Capítulo 14

Gestión de riesgos de seguridad digital

Este capítulo se centra en las políticas públicas para gestionar la seguridad digital. En primer lugar se establece la distinción entre la gestión del riesgo de seguridad digital y otros aspectos de ciberseguridad relativos a la tecnología, aplicación de la ley, seguridad nacional y defensa. A continuación se presentan los elementos clave de las estrategias nacionales que pueden crear las condiciones marco para incrementar la confianza de todas las partes interesadas que utilizan TIC y para crear un entorno digital de prosperidad económica y social. También se examinan las herramientas de medición y evaluación de impacto existentes, y se ofrece un panorama general de los esfuerzos de política pública en la región LAC. Por último, se propone una serie de buenas prácticas en este ámbito.

Los datos estadísticos para Israel son proporcionados por y bajo la responsabilidad de las autoridades israelíes competentes. El uso de estos datos por la OCDE es sin perjuicio del estatus de los Altos del Golán, de Jerusalén Este y delos asentamientos israelíes en Cisjordania bajo los términos del derecho internacional.

La banda ancha y las tecnologías de la información y las comunicaciones (TIC) en general se han convertido en un elemento fundamental para el desarrollo y funcionamiento de la economía en muchas áreas de los países de América Latina y el Caribe (LAC), especialmente para infraestructura crítica como energía, transporte, agua, servicios financieros y servicios públicos esenciales. Ahora bien, los beneficios económicos y sociales solo podrán materializarse si las partes interesadas gestionan el riesgo de seguridad digital, es decir, el riesgo de seguridad vinculado al uso del entorno digital.

Aunque muchos países LAC han desarrollado políticas que tratan algunos aspectos de seguridad digital, generalmente no abordan este tema desde una perspectiva estratégica que establezca una línea clara de cara al futuro y, lo que es más importante, no suelen enfocar la política de ciberseguridad como un medio para aumentar la prosperidad económica y social, sino que se centran en los aspectos técnicos y delictivos de la cuestión, o en la seguridad nacional. Las políticas en vigor carecen a menudo de un nivel adecuado de coordinación entre organismos gubernamentales y partes interesadas, lo que socava los esfuerzos de política pública para fomentar el uso de las TIC a raíz de la limitada comprensión de las dimensiones sociales y económicas de la ciberseguridad.

En esta sección se presenta un conjunto de conceptos e instrumentos políticos que ayudan a desarrollar políticas de gestión del riesgo de seguridad digital en aras de lograr la prosperidad económica y social. Se ofrece un panorama general de la situación en la región LAC, se señalan buenas prácticas en los distintos países y se formulan consejos basados en la recomendación de la OCDE de 2015 sobre gestión del riesgo de seguridad digital para la prosperidad económica y social (*Recommendation on Digital Security Risk Management for Economic and Social Prosperity*) (OCDE, 2015a) y en la labor de otros organismos nacionales e internacionales, como el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA).

Principales objetivos de las políticas para la región LAC

El principal objetivo de las ambiciosas políticas encaminadas a adoptar una estrategia nacional de gestión del riesgo de seguridad digital es crear las condiciones marco para el uso de las TIC por todas las partes interesadas y el entorno digital para la prosperidad económica y social. Este objetivo general conlleva el cumplimiento de ciertas metas esenciales:

- **Comprensión de la seguridad digital y de la responsabilidad de los distintos actores en su gestión.** Todas las partes interesadas han de ser conscientes de que el riesgo de seguridad digital puede afectar a su bienestar económico y social, y de que es posible que su gestión de la seguridad digital repercuta en otros actores. Por ello, es necesario que dispongan de instrucción y capacidades para entender el riesgo y gestionarlo. En concreto, deben comprender que la gestión del riesgo de seguridad digital es un desafío económico y social, y no simplemente una cuestión técnica o de seguridad nacional.
- **Desarrollo de una estrategia nacional para la gestión del riesgo de seguridad digital.** Las estrategias nacionales para la gestión del riesgo de seguridad digital deben centrarse en fomentar la prosperidad económica y social. Han de ser fruto de una amplia coordinación

a nivel gubernamental para garantizar su uniformidad con otras estrategias de prosperidad económica y social, y su coherencia con políticas dirigidas a proteger la infraestructura crítica y a garantizar la provisión de servicios esenciales. El objetivo es luchar contra la delincuencia, proteger la seguridad nacional y preservar la estabilidad nacional. Estas estrategias deben contar con apoyo al más alto nivel gubernamental para garantizar un equilibrio adecuado entre los diferentes intereses en juego. Asimismo, han de ser flexibles y tecnológicamente neutras, al tiempo que preservan y protegen los derechos humanos y los valores fundamentales.

- **Colaboración con otras partes interesadas**. Es preciso que los responsables de políticas potencien la participación activa de todos los actores —desde empresas y sociedad civil, a la comunidad técnica de Internet y el mundo universitario— en el desarrollo e implementación de la estrategia y la política.
- **Fomento de la cooperación internacional y la asistencia mutua**. Los responsables de políticas deben establecer relaciones multilaterales y bilaterales para compartir experiencias y buenas prácticas y promover un enfoque de gestión del riesgo de seguridad digital que no incremente el riesgo de otros países.

Herramientas de medición y análisis en la región LAC

Hay un número limitado de referencias relevantes de indicadores clave de rendimiento y mediciones para los responsables de políticas en el ámbito de la gestión del riesgo de seguridad digital. Entre ellas destacan el *Índice Mundial de Ciberseguridad* de la UIT (UIT, 2014), el *Modelo de Madurez de Capacidad de Seguridad Cibernética* del Centro Global de Capacidad sobre Seguridad Cibernética de la Universidad de Oxford (2014), el *Cybersecurity Dashboard* de Business Software Alliance (BSA, 2015) y, en el ámbito de la energía, el *Modelo de Madurez de Capacidad de Seguridad Cibernética* (C2M2) del Departamento de Energía de los Estados Unidos (2015). Ahora bien, estas referencias generalmente enfocan la ciberseguridad como una cuestión técnica y no como un desafío económico y social. Actualmente se trabaja a nivel nacional en algunos países y en foros internacionales para mejorar la base empírica de las políticas públicas en este ámbito. En los documentos que se mencionan a continuación (recuadro 14.1) se ofrecen recomendaciones de la OCDE y ejemplos de buenas prácticas sobre áreas específicas, mediciones de aspectos de seguridad y privacidad en el contexto del acceso a Internet de menores y Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT o CERT, por sus siglas en inglés).

