.jsp?file_id=125393) (consultado el 14 de junio de 2018).
23. Rafael Mendes Loureiro and Leonardo A F Palhares, "Cybersecurity - Brazil. Getting the Deal Through", Law Business Research Ltd., <https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/> (consultado el 14 de junio de 2018).
24. Ministerio de Relaciones Exteriores, Proceso de adhesión al Convenio de Budapest - Joint Note by the Ministry of Foreign Affairs and the Ministry of Justice and Public Security, Note 309, 2019, <http://www.itamaraty.gov.br/en/press-releases/21149-accession-process-to-the-budapest-convention-joint-note-by-the-ministry-of-foreign-affairs-and-the-ministry-of-justice-and-public-security> (consultado el 15 de abril de 2020).
25. Ministry of Justice and Public Security, Ministry of Justice and Public Security co-ordinates integrated operation against sexual abuse and sexual exploitation committed through the internet, 2019, <https://www.justica.gov.br/news/collective-nitf-content-1553775485.52> (consultado el 15 de abril de 2020).

26. Law No. 13,844, June 2019, establishing the basic organisation of the organs of the Presidency of the Republic and the Ministries, [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/L13844.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm) (consultado el 15 de abril de 2020).
27. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, <https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf> (consultado el 14 de abril de 2018).
28. Ver Cybersecurity Capacity Maturity Model for Nations" (CMM), Revised Edition, <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition> (consultado el 7 de mayo de 2019).
29. Publicaciones pertinentes: M. Williams, Making sense of social research (London: Sage Publications Ltd. 2003), doi: 10.4135/9781849209434; J. Knodel, "The design and analysis of focus group studies: A practical approach", in D. L. Morgan, Successful focus groups: Advancing the state of the art (SAGE Focus Editions 1993) 35-50; Thousand Oaks, CA: SAGE Publications Ltd., doi: 10.4135/9781483349008; R. A. Krueger, and M. A. Casey, Focus groups: A practical guide for applied research (London: Sage Publications Ltd. 2009).
30. Publicaciones pertinentes: J. Kitzinger, "The methodology of focus groups: the importance of interaction between research participants", *Sociology of Health & Illness*, 16(1) (1994), 103-121; J. Kitzinger, 'Qualitative research: introducing focus groups', *British Medical Journal*, 311(7000) (1995), 299- 302; E. F. Fern, 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality', *Journal of Marketing Research*, Vol. 19, No. 1 (1982), 1-13.
31. J. Kitzinger, 'Qualitative research: introducing focus groups', *British Medical Journal*, 311(7000) (1995), 299-302.
32. K. Krippendorff, *Análisis de contenido: Introducción a su metodología* (Sage Publications Inc., 2004). H. F. Hsieh and S. E. Shannon, "Three approaches to qualitative content analysis", *Qualitative Health Research*, 15(9) (2005), 1277-1288; K. A. Neuendorf, *The Content Analysis Guidebook* (Sage Publications Inc., 2002).
