TENDENCIAS DE SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE

Publicado en junio de 2014

Organización de los Estados Americanos

Symantec™

ÍNDICE

Colaboradores

Organización de los Estados Americanos

Organización de los
Estados Americanos

Symantec

AMERIPOL

Anti-Phishing Working Group

La Corporación de Internet para la
Asignación de Nombres y Números

Lacnic

Microsoft

Introducción al Informe de la OEA

Junio de 2014

Una de las prioridades de la Organización de los Estados Americanos (OEA) es respaldar los esfuerzos e iniciativas de nuestros Estados Miembros destinados a fortalecer las capacidades necesarias para que el dominio informático sea más seguro, estable y productivo.

En 2004, los Estados Miembros de la OEA reconocieron formalmente que combatir los delitos cibernéticos y fortalecer la resiliencia cibernética eran cuestiones imperativas para el desarrollo económico y social, la gobernanza democrática, la seguridad nacional y la de los ciudadanos. Asimismo, los Estados Miembros también reconocieron que los usuarios, operadores y reguladores de Internet necesitan acceder a información oportuna y precisa para enfrentar de manera eficaz las amenazas y vulnerabilidades cibernéticas en constante evolución. Atendiendo a esta necesidad, la OEA y Symantec desarrollaron un informe sobre las *Tendencias de Seguridad Informática en América Latina y el Caribe* con el objetivo de continuar describiendo el ecosistema informático en América Latina y el Caribe, paso crucial para implementar acciones de desarrollo de capacidades de seguridad cibernética basadas en datos.

A pedido de los Estados Miembros, la OEA ha promovido específicamente la cooperación entre los sectores público y privado, y entre el sector académico y los usuarios finales para fortalecer la resiliencia cibernética y proteger las infraestructuras críticas. Recientemente, enviamos una delegación de expertos internacionales de alto nivel a Colombia en respuesta a la solicitud de una evaluación cibernética integral formulada por el Presidente Juan Manuel Santos. Como resultado de la misión, se presentaron al gobierno colombiano una serie de recomendaciones y acciones por implementar en materia de seguridad cibernética, que se encuentran en consideración.

Si bien existen otras historias de éxito similares, nuestra región también debe enfrentar importantes desafíos. En los lugares donde se producen delitos cibernéticos, los Estados Miembros deben contar con la capacidad de prevenir, mitigar, responder, investigar y procesar de manera efectiva las conductas criminales, cuando sea pertinente. Asimismo, las autoridades nacionales deben promover la creación de una cultura de la seguridad cibernética y emprender acciones de concientización en esa materia para proteger a los usuarios -quienes en el mundo actual están cada vez más expuestos- con el fin de dotarlos del conocimiento que necesitan para proteger su información. Como destacaron los Estados Miembros, para desarrollar una cultura en seguridad cibernética se requiere la colaboración de todas las partes interesadas a nivel nacional.

De hecho, las asociaciones efectivas entre el sector privado y las entidades de la sociedad civil son relevantes para el fortalecimiento de la seguridad cibernética, ya que las entidades no gubernamentales administran y operan gran parte de la infraestructura crítica de la que dependemos. No sólo se trata de la infraestructura de Internet, sino también la que controlan los sectores de transporte, salud, banca, energía, entre otros. En Davos, Suiza, por ejemplo, me reuní con líderes del sector comercial, gubernamental y de la seguridad cibernética para debatir la iniciativa del Foro Económico Mundial, "Riesgo y Responsabilidad en un Mundo Hiperconectado". Éste y muchos otros eventos revelan la creciente importancia de la seguridad cibernética como cuestión clave a nivel mundial.