Recuadro 14.1. **Referencias de la OCDE sobre mediciones en el ámbito de la seguridad digital**

OCDE (2012a): *Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges Related to Measuring Information Security, Privacy and the Protection of Children Online*

Este informe ofrece una visión de conjunto de los datos y estadísticas existentes en los ámbitos de seguridad de la información, privacidad y protección de menores en Internet. Hace hincapié en el potencial para desarrollar mejores indicadores en estas áreas y muestra que existe una gran cantidad de datos empíricos que, de extraerse y hacerse comparables, enriquecen la base empírica actual para la formulación de políticas. Tales indicadores ayudan a identificar ámbitos en los que la intervención política está claramente justificada y pueden proporcionar orientaciones para diseñar políticas públicas y determinar su efectividad.

Recuadro 14.1. **Referencias de la OCDE sobre mediciones en el ámbito de la seguridad digital** *(cont.)*

A partir de un ámbito amplio que abarca todos los aspectos de seguridad y privacidad, el informe identifica las áreas en las que se pueden desarrollar mejores indicadores de forma inmediata con recursos mínimos:

- mejorar la relevancia de las encuestas modelo de la OCDE sobre el uso de las TIC por empresas y hogares/personas para responsables de políticas en los ámbitos de la seguridad de la información, la privacidad y, sobre todo, la protección de menores en Internet
- mejorar la comparabilidad entre países de estadísticas proporcionadas por los CSIRT nacionales o gubernamentales en el ámbito de la seguridad de la información, y por las autoridades de protección de la privacidad (autoridades de privacidad) en el ámbito de la privacidad.

OCDE (2015b): ***Guidance for improving the comparability of statistics produced by computer security incident response teams (CSIRTs)***

Los CSIRT generan estadísticas basadas en sus actividades diarias —emisión de alertas y advertencias, tramitación de incidentes, etc.—, pero no suelen ser comparables entre sí a nivel internacional. Entre 2013 y 2015, la OCDE colaboró con la comunidad de CSIRT para analizar cómo mejorar la comparabilidad internacional de dichas estadísticas. El fruto de esta colaboración es una guía que pueden utilizar los CSIRT para elaborar estadísticas comparables en términos más generales y que ha de considerarse un primer paso en este ámbito.

La guía ofrece orientaciones para mejorar la comparabilidad internacional de las estadísticas generadas por los CSIRT. Examina numerosos ámbitos de estadísticas de ciberseguridad antes de centrase en dos elementos que pueden aportar mejores mediciones y estadísticas estandarizadas a la formulación de políticas: i) la capacidad y recursos de los CSIRT para mitigar con eficacia los incidentes de seguridad; y ii) los incidentes de seguridad que gestionan los CSIRT. Establece directrices normativas y operativas para mejorar las estadísticas relacionadas con ambos elementos.

En este documento se desarrollan indicadores estadísticos específicos para la capacidad de los CSIRT: presupuesto, competencias, personal y cooperación formal. Todos los equipos de respuesta a incidentes, con independencia de su tamaño o madurez, poseen los datos necesarios para estas estadísticas, lo que los hace más adecuados para la comparación internacional.

La guía describe asimismo una serie de dificultades conceptuales, metodológicas, prácticas y tecnológicas a las que se enfrentan los CSIRT al crear estadísticas comparables sobre incidentes, e indica cómo abordarlas. En este ámbito se requerirá una cooperación permanente tanto entre los CSIRT, como entre las comunidades de respuesta a incidentes, estadísticas y políticas.

El documento también analiza diversas formas de tipificar las estadísticas relacionadas con los incidentes para tener en cuenta las diferencias en el tamaño de la red, antes de concluir con reflexiones finales sobre la difusión y adopción de la guía.

Fuentes: OCDE (2015b); OCDE (2012a).

Panorama de la situación en la región LAC

Estrategias nacionales de seguridad digital

Solo seis países (Colombia, México, Panamá, Paraguay, Trinidad y Tobago y Uruguay) tienen una estrategia nacional de seguridad digital, y en dos de ellos (México y Uruguay) se trata de una estrategia del gobierno nacional, pero no de seguridad digital en sí misma.

Pese a que en el 75% de los países en la región aún no dispone de una estrategia de seguridad digital, un gran número de países, entre ellos Argentina, Brasil, Chile, México y Paraguay, cuentan con entidades del gobierno y del sector público encargadas de coordinar y proteger la seguridad nacional y la infraestructura crítica (OEA y Symantec, 2014).

La OEA ha prestado apoyo y asistencia técnica a Costa Rica, Jamaica (OEA, 2015b), Paraguay y Perú en la implementación y mejora de sus respectivas estrategias nacionales de seguridad digital (OEA, 2015a, 2015b, 2015c y 2015d).

En un estudio reciente de ciberseguridad (BID y OEA, 2016) se evaluó el estado de preparación de 32 países de la región utilizando 49 indicadores divididos en cinco dimensiones: políticas y estrategia; educación; cultura y sociedad; marco jurídico, y tecnologías. Uruguay, Brasil, México, Argentina, Chile, Colombia y Trinidad y Tobago ya han alcanzado un nivel intermedio de preparación, pero aún van por detrás de países avanzados como Estados Unidos, Israel, Estonia y Corea.

Asimismo, el porcentaje de países LAC con legislación sustantiva y procesal para investigar y perseguir delitos informáticos y relacionados con Internet aún es bajo (alrededor del 44%). Únicamente en 11 casos (Chile, Colombia, Costa Rica, la República Dominicana, Jamaica, México, Paraguay, Perú, Trinidad y Tobago, Uruguay y Venezuela) se dispone de legislación penal sustantiva y procesal para combatir la ciberdelincuencia. Sin embargo, algunos países han declarado problemas no solo respecto al cumplimiento de las leyes y a la forma de mantener actualizada la legislación contra la ciberdelincuencia, sino también derivados de la necesidad de formar a fiscales y jueces para aumentar la capacidad de aplicar la ley, habida cuenta de la falta de conocimientos entre los expertos en este ámbito, así como de las restricciones presupuestarias (BID y OEA, 2014).

La mayoría de los organismos gubernamentales de los países de la región tienden a considerar la seguridad digital en una única dimensión (política, técnica, específica del sector) en lugar de basarse en un enfoque multidimensional (BID y OEA, 2014). Se concede poca importancia a las dimensiones económicas y sociales, por lo que los gobiernos no recurren con la suficiente frecuencia a alianzas público-privadas o a la cooperación para promover los objetivo de política pública en este ámbito.