33. E. F. Fern, "The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality", *Journal of Marketing Research*, Vol. 19, No. 1 (1982), 1-13, 1982.
34. S. Elo and H. Kyngas, "The qualitative content analysis process", *Journal of Advanced Nursing*, 62(1) (2008), 107-115; H. F. Hsieh and S. E. Shannon, "Three approaches to qualitative content analysis," *Qualitative Health Research*, 15(9) (2005), 1277-1288.
35. P. D. Barbara Downe-Wamboldt RN, "Análisis de contenido: Método, aplicaciones, y problemas", *Health Care for Women International*, 13(3) (1992), 313-321.
36. I. Dey, *Análisis de datos cualitativos: A user-friendly guide for social scientists* (London: Routledge, 1993).
37. <https://cetic.br/noticia/acesso-a-internet-por-banda-larga-volta-a-crescer-nos-domicilios-brasileiros/> (accessed 7 Mayo 2019).
38. <https://www.itu.int/net4/ITU-D/idi/2017/index.html> (accessed 7 Mayo 2019).
39. <http://reports.weforum.org/global-competitiveness-index-2017-2018/countryeconomy-profiles/#economy=BRA> (accessed 7 Mayo 2019).
40. [https://ww2.frost.com/files/5515/2878/9339/Digital\\_Market\\_Overview\\_FCO\\_Brazil\\_25May18.pdf](https://ww2.frost.com/files/5515/2878/9339/Digital_Market_Overview_FCO_Brazil_25May18.pdf) (consultado el 7 de mayo de 2019).
41. Ibid.
42. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, <https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf> (consultado el 7 de mayo de 2019).
43. Brazil 2022, Presidencia da República Secretaria De Assuntos Estratégicos, 2010.
44. Livro Verde: Segurança Cibernética no Brasil, Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações, Brasília, 2010, [http://dsic.planalto.gov.br/legislacao/1\\_Livro\\_Verde\\_SEG\\_CIBER.pdf/view](http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf/view) (accessed 29 Julio 2018).
45. National Strategy of Defence, Ministry of Defence, 2012, [http://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2008/Decreto/D6703.htm](http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm) (accessed 29 Julio 2018).
46. "Estrategia de seguridad de la información y las comunicaciones y seguridad cibernética de la Administración Pública Federal 2015-2018", Oficina de Seguridad Institucional de la Presidencia de la República Secretaría Ejecutiva del Departamento de Seguridad de la Información y las Comunicaciones, 2015, [http://dsic.planalto.gov.br/legislacao/4\\_Estrategia\\_de\\_SIC.pdf](http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf) (consultado el 29 de julio de 2018).
47. El documento Estrategia no está traducido al inglés y utilizamos los servicios de traducción de Google.
48. <http://www2.planalto.gov.br/conheca-a-presidencia/ministros> (consultado el 7 de mayo de 2019).
49. Article 19, "Brazil: Cyber-security strategy", 2016; G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil", 2014, Strategic Paper.
50. <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23> (consultado el 7 de mayo de 2019).
51. Ibid., Art. 5.
52. Ibid., Art. 6.
53. <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23> art 6 (consultado el 7 de mayo de 2019).