Coordinación intra-gubernamental

El porcentaje de países LAC con mecanismos de coordinación gubernamental es muy bajo (alrededor del 30%). Solo ocho países (Brasil, Colombia, la República Dominicana, Jamaica, México, Perú, Trinidad y Tobago y Uruguay) abordan algunos aspectos de coordinación gubernamental en el desarrollo de su estrategia nacional de seguridad digital. No obstante, la información proporcionada indica que en la práctica la coordinación intra-gubernamental es reducida y que la mayor parte de los países LAC aún no aplica un enfoque de gobierno completo al riesgo de seguridad digital.

Los países miembros de la OEA han señalado tener problemas de coordinación y armonización entre las políticas de seguridad digital de los distintos organismos gubernamentales. Declaran “una ausencia general de cultura de colaboración que, unida a las restricciones presupuestarias, hace que la coordinación de las políticas de seguridad digital constituya una gran dificultad dentro del gobierno”. Otros miembros de la OEA han notificado un enfoque fragmentado en materia de seguridad digital dentro de sus gobiernos, con instituciones independientes que actúan de forma aislada más que de forma coordinada (BID y OEA, 2014).

Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT)

El porcentaje de países LAC con un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) plenamente respaldado por el gobierno es relativamente alto (más del 50%). Doce países (Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, Jamaica, México,

Paraguay, Perú, Trinidad y Tobago y Uruguay) tienen un CSIRT que cuenta con el pleno aval o apoyo de su gobierno nacional.

El Comité Interamericano contra el Terrorismo de la OEA (CICTE) ha estado trabajando en estrecha colaboración con todos los países de las Américas para crear y mejorar capacidades de respuesta a incidentes a través del *Programa de Seguridad Cibernética* de la OEA, que ha permitido aumentar el número de CSIRT nacionales en la región de 5 a 18. Sin embargo, según los informes "la falta de recursos financieros y de capacitación del personal son los principales obstáculos para implementar un CSIRT nacional y mejorar la capacidad de respuesta de los países frente a las amenazas cibernéticas en las Américas" (BID y OEA, 2014).

Concienciación y formación de personal cualificado que pueda gestionar el riesgo de seguridad digital

Muchos países de la región LAC han incrementado y mejorado sus actividades de concienciación para reforzar la seguridad digital y combatir la ciberdelincuencia (recuadro 14.2). La alianza entre múltiples partes interesadas "Stop. Think. Connect" ("Para. Piensa. Conéctate"), iniciada en octubre de 2010 para contribuir a la protección y seguridad en Internet de los ciudadanos conectados, sigue ampliándose y ya incluye a cinco autoridades gubernamentales de países LAC (la República Dominicana, Jamaica, Panamá, Paraguay y Uruguay), el CICTE y otras organizaciones públicas y privadas de la región.[1]

Recuadro 14.2. **Programas de concienciación sobre seguridad digital**

México: Programa Nacional de Seguridad Pública

México ha implementado un programa nacional de seguridad pública (*Programa Nacional de Seguridad Pública 2014-2018*) que en su apartado 4.2.9 establece como objetivo: "Impulsar la cultura de seguridad cibernética, especialmente entre niños y jóvenes, para prevenir que sean víctimas de delitos por internet".

Fuente: Programa Nacional de Seguridad Pública 2014-2018, http://dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014.

México: Semana Nacional de la Ciberseguridad

En octubre de 2015, como parte de las actividades de concienciación pública sobre seguridad digital, la Secretaría de Gobernación (SEGOB), la Comisión Nacional de Seguridad (CNS), la Policía Federal (PF) y la OEA organizaron la Semana Nacional de la Ciberseguridad en la que tuvieron lugar una serie de conferencias, seminarios y actividades de formación sobre seguridad de la información para combatir la ciberdelincuencia a nivel nacional.

Fuente: Protección Datos México (ProtDataMx), http://protecciondatos.mx/2015/10/essemana-nacional-de-la-ciberseguridad-2015ennational-cybersecurity-week-2015/.

Campaña de Perú para incrementar la seguridad de la información gubernamental

El CSIRT nacional de Perú (Pe-CERT) difunde información para incrementar y mejorar los niveles de seguridad de los sistemas y redes nacionales de información, y ofrece con regularidad formación y capacitación sobre TIC.

Fuente: PeCERT, *www.pecert.gob.pe/pecert-acerca-de.html.*

Uruguay: Campaña nacional *Seguro te conectás*

El CSIRT nacional de Uruguay (CERT-Uy) organiza conferencias y ejercicios de simulación sobre seguridad de la información, y ha promovido campañas nacionales de sensibilización como ***Seguro te conectás***, que promueve el uso responsable de Internet con una serie de recomendaciones audiovisuales y buenas prácticas orientadas a sensibilizar al público sobre los riesgos del mal uso de las TIC.

Fuente: CERT-Uy e información sobre la campaña *Seguro te conectás*, *www.cert.uy/Seguro-te-conectas/.*

Recientemente la OEA ha lanzado un kit de herramientas para la campaña de concienciación sobre ciberseguridad, diseñado para proporcionar a los gobiernos y organizaciones orientación y recursos para el desarrollo de una campaña de concienciación en materia de seguridad cibernética (OEA, 2015e). Ahora bien, las capacidades y la formación en los países de la región a menudo se limitan a aspectos técnicos, y aún no incluyen competencias para gestionar la seguridad digital desde una perspectiva más general.

Creación de un marco jurídico global para combatir la ciberdelincuencia

La República Dominicana y Panamá son los únicos países LAC que han ratificado el Convenio de Budapest de 2001 sobre Ciberdelincuencia (CoE, 2016), pese a que el Consejo de Europa ha invitado oficialmente a otros siete países latinoamericanos (Argentina, Chile, Colombia, Costa Rica, México, Paraguay y Perú) a que lo suscriban (CoE, 2014).

No obstante, el porcentaje de países LAC con legislación sustantiva y procesal acorde con el Convenio de Budapest sigue creciendo (cerca del 43%), y once de ellos (Chile, Colombia, Costa Rica, la República Dominicana, Jamaica, México, Paraguay, Perú, Trinidad y Tobago, Uruguay y Venezuela) han aprobado reglamentación contra la ciberdelincuencia. Destacan especialmente los casos de la República Dominicana y Panamá (recuadro 14.3).

Recuadro 14.3. **Algunos países que han ratificado el Convenio de Budapest**

República Dominicana

La República Dominicana fue uno de los primeros países LAC que aprobó una ley independiente para investigar, enjuiciar y castigar la ciberdelincuencia con arreglo a las disposiciones sustantivas, procesales y de cooperación internacional del Convenio de Budapest (Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología), que está en vigor desde el 18 de enero de 2007. Asimismo, fue el primer país LAC en ratificar el Convenio de Budapest.

Fuente: República Dominicana (2007), *Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología*, *www.oas.org/juridico/PDFs/repdom_ley5307.pdf*.

Panamá

Panamá fue el segundo país LAC en ratificar el Convenio de Budapest, el 1 de julio de 2014. Aunque aún no cuenta con una ley independiente para investigar, enjuiciar y castigar la ciberdelincuencia, existe un proyecto de ley para reformar el Código Penal que está pendiente de aprobación por la Asamblea Nacional, en el que se incluye la tipificación como delito de actos cometidos a través de las tecnologías de la información, conforme a las disposiciones del Convenio de Budapest.

Asignación de presupuesto y recursos para establecer una estrategia de seguridad digital

Como se señaló en el capítulo 2 sobre marcos regulatorios y estrategias digitales, la gran mayoría de los países LAC disponen de una asignación presupuestaria anual destinada a una estrategia digital nacional, aunque el presupuesto otorgado varía significativamente de unos países a otros. La Estrategia Digital Nacional de México, por ejemplo, cuenta con un presupuesto anual de 1740 millones de USD (29 millones de MXN), mientras que Colombia asignó a la suya (*Vive Digital*) cerca de 2,6 millones de USD durante los tres primeros años, y Chile presupuestó 850 millones de USD. No obstante, los porcentajes dedicados a la seguridad digital no están claros.

Además del presupuesto general anual para las estrategias digitales nacionales, determinados ministerios también pueden asignar sus propios presupuestos a la estrategia de seguridad digital, aunque esto no suele ser habitual en la mayoría de los países LAC. En 2014,

solo Colombia otorgó un presupuesto anual al Ministerio de Defensa Nacional, equivalente a 1,5 millones de USD (4,6 millones COP), para el Grupo de Respuesta a Emergencias Cibernéticas (colCERT), el Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCOC).

Más recientemente, la Secretaría de la Defensa Nacional de México solicitó un presupuesto anual de 100 millones de USD para crear el Centro de Operaciones del Ciberespacio en 2016, cuyo principal objetivo es reforzar la capacitación y formación estratégicas para combatir la ciberdelincuencia y las amenazas a la seguridad de la información, además de proteger la infraestructura crítica nacional (Stettin, 2015).

Cooperación internacional y asistencia mutua

El porcentaje de países LAC que practica la cooperación internacional y la asistencia judicial mutua es bajo. Solo cinco de ellos (Brasil, Chile, México, Perú y la República Dominicana) forman parte de la Red 24/7 del G-8, diseñada para ayudar a las fuerzas de seguridad de terceros países a obtener e intercambiar información relacionada con investigaciones penales transfronterizas, incluidos delitos cometidos mediante el uso de las TIC (Velasco, 2016).

En cambio, el número de países LAC con tratados de asistencia judicial mutua en materia de extradición y cooperación judicial regional es relativamente alto. Quince países (Brasil, el Estado Plurinacional de Bolivia, Chile, Colombia, Costa Rica, la República Dominicana, Ecuador, Guatemala, Honduras, México, Panamá, Paraguay, Perú, Uruguay y Venezuela) tienen tratados de extradición y acuerdos bilaterales de cooperación judicial internacional en materia penal en vigor.

Situación general

Varios países LAC han adoptado estrategias digitales nacionales o están en vías de implementarlas. Lamentablemente, la gran mayoría de estas estrategias carecen de una visión a largo plazo clara sobre el riesgo de seguridad digital y deben responder a diversos desafíos, tales como:

- creación y mejora de marcos jurídicos de seguridad digital
- creación de capacidades operativas para gestionar el riesgo de seguridad
- distribución clara de responsabilidades entre las instituciones gubernamentales
- cooperación internacional entre múltiples partes interesadas (OEA, 2014).

Todo apunta a que la mayor parte de los países LAC no están enfocando el riesgo de seguridad digital desde un punto de vista económico y social, a diferencia de lo que propugna la OCDE. En el momento de redactar la presente publicación el enfoque de la OCDE era relativamente nuevo, por lo que no sorprende que aún no se vea reflejado en los marcos de las políticas en vigor. También hay que reconocer que algunos países LAC afrontan otros desafíos adicionales que limitan su capacidad para adoptar dicho enfoque (OEA y Symantec, 2014).

La implementación de mecanismos de coordinación en los gobiernos para formular y ejecutar estrategias nacionales de seguridad digital es uno de los grandes retos de los países LAC. Sin embargo, en lugar de distinguir claramente las diferentes facetas de lo que a menudo se conoce como “ciberseguridad” y abordarlas bajo una estrategia global que garantice la coordinación y coherencia a nivel estatal, los gobiernos suelen enfocar este tema desde una perspectiva única, como la seguridad internacional o la ciberdelincuencia. Esto lleva a dejar de lado los aspectos económicos y a tratar la cuestión en un compartimento estanco de políticas públicas, al margen de los actores no gubernamentales. Las restricciones presupuestarias han limitado la adopción de mecanismos de coordinación entre los organismos gubernamentales

de la región, y solo en unos pocos países los correspondientes ministerios y autoridades competentes han asignado presupuestos anuales a estrategias digitales nacionales.

Si bien ha mejorado la participación de las partes interesadas en la mayoría de las estrategias nacionales de seguridad digital, todavía no está consolidada en gran parte de los países LAC, muchos de los cuales carecen de mecanismos flexibles y de planes a medio y largo plazo para apoyar a los distintos actores en el desarrollo de políticas y marcos jurídicos sobre seguridad digital (OEA y Symantec, 2014). En cambio, numerosos países, entre ellos Colombia, México, Panamá y Perú, han establecido CSIRT nacionales plenamente respaldados por sus respectivos gobiernos, que contribuyen activamente a facilitar el intercambio de información sobre incidentes y amenazas de seguridad informática, además de ofrecer formación a su personal y al público en general sobre seguridad de la información.

Sigue aumentando el número de países LAC que ha aprobado legislación para combatir la ciberdelincuencia con arreglo al Convenio de Budapest del Consejo de Europa, y son muchos los interesados en solicitar formalmente la adhesión a dicho convenio y a su protocolo adicional, pese a que implicará un proceso político complejo y a largo plazo.