54. National Cybersecurity Strategy, 2020, Federal Decree No. 10.222, <http://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419> (consultado el 16 de abril de 2020).
55. OneTrust Data Guidance, "Brazil: President approves national cybersecurity strategy", 2020, <https://platform.dataguidance.com/news/brazil-president-approves-national-cybersecurity-strategy> (consultado el 16 de abril de 2020).
56. Ibid..
57. Law No. 13,844, June 2019, establishing the basic organisation of the organs of the Presidency of the Republic and the Ministries, [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/L13844.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm) (consultado el 15 de abril de 2020).
58. Image from <https://www.cert.br/csirts/brazil/> (accessed 7 Mayo 2019).
59. Núcleo de Informação e Coordenação do Ponto BR, <https://bcp.nic.br/> (consultado el 7 de mayo de 2019).
60. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, <https://cartilha.cert.br/> (consultado el 7 de mayo de 2019).
61. Brazilian Computer Security and Incident Response Teams, <https://www.cert.br/csirts/brazil/> (consultado el 7 de mayo de 2019).
62. Cristine Hoepers, "Incident Handling in Brazil," 2010, <https://www.cert.br/docs/palestras/certbr-certpt2010.pdf> 12 (consultado el 7 de mayo de 2019).
63. Lucimara Desiderá, "Incident Handling in High Profile International Events: Lessons Learned and the Road Ahead", 2016, <https://www.cert.br/docs/palestras/certbr-tcfirst-praga2016.pdf> (consultado el 7 de mayo de 2019).
64. Cristine Hoepers, "Evolution of the Scenario of Incidents in Brazil", 2018, <https://www.cert.br/docs/palestras/certbr-oas2018.pdf> 21 (consultado el 7 de mayo de 2019).
65. Ibid..
66. Brazilian Computer Security and Incident Response Teams, Spampots Project, <https://honeytarg.cert.br/spampots/> (consultado el 7 de mayo de 2019)
67. Department of Information Security, [http://dsic.planalto.gov.br/legislacao/2\\_Guia\\_SICI.pdf/view](http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view) (consultado el 7 de mayo de 2019)
68. <http://www.planejamento.gov.br/assuntos/orcamento-1/orcamentos-anuais/2018/legislacao/alteracoes/lei-no-13-749-de-22-de-novembro-de-2018.pdf> (consultado el 7 de mayo de 2019).
69. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil", Strategic Paper, 2014.
70. [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2015/Decreto/D8491.htm#art2](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8491.htm#art2) (consultado el 7 de mayo de 2019).
71. <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23> art 6 (consultado el 7 de mayo de 2019).
72. [https://www.defesa.gov.br/arquivos/estado\\_e\\_defesa/END-PND\\_Optimized.pdf](https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf) 93-95 (consultado el 7 de mayo de 2019).
73. <http://www.serpro.gov.br/> (consultado el 7 de mayo de 2019).
74. CIG-IPSOS "Global Survey on Internet Security and Trust" (2018 Poll, "Part 1: Privacy, Security, Access and Trust").
75. [https://gvpesquisa.fgv.br/sites/gvpesquisa.fgv.br/files/arquivos/meirelles\\_-\\_information\\_technology\\_and\\_egovernment\\_in\\_brazil\\_.pdf](https://gvpesquisa.fgv.br/sites/gvpesquisa.fgv.br/files/arquivos/meirelles_-_information_technology_and_egovernment_in_brazil_.pdf) (consultado el 7 de mayo de 2019).
76. <https://www.bb.com.br/pbb/pagina-inicial/bb-seguranca/dicas-de-seguranca#/> (consultado el 7 de mayo de 2019).
77. <https://www.itau.com.br/seguranca/> (consultado el 7 de mayo de 2019).
78. <http://www.planejamento.gov.br/EGD/arquivos/revisao-da-estrategia-de-governanca-digital-2015-2019.pdf> (consultado el 7 de mayo de 2019).
79. <https://principios.cgi.br/> (consultado el 7 de mayo de 2019).
80. "Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector", OECD, 2018.
81. See e.g. <http://www.ejeg.com/issue/download.html?idArticle=417147>; [https://www.cetic.br/media/docs/publicacoes/2/TIC\\_eGOV\\_2017\\_livro\\_eletronico.pdf](https://www.cetic.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf) 219 (consultado el 7 de mayo de 2019).
82. [https://www.ctir.gov.br/arquivos/alertas/2018/ALERTA\\_CTIRGOV\\_2018\\_03\\_SQL\\_Injection.pdf](https://www.ctir.gov.br/arquivos/alertas/2018/ALERTA_CTIRGOV_2018_03_SQL_Injection.pdf) (consultado el 7 de mayo de 2019).
83. [https://www.cetic.br/media/docs/publicacoes/2/tic\\_dom\\_2017\\_livro\\_eletronico.pdf](https://www.cetic.br/media/docs/publicacoes/2/tic_dom_2017_livro_eletronico.pdf) 253 & 333 (consultado el 7 de mayo de 2019).
84. See e.g. <https://www.kabum.com.br/cgi-local/site/institucional/politicas.cgi> (consultado el 7 de mayo de 2019).
85. See e.g. <https://www.magazineluiza.com.br/estaticas/seguranca-maxima/> (consultado el 7 de mayo de 2019).
86. <https://nic.br/media/docs/publicacoes/13/fasciculo-comercio-eletronico.pdf> (consultado el 7 de mayo de 2019).