Buenas prácticas para la región LAC

Concienciación y comprensión de la gestión del riesgo de seguridad digital

Con los años ha aumentado en todo el mundo la concienciación de las amenazas e incidentes digitales, pero el grado de comprensión de algunos aspectos es insuficiente y, en particular, existe confusión sobre su dimensión económica y social. La recomendación de la OCDE de 2015 sobre gestión del riesgo de seguridad digital para la prosperidad económica y social (*Recommendation on Digital Security Risk Management for Economic and Social Prosperity*) y su documento de acompañamiento proporcionan conceptos, principios y orientaciones fundamentales para la elaboración de políticas públicas en este ámbito, así como de políticas para la gestión del riesgo en organismos públicos y privados (OCDE, 2015a). El enfoque de la OCDE se basa en el reconocimiento de los siguientes aspectos:

- El riesgo de seguridad digital es una **cuestión económica y social**, y no solamente un desafío técnico.
- Es imposible crear un **entorno digital totalmente protegido y seguro** en el que se evite por completo el riesgo, a menos que se elimine su apertura digital, interconexión y dinamismo renunciando con ello a los beneficios económicos y sociales que conlleva.
- No obstante, se puede gestionar y reducir el **riesgo a un nivel** aceptable que viene dado tanto por los objetivos económicos y sociales y sus correspondientes beneficios, como por el contexto.
- La gestión del riesgo de seguridad digital puede guiar la selección de **medidas adecuadas** en este ámbito que no socaven la actividad que pretenden proteger, tengan en cuenta los intereses de los demás y preserven los derechos humanos y los valores fundamentales.
- Los **dirigentes y los responsables** de la toma de decisiones son los más indicados para encabezar los cambios necesarios que permitan reducir el riesgo a un nivel aceptable.
- La gestión del riesgo de seguridad digital debe **integrarse en la toma de decisiones económicas** y en el **marco más amplio de gestión del riesgo** para facilitar un liderazgo estratégico, ágil y eficaz.

Estrategia nacional para la gestión del riesgo de seguridad digital

Muchos países de todo el mundo están adoptando lo que suelen denominar "estrategias de ciberseguridad" nacionales, cuyo contenido varía considerablemente. Con independencia

del nombre que se les otorgue y del tipo de documentos en los que se plasmen, es esencial que los gobiernos adopten estrategias que creen las condiciones para que todas las partes interesadas gestionen el riesgo de seguridad digital, junto con aumentar la confianza en el entorno digital. Una estrategia de este tipo puede formar parte de una **política general** que aborde la dimensión nacional e internacional de la ciberseguridad, así como la lucha contra la ciberdelincuencia. También puede incluirse en una estrategia digital nacional destinada a promover el uso de las TIC para la prosperidad económica y social.

Tal estrategia debe establecer claramente que tiene por objeto:

- **aprovechar el entorno digital abierto** para la prosperidad económica y social reduciendo el nivel general de riesgo de seguridad digital dentro y fuera de las fronteras, sin restringir innecesariamente el flujo de tecnologías, comunicaciones y datos
- **garantizar la prestación de servicios esenciales** y el funcionamiento de la **infraestructura crítica**, **protegiendo a los ciudadanos** de amenazas a la seguridad digital a la vez que se tiene en cuenta la necesidad de salvaguardar la seguridad nacional e internacional y de preservar los derechos humanos y los valores fundamentales.

Es preciso que la estrategia se **dirija a todas las partes interesadas**, se adapte según convenga a las pequeñas y medianas empresas y a los ciudadanos, y explique claramente la responsabilidad y rendición de cuentas de los distintos actores conforme a sus funciones, su capacidad de acción y el contexto en el que operan.

Por último, debe ser el resultado de un enfoque de **coordinación intragubernamental** y un proceso abierto y transparente en el que participen todas la partes interesadas. Asimismo, se ha de revisar y mejorar periódicamente a partir de la experiencia y las mejores prácticas, y utilizando sistemas de medición comparables a escala internacional cuando estén disponibles.

La recomendación de la OCDE sobre gestión del riesgo de seguridad digital para la prosperidad económica y social (OCDE, 2015a) contiene orientaciones sobre medidas que cabe incluir en esta estrategia, como la forma en que los gobiernos pueden dar ejemplo, las medidas para fortalecer la cooperación internacional y la asistencia mutua, cómo colaborar con otras partes interesadas y cómo crear las condiciones para que todos los actores participen en la gestión del riesgo de seguridad digital. Tales medidas comprenden, por ejemplo:

- garantizar que la estrategia digital nacional se aplica y gestiona de forma que favorezca la **innovación y la prosperidad**, además de mantener un entorno abierto, maximizar el potencial de las TIC para el crecimiento y el desarrollo, y facilitar la cooperación regional e internacional
- mejorar y actualizar los programas de formación y garantizar la organización de **campañas nacionales de concienciación**
- crear un programa nacional global para **medir el riesgo de seguridad digital** y **facilitar mecanismos de coordinación** y la distribución de responsabilidades entre organismos gubernamentales
- fomentar la **asistencia mutua** entre las fuerzas de seguridad de la región en la identificación de actividades delictivas en Internet y el enjuiciamiento de los autores
- establecer **puntos de contacto nacionales para tratar peticiones transfronterizas** relacionadas con la gestión del riesgo de seguridad digital y mejorar las respuestas a incidentes y amenazas nacionales y transfronterizos, principalmente a través de la cooperación con los CSIRT, actuaciones coordinadas y otros medios de colaboración

- impulsar **alianzas nacionales entre empresas de TIC y organismos gubernamentales** en materia de seguridad digital y la creación de mecanismos flexibles de cooperación transfronteriza.

Cooperación internacional y asistencia mutua

La cooperación internacional y la asistencia mutua constituyen una buena práctica en las políticas, que puede contribuir a detectar delitos transfronterizos y a desarrollar mecanismos de cooperación regional e internacional para aplicar leyes nacionales a delincuentes ubicados en distintas jurisdicciones.

Colombia, México, Perú, Paraguay y Uruguay participan activamente en el Programa de Seguridad Cibernética de la OEA y en las diversas actividades organizadas por el Comité Interamericano contra el Terrorismo (CICTE)[2] para combatir la ciberdelincuencia con la participación de distintos actores, tanto del sector público como privado.

Colaboración con otras partes interesadas

También es una buena práctica en las políticas promover la participación activa de las partes interesadas a través de consultas nacionales sobre seguridad digital, potenciar la gestión de la seguridad digital entre los diferentes actores y distribuir responsabilidades (recuadro 14.4).

Recuadro 14.4. **Algunos casos de participación de partes interesadas nacionales**

Colombia

Colombia contempla de forma expresa la participación de las partes interesadas en el documento *Lineamientos de política para ciberseguridad y ciberdefensa*.