87. CIGI-IPSOS “Global Survey on Internet Security and Trust” (2018 Poll, “Part 2: E-commerce”) <https://www.cigionline.org/internet-survey-2018> (consultado el 7 de mayo de 2019).
88. <https://www1.folha.uol.com.br/mercado/2018/07/senado-aprova-projeto-sobre-protexcao-de-dados-pessoais.shtml>; [g1.globo.com/jornal-nacional/noticia/2018/07/comissao-do-senado-aprova-projeto-de-lei-de-protexcao-de-dados-pessoais.html](http://g1.globo.com/jornal-nacional/noticia/2018/07/comissao-do-senado-aprova-projeto-de-lei-de-protexcao-de-dados-pessoais.html) (accessed 7 Mayo 2019); <https://www.cartacapital.com.br/sociedade/entenda-o-que-muda-com-a-nova-lei-de-protexcao-de-dados> (consultado el 7 de mayo de 2019).
89. <http://www.inhope.org/gns/our-members/Brazil.aspx>, <http://new.safernet.org.br/> (consultado el 7 de mayo de 2019).
90. <http://www.pf.gov.br/> (consultado el 7 de mayo de 2019).
91. <http://www.disque100.gov.br> (consultado el 7 de mayo de 2019).
92. <http://www.caixa.gov.br/site/english/About-Caixa/Paginas/default.aspx> (consultado el 7 de mayo de 2019).
93. <http://www.bcb.gov.br/en#!/home> (consultado el 7 de mayo de 2019).
94. <http://g1.globo.com/tecnologia/noticia/2016/02/facebook-cria-central-de-prevencao-ao-bullying-no-brasil.html> (consultado el 7 de mayo de 2019).
95. SaferNet Brazil, <http://new.safernet.org.br/content/o-que-fazemos> (consultado 14 de julio de 2018).
96. INHOPE Association, SaferNet Brazil, <http://www.inhope.org/gns/our-members/Brazil.aspx> (consultado 14 de julio de 2018).
97. Hotline, <http://new.safernet.org.br/denuncie> (consultado 14 de julio de 2018).
98. SaferNet Brazil, <http://new.safernet.org.br/content/o-que-fazemos> (consultado 14 de julio de 2018).
99. SaferNet Brazil partnership with Google Brazil, <http://www.safernet.org.br/site/institucional/parcerias/google> (consultado 14 de julio de 2018).
100. CGI.br, <https://www.cgi.br/about/> (consultado 14 de julio de 2018).
101. Brazilian Network Information Centre (NIC.br), <https://www.nic.br/who-we-are/> (consultado 14 de julio de 2018).
102. Antispam.br, <http://www.antispam.br/> (consultado 14 de julio de 2018).
103. InternetSegura.br, <https://www.internetsegura.br/> (consultado 14 de julio de 2018).
104. CERT.br “Team Update: New Awareness Materials”, 2017, <https://www.cert.br/docs/palestras/certbr-natcsirts2017-2.pdf> (consultado 12 de julio de 2018).
105. Ministerio Público Federal, Em parceria com Safernet, MPF debate segurança e bom uso da internet com educadores pessoais, 2015, <http://pfdc.pgr.mpf.mp.br/informativos/edicoes-2015/dezembro/em-parceria-com-safernet-mpf-debate-seguranca-e-bom-uso-da-internet-com-educadores-pessoais> (consultado el 10 de septiembre de 2018).
106. Federation of Industry of the State of Sao Paulo (FIESP) <http://www.fiesp.com.br/?temas=seguranca> (consultado el 10 de septiembre de 2018).
107. Brasscom, <https://brasscom.org.br/events/forum-nacional-seguranca-cibernetica-nas-instituicoes-financeiras-impactos-da-resolucao-no-4-658/> (consultado el 10 de septiembre de 2018).
108. <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23> (consultado el 7 de mayo de 2019).
109. See Footnote 94.
110. Ministry of Education, Catálogo Nacional dos Cursos Superiores de Tecnologia, <http://portal.mec.gov.br/catalogo-nacional-dos-cursos-superiores-de-tecnologia-> (consultado el 10 de septiembre de 2018).
111. Ibid.
112. University of Sao Paulo courses, <http://www5.usp.br/english/education/undergraduate/courses-offered/?lang=en> (consultado el 25 de julio de 2018).
113. Federal University of ABC, Computer Science, <http://ufabc.edu.br/en/graduate-program/?id=6> (consultado el 25 de julio de 2018).
114. Ibid...
115. RNP, Cybersecurity Training, <https://esr.rnp.br/seg12> (consultado el 25 de julio de 2018).
116. RNP, International Computer Security Day, <https://disi.rnp.br/en> (consultado el 10 de septiembre de 2018).
117. Senac College, post-graduate course in cyber-defence, <https://www.df.senac.br/faculdade/wp-content/uploads/2018/01/desefa-ciberntica.pdf> (consultado el 25 de julio de 2018).
118. Trend Micro, “The rise of the Brazilian underground”, 2016, <https://blog.trendmicro.com/the-rise-of-the-brazilian-underground/> (consultado el 11 de julio de 2018).

119. Base Nacional Comum, [http://basenacionalcomum.mec.gov.br/wp-content/uploads/2018/04/BNCC\\_EnsinoMedio\\_embaixa\\_site.pdf%20https://www.youtube.com/watch/?v=NT9Whez23gE](http://basenacionalcomum.mec.gov.br/wp-content/uploads/2018/04/BNCC_EnsinoMedio_embaixa_site.pdf%20https://www.youtube.com/watch/?v=NT9Whez23gE) (consultado el 25 de julio de 2018).
120. Division courses taught by CERT.br, <https://www.cert.br/cursos/> (consultado el 14 de julio de 2018).
121. Best Practices Portal (BCP.nic.br) <https://bcp.nic.br/sobre/> (consultado el 14 de julio de 2018).
122. Ibid..
123. ITU, Cyberwellness Profile, Brazil, 2012, [https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country\\_Profiles/Brazil.pdf](https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf) (consultado el 11 de mayo de 2018).
124. CERT.br courses, <https://www.cert.br/cursos/> (accessed 10 September 2018).
125. Cyber Defense Command. <https://ava-enadciber.eb.mil.br/> (consultado el 25 de julio de 2018).
126. Fundação Bradesco, Information Security course, <https://www.ev.org.br/curso/informatica/infraestrutura-de-ti/seguranca-da-informacao?return=/cursos/informatica> (consultado el 25 de julio de 2018).
127. J. L. Marciano, "Applying COBIT in a Government Organization", 2015, [http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Focus-Applying-COBIT-in-a-Government-Organization\\_nlt\\_Eng\\_0415.pdf](http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Focus-Applying-COBIT-in-a-Government-Organization_nlt_Eng_0415.pdf) (consultado el 13 de julio de 2018).
128. Ibid.
129. Federação Brasileira de Bancos, <https://portal.febraban.org.br/> (consultado el 8 de mayo de 2019).
130. Cyber Crimes Act (Law No. 12,737/2012) also known as "Carolina Dieckmann Law", [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2012/Lei/L12737.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm) (accessed 14 May 2018).
131. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishing the principles, guarantees, rights and duties for use of the Internet in Brazil - Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204), [bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian\\_framework\\_%20internet.pdf?sequence=1](http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1) The Brazilian Civil Framework of the Internet in English (accessed 14 April 2018).
132. Diego R. Canabarro and Thiago Borne, "Reflections on the Fog of (Cyber) War", NCDG Policy Working Paper No. 13-002 (2013), <https://www.umass.edu/digitalcenter/sites/default/files/Brazil%20and%20The%20Fog%20of%20%28Cyber%29War.pdf> (consultado el 11 de mayo de 2018).
133. Ministry of Defence, Cyber Defence Policy, Administrative Normative Rule No. 3,389, 2012, <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2012&jornal=1&pagina=11&totalArquivos=304> (consultado el 11 de mayo de 2018).
134. White Paper on National Defence 2012, [https://www.defesa.gov.br/arquivos/estado\\_e\\_defesa/livro\\_branco/lbdn\\_2013\\_ing\\_net.pdf](https://www.defesa.gov.br/arquivos/estado_e_defesa/livro_branco/lbdn_2013_ing_net.pdf) (consultado el 11 de mayo de 2018).
135. National Defence Strategy Decree 6703, 2008, [http://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2008/Decreto/D6703.htm](http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm) (consultado el 11 de mayo de 2018).
136. Presidency of the Republic, Critical Information and Communication Infrastructure Protection, 2010, [http://dsic.planalto.gov.br/legislacao/2\\_Guia\\_SICI.pdf/view](http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view) (consultado el 11 de mayo de 2018).
137. Anatel - Public Consultation No. 21, "Regulation on the risk management of telecommunications networks and use of telecommunications services in emergency and disaster situations", <https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C1674&Tipo=1&Opcao=finalizadas> (consultado el 11 de mayo de 2018).
138. ITU, Cyberwellness Profile, Brazil, 2012, [https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country\\_Profiles/Brazil.pdf](https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf) (consultado el 11 de mayo de 2018).
139. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review (Fourth Edition, Law Business Research Ltd., 2017).
140. Carolina Dieckmann is a famous Brazilian actress whose email account was hacked and her intimate photos were published on the Internet.
141. Penal Code (1940) Decree-Law No. 2.848, 7 December 1940, [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm) (consultado el 11 de mayo de 2018).
142. S. S. M. Ribeiro, Democracy after the internet: Brazil between facts, norms, and code (Vol. 27, Springer 2016).
143. Ibid.
144. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishing the principles, guarantees, rights and duties for use of the Internet in Brazil. Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204), [bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian\\_framework\\_%20internet.pdf?sequence=1](http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1) Brazilian Civil Framework of the Internet in English (consultado el 14 de abril de 2018).
145. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd. 2017).