Este Documento Conpes 3701 de julio de 2011 establece que el CSIRT nacional (colCERT) y el Centro Cibernético Policial (CCP) articularán iniciativas con el sector privado y la sociedad civil para gestionar incidentes de seguridad en la infraestructura crítica nacional.

Fuente: Lineamientos de política para ciberseguridad y ciberdefensa, www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

Brasil

El Comité Gestor de Internet en Brasil (*Comitê Gestor da Internet no Brasil*, *CGI.br*) es un ejemplo de buena práctica de cooperación entre múltiples partes interesadas, que van desde la comunidad técnica y el mundo universitario a la sociedad civil. En este caso, todas ellas comparten la responsabilidad de notificar, revisar y responder a los incidentes de seguridad informática. También forman parte de su labor responder a amenazas a las redes y sistemas de los sectores público y privado y elaborar políticas nacionales de seguridad de la información.

Fuente: Comitê Gestor da Internet *no Brasil, www.cgi.br/.*

Jamaica

En 2013, Jamaica estableció un Grupo de Trabajo sobre Ciberseguridad con partes interesadas de los sectores público y privado que juntas contribuyen a proponer, redactar y hacer avanzar políticas nacionales de seguridad digital, entre ellas la Estrategia Nacional de Seguridad Cibernética de Jamaica.

Fuente: Gobierno de Jamaica (2015), *Jamaica's National Cyber Security Strategy*, *http://mstem.gov.jm/?q=national-cyber-security-strategy*.

Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT)

Los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) desempeñan un papel esencial en la identificación de amenazas a los sistemas y redes de seguridad de la información y delitos cometidos mediante el uso de las tecnologías de la información. Hay

consenso en que un CSIRT es un "equipo de expertos que responde a incidentes informáticos, coordina su resolución, informa a las partes involucradas, intercambia información con otros actores y ayuda a mitigar el incidente" (recuadro 14.5). Los CSIRT también sirven de puntos de contacto fiables para notificar incidentes de seguridad, difundir información pertinente sobre incidentes informáticos, disminuir los riesgos de seguridad y coordinar sus iniciativas de respuesta con otras instituciones similares. El establecimiento de un CSIRT nacional constituye una buena práctica en las políticas para facilitar la cooperación regional e internacional sobre seguridad de la información. También se pueden impulsar CSIRT en el sector privado (empresas, y sector académico).

Recuadro 14.5. **Recomendaciones para la comunidad de CSIRT**

El Foro de Gobernanza de Internet (IGF por sus siglas en inglés) eligió los CSIRT como uno de los temas de los Foros de Mejores Prácticas de 2014. A continuación se enumera una selección de las recomendaciones formuladas en dichos foros:

- Es necesario que los responsables de políticas debatan con la comunidad de CSIRT sobre el papel de estos equipos para evitar ideas equivocadas acerca de su cometido.
- Se recomienda a los CSIRT participar activamente en los debates de políticas que resulten pertinentes, tanto a nivel nacional como internacional. En aras de colaborar con otras partes interesadas es importante estar donde ellas estén, puesto que de esta forma se ejerce influencia y se facilita la comprensión, tal y como muestran los ejemplos proporcionados.
- Cualquier gobierno tiene derecho a crear los CSIRT que necesite, aunque conviene tomar una decisión fundada que tenga en cuenta las posibles consecuencias.
- En lo referente a los CSIRT la privacidad y la seguridad han de ir de la mano para que resulten realmente eficaces.
- El término protección de datos se entiende mejor en un sentido general que el de privacidad, por lo que es aconsejable optar por él en un contexto de CSIRT al ser mucho más concreto.
- El núcleo de la labor de los CSIRT debe ser la protección de datos.
- Es recomendable implicar en mayor medida a los responsables de protección de datos en la labor de los CSIRT.
- Para garantizar la transparencia y la rendición de cuentas en lo que respecta a la protección de datos se recomienda realizar estudios para dilucidar si un protocolo estándar puede contribuir al fomento de la transparencia, además de la adopción de decisiones más conscientes sobre los límites de la información compartida, la anonimización de datos en la medida de lo posible y la manipulación de los datos por los CSIRT.
- Conviene que los CSIRT minimicen la recopilación y el tratamiento de datos y se centren en su circunscripción y en la anonimización de la información pertinente.
- Un CSIRT bien gestionado es parte esencial de la protección de datos y la seguridad en una sociedad.
- Se recomienda estudiar con mayor detalle la función cada vez más amplia de los CSIRT. Podría examinarse, por ejemplo, si existen límites razonables a las tareas asignadas y qué papel puede desempeñar un CSIRT en la mejora de la cooperación en la cadena de seguridad entre otros actores, como fabricantes de productos TIC y proveedores de servicios TIC, o analizar si la definición actual de CSIRT se ajusta a la realidad de la labor requerida y encomendada.
- Se aconseja un estudio más profundo de la forma en que los CSIRT y las fuerzas de seguridad pueden aumentar su cooperación de manera significativa en el marco de sus respectivas misiones.

Recuadro 14.5. **Recomendaciones para la comunidad de CSIRT** *(cont.)*

- Conviene profundizar en la divulgación responsable de la información y en cómo crear condiciones para que los *hackers* éticos puedan contribuir a que Internet sea más segura para todos.
- Los CSIRT contribuyen a tratar los efectos de la ciberdelincuencia y a aportar apoyo técnico a las investigaciones; pero el ciberdelito es ante todo un delito y, como tal, debe ser tratado por organismos de seguridad, como la policía. Si un CSIRT dedica demasiados esfuerzos a esta labor o forma parte de un organismo encargado de aplicar la ley es probable que su capacidad para trabajar con el sector privado se vea afectada.

Fuente: (IGF, 2015), CSIRT Best Practice Forum, *www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/627-bpf-csirt-2015-report-final-v2/file*

Como se señaló anteriormente, 12 países de la región LAC cuentan con un CSIRT plenamente avalado o apoyado por el gobierno nacional. A continuación se describen los casos de Brasil, Costa Rica y México (recuadro 14.6).

Recuadro 14.6. **Algunos CSIRT nacionales**

Brasil

Brasil tiene dos CSIRT nacionales que colaboran activamente. El Centro de Tratamiento de Incidentes de Seguridad en Redes Informáticas de la Administración Pública Federal (CTIR Gov) está coordinado por el Departamento de Seguridad de la Información y las Comunicaciones del Gabinete de Seguridad Institucional de la Presidencia de Brasil. Su finalidad principal es la supervisión y el seguimiento de incidentes y amenazas a los sistemas y redes informáticos de la Administración Pública Federal.[1] El *Cert.Br*, por su parte, está respaldado, coordinado y financiado por el Comité Gestor de Internet (*Comitê Gestor da Internet no Brasil, CGI.br*) y se encarga principalmente de los sistemas y redes de seguridad de la información del sector privado y el mundo universitario.