146. Federal Prosecution Service, technical note about the ETS 185 Convention of the Council of Europe – convention on cybercrime – Budapest convention, Technical note 2nd CCR/SCI No. 1/2018, 2018, <http://www.transparencia.mpf.mp.br/conteudo/servico-de-informacao-ao-cidadao/validacao-de-documentos> (consultado el 14 de junio de 2018).
147. “How to be compliant with Brazil’s Data Protection Act”, IAPP, 2018, [https://iapp.org/news/a/how-tobecompliantwithbrazilsdataprotectionact/?mkt\\_](https://iapp.org/news/a/how-tobecompliantwithbrazilsdataprotectionact/?mkt_) (consultado el 10 de septiembre de 2018).
148. Constitution of the Federative Republic of Brazil, 1998, <http://english.tse.jus.br/arquivos/federal-constitution> (consultado el 14 de mayo de 2018).
149. Penal Code (Decree-Law No. 2.848, 7 December 1940) (1940) [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm) (consultado el 11 de mayo de 2018).
150. Consumer Protection Code (Law 8,078/1990) (1990) [https://www.emergogroup.com/sites/default/files/file/lei\\_8.078\\_1990\\_consumer\\_protection\\_code.pdf](https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf) (consultado el 14 de mayo de 2018).
151. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishing the principles, guarantees, rights and duties for use of the Internet in Brazil. Brasília: Chamber of Deputies, Edições Câmara, 2016, (Série legislação; No. 204), [bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian\\_framework\\_%20internet.pdf?sequence=1](http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1) Brazilian Civil Framework of the Internet in English (consultado el 14 de abril de 2018).
152. “Brazil president approves data protection bill – but vetoes key accountability measures”, Accessnow, 2018, <https://www.accessnow.org/brazil-president-approves-data-protection-bill-but-vetoes-key-accountability-measures/> (consultado el 10 de septiembre de 2018).
153. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd., 2017).
154. C. Barbosa, P. Vilhena, K. L. Advogados, “Data protection in Brazil: overview”, Practical Law, Global Guide 2016-17, 2016, [https://uk.practicalaw.thomsonreuters.com/4-5201732?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk](https://uk.practicalaw.thomsonreuters.com/4-5201732?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk) (consultado el 14 de junio de 2018).
155. Brazilian Civil Code, 2002, [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=226198](http://www.wipo.int/wipolex/en/text.jsp?file_id=226198) (consultado el 14 de junio de 2018).
156. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity – Brazil. Getting the Deal Through (Law Business Research Ltd.) <https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/> (consultado el 14 de junio de 2018).
157. Law on Copyright and Neighbouring Rights, Law No. 9.610, 1998, [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=125393](http://www.wipo.int/wipolex/en/text.jsp?file_id=125393) (consultado el 14 de junio de 2018).
158. Hunton Andrews Kurth, “Brazil’s Senate Passes General Data Protection Law”, 2018, <https://www.huntonprivacyblog.com/2018/07/11/brazils-senate-passes-general-data-protection-law/> (consultado el 10 de septiembre de 2018).
159. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity – Brazil. Getting the Deal Through (Law Business Research Ltd.) <https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/> (consultado el 14 de junio de 2018).
160. Human Rights Watch, World Report 2017, <https://www.hrw.org/world-report/2017/country-chapters/brazil> (consultado el 14 de junio de 2018).
161. Ibid..
162. “Brazil court orders WhatsApp messaging to be suspended”, BBC News, 2015, <https://www.bbc.co.uk/news/world-latin-america-35119235> (consultado el 14 de junio de 2018).
163. W. Connors, “Facebook Executive Arrested in Brazil”, Wall Street Journal, 2016, <https://www.wsj.com/articles/facebook-executive-arrested-in-brazil-1456851506> (consultado el 16 de junio de 2018).
164. Law to combat child pornography online, “Statute of Children and Adolescents, to improve combat the production, sale and distribution of child pornography and criminalize the acquisition and possession of such material and other related behaviors to pedophilia on the internet”, 2008, [https://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2008/lei/111829.htm](https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/111829.htm) (consultado el 16 de junio de 2018).
165. ITU, Cyberwellness Profile, Brazil, 2012, [https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country\\_Profiles/Brazil.pdf](https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf) (consultado el 11 de mayo de 2018).
166. Ibid..
167. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd. 2017).
168. Janice K. Song, “Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying”, World Bank, License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 2015, [https://www.icmec.org/wpcontent/uploads/2015/10/Protecting\\_Children\\_from\\_Cybercrime\\_\\_Legislative\\_Responses\\_in\\_Asia\\_to\\_Fight\\_Child\\_Pornography\\_\\_Online\\_Grooming\\_\\_and\\_Cyberbullying\\_2015.pdf](https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf) (consultado el 16 de junio de 2018).
169. Ibid..
170. ITU, Cyberwellness Profile, Brazil, 2012, [https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country\\_Profiles/Brazil.pdf](https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf) (consultado el 11 de mayo de 2018).

171. Ibid..

172. Law on Copyright and Neighbouring Rights, Law No. 9.610 (1998), [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=125393](http://www.wipo.int/wipolex/en/text.jsp?file_id=125393) (consultado el 14 de junio de 2018).

173. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity - Brazil Getting the Deal Through (Law Business Research Ltd.) <https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/> (consultado el 14 de junio de 2018).

174. Law on Protection of Intellectual Property of Software, its Commercialisation in the Country, and Other Provisions, Law No. 9.609 (1998), <http://www.wipo.int/wipolex/en/details.jsp?id=513> (consultado el 14 de junio de 2018).

175. Internet Act Decree No. 8,771/2016 (2016), <http://www.internetlab.org.br/wp-content/uploads/2016/05/Decree-MarcoCivil-English.pdf> (consultado el 14 de junio de 2018).

176. Ibid..

177. Consumer Protection Code (Law 8,078/1990) (1990) [https://www.emergogroup.com/sites/default/files/file/lei\\_8.078\\_1990\\_consumer\\_protection\\_code.pdf](https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf) (consultado el 14 de mayo de 2018).

178. C. Barbosa, P. Vilhena, and K. L. Advogados, "Data protection in Brazil: overview", Practical Law, Global Guide 2016-17, 2016, [https://uk.practicallaw.thomsonreuters.com/4-5201732?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk](https://uk.practicallaw.thomsonreuters.com/4-5201732?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk) (consultado el 14 de junio de 2018).

179. Data protection and Privacy - Brazil, 2017, Ricardo Barretto Ferreira da Silva and Paulo Branch, "Getting the Deal Through", Law Business Research Ltd., <https://gettingthedealthrough.com/area/52/jurisdiction/6/data-protection-privacy-brazil/> (consultado el 14 de junio de 2018).

180. Ibid..

181. E-commerce - Brazil, 2017, Raphael de Cunto, Pedro Paulo Barradas Barata and Beatriz Landi Laterza Figueiredo, "Getting the Deal Through", <https://gettingthedealthrough.com/area/11/jurisdiction/6/e-commerce-brazil/> (consultado el 14 de junio de 2018).

182. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishing the principles, guarantees, rights and duties for use of the Internet in Brazil. Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204), [bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian\\_framework\\_%20internet.pdf?sequence=1](http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1) Brazilian Civil Framework of the Internet in English (consultado el 14 de abril de 2018).

183. Sexual Harassment Law (No. 13,718) [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Lei/L13718.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm) (consultado el 16 de abril de 2020).

184. Economic Commission for Latin America, Comprehensive National-Level Review Report on the Implementation of the Beijing Declaration and Platform for Action - Brazil, 2019, [https://www.cepal.org/sites/default/files/informe\\_beijing25\\_brasil.pdf](https://www.cepal.org/sites/default/files/informe_beijing25_brasil.pdf) (consultado el 16 de abril de 2020).

185. "Brazilian government approves law that guarantees more protection to women", Government of Brazil, 2018, <http://www.brazil.gov.br/about-brazil/news/2018/09/brazilian-government-approves-law-that-guarantees-more-protection-to-women-1> (consultado el 16 de abril de 2020).

186. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, <https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf> (consultado el 14 de abril de 2018).

187. Ibid..

188. Ibid..

189. "Skills of the Federal Police gain international recognition", Federal Police, 2014, <http://www.pf.gov.br/agencia/noticias/2014/10/pericias-da-policia-federal-ganham-reconhecimento-internacional> (consultado el 10 de septiembre de 2018).

190. Janice K. Song, "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying", World Bank, 2015, license: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), [https://www.icmec.org/wpcontent/uploads/2015/10/Protecting\\_Children\\_from\\_Cybercrime\\_\\_Legislative\\_Responses\\_in\\_Asia\\_to\\_Fight\\_Child\\_Pornography\\_\\_Online\\_Grooming\\_\\_and\\_Cyberbullying\\_2015.pdf](https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf) (consultado el 16 de junio de 2018).

191. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity - Brazil. Getting the Deal Through (Law Business Research Ltd.) <https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/> (consultado el 14 de junio de 2018).

192. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishes the principles, guarantees, rights and duties for use of the Internet in Brazil. Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204), [bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian\\_framework\\_%20internet.pdf?sequence=1](http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1) The Brazilian Civil Framework of the Internet in English (consultado el 14 de abril de 2018).

193. Electronic Frontier Communication, "State Surveillance of Communications in Brazil", [https://necessaryandproportionate.org/files/2016/07/08/brazil\\_faq\\_en.pdf](https://necessaryandproportionate.org/files/2016/07/08/brazil_faq_en.pdf) (consultado el 14 de junio de 2018).

194. Federal Public Ministry, 2014, <http://www.mpf.mp.br/atuacaotematica/ccr2/coordenacao/comissoesegruposdetrabalho/combatecrimesciberneticos/relatorios/Oficio%20PRSP%20GABPRR28MGBAS%2066526%20-%202014.11.12.pdf> (consultado el 10 de septiembre de 2018).