1. Puede obtenerse más información sobre CTIR Gov en *www.ctir.gov.br/*.

Fuente: www.cert.br/.

Costa Rica

Costa Rica creó un CSIRT nacional (CSIRT-CR) en 2012 como parte de la publicación del Decreto Ejecutivo Nº 37052-MICIT del 9 de marzo de 2012. Está integrado por los responsables de los principales ministerios nacionales y se encarga de apoyar y cooperar con las autoridades administrativas y judiciales para la investigación y enjuiciamiento de delitos informáticos, así como de coordinar actividades con la Interpol y el Comité Interamericano contra el Terrorismo de la OEA (CICTE).

Fuente: www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC.

México

La División Científica de la Policía Federal de México gestiona un CSIRT nacional (CERT-MX), que actualmente es el CSIRT oficial del gobierno nacional. El CERT-MX sirve de principal punto de contacto con la Interpol y con el Departamento de Justicia de los Estados Unidos. Entre sus actividades destacan la identificación y seguimiento de los incidentes de seguridad informática, la protección de la infraestructura crítica e industrial y la organización de campañas públicas nacionales de concienciación sobre la seguridad de la información.

Fuente: www.cns.gob.mx/portalWebApp/wlp.c?__c=fdd.

Conclusión

Este capítulo se centró en las políticas públicas para incrementar la gestión del riesgo de seguridad digital para la prosperidad económica y social, que se distingue de otros aspectos de ciberseguridad relativos a la tecnología, aplicación de la ley, seguridad nacional y defensa. Se presentaron los elementos clave de las estrategias nacionales que pueden crear las condiciones marco para incrementar la confianza de todas las partes interesadas, de tal forma que sea posible utilizar las TIC y el entorno digital para la prosperidad económica y social. Entre estos elementos destaca la comprensión de la gestión del riesgo como un enfoque que se centra en las actividades basadas en el entorno digital, y no solo en el propio entorno digital.

También se indicaron herramientas de medición y evaluación de impacto existentes, y se describió un panorama general de los esfuerzos de política pública desplegados en la región LAC. La situación general de la región muestra que varios países han adoptado estrategias digitales nacionales o están en vías de implementarlas. Lamentablemente, la gran mayoría de estas estrategias carecen de una visión a largo plazo clara y general en relación con el riesgo de seguridad digital y deben hacer frente a diversos desafíos, como la creación y mejora de marcos jurídicos de seguridad digital, la creación de capacidades operativas para gestionar el riesgo de seguridad, la distribución clara de responsabilidades entre las instituciones gubernamentales, y la cooperación internacional entre múltiples partes interesadas. Todo apunta a que la mayor parte de los países LAC no enfocan el riesgo de seguridad digital desde un punto de vista económico y social, a diferencia de lo que propugna la OCDE. Ahora bien, en el momento de la redactar la presente publicación el enfoque de la OCDE era relativamente nuevo, por lo que no sorprende que aún no se vea reflejado en los marcos de las políticas en vigor.

Por último, el capítulo mostró diversas buenas prácticas para fomentar las políticas y estrategias de gestión del riesgo de seguridad digital, basadas en la recomendación de la OCDE de 2015 sobre gestión del riesgo de seguridad digital para la prosperidad económica y social (*Recommendation on Digital Security Risk Management for Economic and Social Prosperity*) y su documento anexo (OCDE, 2015a). En concreto, los responsables de políticas deben reconocer que el riesgo de seguridad digital es una cuestión económica y social, y no solamente un desafío técnico. También han de tener en cuenta que es imposible crear un entorno digital totalmente protegido y seguro en el que se evite por completo el riesgo, por lo que conviene que potencien un enfoque en el que los dirigentes y los responsables de la toma de decisiones asuman la responsabilidad de gestionar dicho riesgo. Esto implica reducirlo a un nivel aceptable que viene dado tanto por los objetivos económicos y sociales y sus correspondientes beneficios, como por el contexto. Todas las medidas incluidas en las estrategias de ciberseguridad nacionales deben reflejar este enfoque, tanto si están relacionadas con infraestructura crítica de información, como con la cooperación internacional o los CSIRT.

Notas

1. *Stop.Think.Connect* puede consultarse en: *www.stopthinkconnect.org/*.
2. Programa de Seguridad Cibernética de la OEA *www.oas.org/es/sms/cicte/programas_cibernetica.asp*.

Bibliografía

BID y OEA (2016), *2016 Ciberseguridad en América Latina y el Caribe ¿Estamos preparados?*, Organización de los Estados Americanos, Washington D.C., *www.iadb.org/ciberseguridad*.

BID y OEA (2014), *Informe de resultados de las Políticas de Seguridad Cibernética*, Organización de los Estados Americanos, Washington D.C., *www.iadb.org/es/noticias/comunicados-de-prensa/2014-10-22/taller-sobre-ciberseguridad-en-america-latina,10957.html*.

BSA (2015), *EU Cybersecurity Dashboard*, *http://cybersecurity.bsa.org/*.

CoE (2016), "Chart of Signatures and Ratifications of Treaty 185", *Convention on Cybercrime*, Consejo de Europa, *www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures*.

CoE (2014), *Memoria del "Taller sobre legislación en materia de ciberdelincuencia en América Latina", co-auspiciado por el Gobierno de México y el Consejo de Europa*, Consejo de Europa/Gobierno de México, *https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/Memoria%20Taller%20Ciberdelito.pdf*.

Departamento de Energía de los Estados Unidos (2015), *Cybersecurity Capability Maturity Model (C2M2) Program*, Department of Energy, Washington D.C., *http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program*.

Global Cybersecurity Capacity Centre (2014), *Cyber Security Capability Maturity Model (CMM) – V1.2*, Oxford, *www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version1.2.pdf*.

Gobierno de Jamaica (2015), *Jamaica's National Cyber Security Strategy*, *http://mstem.gov.jm/?q=national-cyber-security-strategy*.

IGF BPF (2015), *"Best Practices Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet Security (2015)"*, Foro de Gobernanza de Internet 2015, Ginebra, *www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/627-bpf-csirt-2015-report-final-v2/file*.

OEA (2015a), "OEA apoya a Costa Rica en el desarrollo de su Estrategia Nacional de Seguridad Cibernética", comunicado de prensa C-063/15, Organización de los Estados Americanos, Washington D.C., *www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/15*.