195. Cybercrime@coe Update, Council of Europe, 2018, <https://rm.coe.int/cybercrime-coe-update-2018-q1/16807baf95> (consultado el 14 de junio de 2018).
196. Octopus 2018: Co-operation against Cybercrime, 11-13 July 2018, Council of Europe, Strasbourg, France, <https://www.coe.int/en/web/cybercrime/octopus-interface-2018> (consultado el 14 de julio de 2018).
197. OAS, Cybercrime, <https://www.oas.org/juridico/english/cyber.htm> (consultado el 10 de septiembre de 2018).
198. A. Mari, "Microsoft Brazil to deliver digital crime training program to Public Prosecutor's Office", ZDnet, 2018, <https://www.zdnet.com/article/microsoft-brazil-to-deliver-digital-crime-training-program-to-public-prosecutors-office/> (consultado el 14 de junio de 2018)
199. Ministry of Justice and Public Security, "Ministry of Justice and Public Security co-ordinates integrated operation against sexual abuse and sexual exploitation committed through the internet", 2019, <https://www.justica.gov.br/news/collective-nitf-content-1553775485.52> (consultado el 15 de abril de 2020)
200. Law No. 13,844, June 2019, establishing the basic organisation of the organs of the Presidency of the Republic and the Ministries, [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/L13844.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm) (consultado el 15 de abril de 2020).
201. ITU, Cyberwellness Profile, Brazil, 2012, [https://www.itu.int/en/ITUUD/Cybersecurity/Documents/Country\\_Profiles/Brazil.pdf](https://www.itu.int/en/ITUUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf) (consultado el 11 de mayo de 2018)
202. Ibid..
203. Ibid..
204. FIRST, Cert.br, <https://www.first.org/members/teams/cert-br> (consultado el 11 de mayo de 2018)
205. "INTERPOL and Banco do Brasil S/A sign co-operation agreement against cybercrime", INTERPOL, 2018, <https://www.interpol.int/News-and-media/News/2018/N2018-046> (consultado el 14 de julio de 2018)
206. G. Diniz, R. Muggah, and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, <https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf> (consultado el 14 de abril de 2018).
207. INTERPOL, Brazil, <https://www.interpol.int/Member-countries/Americas/Brazil> (consultado el 14 de julio de 2018).
208. "Today, Brazil and Europol signed an agreement to expand co-operation to combat cross-border criminal activities", Europol, 2017, <https://www.europol.europa.eu/newsroom/news/today-brazil-and-europol-signed-agreement-to-expand-co-operation-to-combat-cross-border-criminal-activities> (consultado el 14 de julio de 2018).
209. [http://dsic.planalto.gov.br/legislacao/2\\_Guia\\_SICI.pdf/view](http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view) (accessed 11 May 2019).
210. <https://www.pcisecuritystandards.org> (consultado el 11 de mayo de 2019).
211. <http://www.mastercard.com/sea/consumer/standard-mastercard.html> (accessed 11 May 2019).
212. <https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf> (consultado el 11 de mayo de 2019).
213. <https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf> (accessed 10 May 2019).
214. <https://cetic.br/noticia/acesso-a-internet-por-banda-larga-volta-a-crescer-nos-domicilios-brasileiros/> (consultado el 11 de mayo de 2019).
215. <http://www.allisps.com/en/offers/BRAZIL> (consultado el 11 de mayo de 2019).
216. <http://www.abranet.org.br/?UserActiveTemplate=site> (consultado el 11 de mayo de 2019).
217. S. H. Bucke Brito, M. A. Silva Santos, R. dos Reis Fontes, D. A. Lachos Perez, H. Lourenço da Silva, and C. R. Esteve Rothenberg, "An Analysis of the Largest National Ecosystem of Public Internet eXchange Points: The Case of Brazil", *Journal of Communication and Information Systems*, 31(1), 2016.
218. <http://ix.br> (consultado el 11 de mayo de 2019).
219. See e.g., Central Bank of Brazil, Resolution CMN 4,658, 26 April, 2018, <https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf> (consultado el 13 de mayo de 2019).
220. CGI.br-NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro - TIC Governo Eletrônico, 2017, <https://www.cetic.br/tics/governo/2017/orgaos/B6/> (accessed 17 May 2019).
221. [http://www.planalto.gov.br/ccivil\\_03/mpv/Antigas\\_2001/2200-2.htm](http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm) (consultado el 13 de mayo de 2019).
222. <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23> (consultado el 7 de mayo de 2019).

**Revisión de capacidades de**  
**Ciberseguridad**

**República Federativa de Brasil**



**Revisión de capacidades de**  
**Ciberseguridad**

**República Federativa de Brasil**



Global  
Cyber Security  
Capacity Centre



OECD Más derechos  
para más gente

# Revisión de capacidades de **Ciberseguridad**

**República Federativa de Brasil**