OEA (2015a), "OEA coorganizó el lanzamiento de la Estrategia Nacional de Seguridad Cibernética de Jamaica", comunicado de prensa C019/15, Organización de los Estados Americanos, Washington D.C., *www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-019/15*.

OEA (2015c), "La OEA apoya a Paraguay en el Desarrollo de su Plan Nacional de Ciberseguridad", comunicado de prensa C-169/15, Organización de los Estados Americanos, Washington D.C., *www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-169/15*.

OEA (2015d), "OEA apoya a Perú en el desarrollo de su Estrategia Nacional de Seguridad Cibernética, comunicado de prensa 25/15, Organización de los Estados Americanos Washington D.C., *www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-125/15*.

OEA (2015e), *Ciberseguridad - Kit de herramientas para la campaña de concienciación*, Organización de los Estados Americanos – Secretaría de Seguridad Multidimensional, Washington D.C., *https://www.sites.oas.org/cyber/Documents/2015%20OEA%20-%20Ciberseguridad%20Kit%20de%20Herramientas%20para%20la%20Campa%C3%B1a%20de%20Concientizaci%C3%B3n%20(Espa%C3%B1ol).pdf*.

OEA (2014), "Misión de asistencia técnica en seguridad cibernética. Conclusiones y recomendaciones", 4 de abril, Organización de los Estados Americanos, Bogotá, *www.digiware.net/sites/default/files/Recomendaciones_COLOMBIA_SPA.pdf*.

OEA y Symantec (2014), *Tendencias de seguridad cibernética en América Latina y el Caribe*, Organización de los Estados Americanos, Washington D.C., *www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf*.

OCDE (2015a), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, París, septiembre, *www.oecd.org/sti/ieconomy/Digital-Security-Risk-Management.htm*.

OCDE (2015b), *Guidance for Improving the Comparability of Statistics Produced by Computer Security Incident Response Teams*, Working Party on Security and Privacy in the Digital Economy, junio, *www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2013)9/FINAL&doclanguage=en*.

OCDE (2013), *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, París, *www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm*.

OCDE (2012a), "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online", *OECD Digital Economy Papers*, No. 214, OECD Publishing, París, *http://dx.doi.org/10.1787/5k4dq3rkb19n-en*.

OCDE (2012b), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, París, *http://dx.doi.org/10.1787/5k8zq92vdgtl-en*.

República Dominicana (2007), *Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología*, *www.oas.org/juridico/PDFs/repdom_ley5307.pdf*.

Rodríguez Florez, M.E. (2013), *América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?*, Trabajos de Investigación en Políticas Públicas No. 16, septiembre, Universidad de Chile, Santiago, Chile, *www.econ.uchile.cl/uploads/publicacion/9ba7739a0ac26598402dab53c990c58e49fc259a.pdf*.

Stettin, C. (2015), "Ante amenazas de 'hackers' la Sedena pide mil 700 mdp", *Milenio*, *www.milenio.com/policia/amenazas-hackers-Sedena-pide-mdp_0_590940917.html*.

UIT (2014), *Índice Mundial de Ciberseguridad*, Unión Internacional de Telecomunicaciones, Ginebra, *www.itu.int/pub/D-STR-SECU-2015/es*.

Velasco, C. (2016), "Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos", *Monografías*, Tirant lo Blanch, Valencia, *www.tirant.com/libreria/libro/jurisdiccion-y-competencia-penal-en-relacion-al-acceso-transfronterizo-en-materia-de-ciberdelitos-cristos-velasco-san-martin-9788490869925*.

ANEXO 14.A1

Referencias a estrategias nacionales de seguridad digital y legislación nacional en la región LAC

	Estrategias nacionales de seguridad digital y legislación nacional
Argentina	**Disposición 3/2013 sobre Política de Seguridad de la Información Modelo para la Administración Pública Nacional** publicada por el Director Nacional de la Oficina Nacional de Tecnologías de Información el 27 de agosto de 2013: *www.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219163/norma.htm*
Brasil	***Comitê Gestor da Internet no Brasil* (CGI.br):** *www.cgi.br/* **Centro de Tratamiento de Incidentes de Seguridad en Redes Informáticas de la Administración Pública Federal de Brasil (CTIR Gov):** *www.ctir.gov.br/* **Cert.br:** *www.cert.br/*
Chile	**Decreto Supremo Nº 1299 Programa para mejorar la gestión y seguridad de la información** *www.csirt.gob.cl/decreto_1299.html* **Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-CL):** *www.csirt.gob.cl*
Colombia	**Política nacional de ciberseguridad y ciberdefensa:** *www.oas.org/cyber/presentations/Presentaci%C3%B3n%20Ottawa%20Colombia.pdf* *Documento Conpes 3701* ***"Lineamientos de política para ciberseguridad y ciberdefensa"*** 14 de julio de 2011**:** *www.mintic.gov.co/portal/604/articles-3510_documento.pdf* **Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT):** *www.colcert.gov.co/*
Costa Rica	**Estrategia Nacional de Seguridad Cibernética:** *www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/15* **Decreto Ejecutivo Nº 37052-MICIT** por el que se crea el CSIRT-CR de Costa Rica: *www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC*
República Dominicana	***Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología de la República Dominicana*:** *www.oas.org/juridico/PDFs/repdom_ley5307.pdf*
México	**Estrategia Digital Nacional y Estrategia Nacional de Seguridad de la Información:** *www.presidencia.gob.mx/edn/* ***Programa Nacional de Seguridad Pública 2014-2018***, publicado en el Diario Oficial de la Federación el 30 de abril de 2014: *http://dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014* **Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX)** de la División Científica de la Policía Federal de México: *www.cns.gob.mx/portalWebApp/wlp.c?__c=fdd*
Panamá	**Estrategia nacional de seguridad cibernética y de protección de la Infraestructura crítica:** *www.oas.org/cyber/events/Panama%20National%20Strategy.pdf* **Decreto Ejecutivo Nº 709 de 26 de septiembre de 2011** por el cual se crea el **Equipo Nacional de Respuesta a Incidentes de Seguridad de la Información del Estado Panameño (CSIRT PANAMÁ):** *www.gacetaoficial.gob.pa/pdfTemp/26880/34793.pdf*
Perú	**Estrategia Nacional de Seguridad Cibernética:** *www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-125/15* **Equipo de Respuesta a Incidentes de Seguridad Informática (PeCERT):** *www.pecert.gob.pe/pecert-acerca-de.html*
Uruguay	**Centro de Respuesta a Incidentes de Seguridad Informática (CERTuy):** *www.cert.uy* **Campaña *Seguro te conectás*** *www.cert.uy/Seguro-te-conectas/*