Así pues, el informe representa el esfuerzo de múltiples actores, con el aporte de Symantec, AMERIPOL, Microsoft, LACNIC, ICANN, y el Grupo de Trabajo *Anti-Phishing* (APWG). El informe también brinda un panorama integral de la seguridad cibernética en América, con el aporte de 30 de los 32 países de América Latina y el Caribe.[01] Se ha utilizado la información en conjunto para brindar la imagen más clara a la fecha de la posición que ocupa la región en materia de seguridad cibernética. Sin embargo, reconocemos que se trata simplemente de la captura de un momento específico en un panorama dinámico. Por lo tanto, se espera que este informe evolucione para reflejar los cambios en esta área y se actualice cuando surja nueva información pertinente. De esta manera, el informe servirá como base para identificar áreas que necesitan mejoras y desarrollar estrategias basadas en la evidencia de forma oportuna. Esperamos que esta información ayude a guiar y fortalecer todos nuestros esfuerzos a futuro, y que facilite especialmente el desarrollo de asociaciones con otras partes que comparten nuestro compromiso con la misión esencial de crear un mundo digital seguro y estable.

Atentamente,

Emb. Adam Blackwell

Secretario de Seguridad Multidimensional
Organización de los Estados Americanos

01 Las Bahamas aportó información de forma anónima, que se incorporó en la sección de resumen y tendencias generales.

Introducción al Informe de Symantec

Junio de 2014

Symantec tiene una larga y exitosa experiencia en la participación de alianzas público-privadas alrededor del mundo. Creemos que compartir la información acerca de amenazas, vulnerabilidades e incidentes de manera eficaz es fundamental para mejorar la seguridad cibernética y combatir los delitos cibernéticos. Por lo tanto, nos complace asociarnos con la Organización de los Estados Americanos (OEA) para redactar este informe, *Tendencias de Seguridad Cibernética en América Latina y el Caribe*.

En el mundo conectado de hoy día, dependemos del papel que la tecnología desempeña virtualmente en casi todos los aspectos de nuestra vida; desde las operaciones bancarias móviles, hasta la seguridad de nuestros sistemas más críticos. Con el mayor uso de la tecnología también aumenta el volumen y sofisticación de las amenazas. Los criminales buscan constantemente explotar nuevas vulnerabilidades para robar dinero, propiedad intelectual e identidades. Este desafío se ve agravado por la falta de fronteras en el ciberespacio, que permite cometer delitos a gran distancia. De hecho, todas las computadoras del mundo son un punto de entrada potencial, lo que dificulta la investigación y procesamiento de los delitos cibernéticos.

En 2013 observamos un aumento de las violaciones de datos, troyanos implantados en el sistema bancario, *malware* orientado a dispositivos móviles y otras amenazas en la red. El *hacktivismo* siguió presentando desafíos a muchos países de la región, si bien hay indicadores de que esta tendencia podría estar declinando en algunos países. En el presente informe, se expone un análisis en profundidad de las tendencias observadas y se proporcionan indicaciones acerca de ciertas medidas preventivas que pueden tomar los usuarios para protegerse de manera más eficaz. El informe detalla, además, una cantidad de nuevas tendencias y vulnerabilidades alarmantes registradas a nivel mundial, así como las específicas de América Latina y el Caribe.

Esta región posee una de las poblaciones de usuarios de Internet de más rápido crecimiento del mundo, lo que presenta una importante cantidad de desafíos en materia de seguridad cibernética en el presente y a futuro. El objetivo de este informe es ofrecer un panorama general basado en datos de la variedad de amenazas presentes, así como algunas recomendaciones prácticas para mejorar la seguridad cibernética en consonancia con la evolución de esas amenazas. En Symantec hemos asumido el compromiso de mejorar la protección de la información en todo el mundo, y continuaremos trabajando en asociación con la industria, los gobiernos y la sociedad civil para lograrlo.

Atentamente,

Cheri F. McGuire

Vicepresidente de Asuntos Gubernamentales
y Políticas Globales de Seguridad Cibernética

Symantec Corporation

Introducción

El presente informe proporciona un panorama general de las novedades en materia de seguridad cibernética y delito cibernético que tuvieron lugar en América Latina y el Caribe durante 2013. Evalúa las tendencias más importantes observadas en la región en lo que respecta a amenazas al dominio cibernético y a quienes dependen de él, desde instituciones gubernamentales hasta empresas privadas y usuarios individuales. Asimismo, analiza los avances efectuados por las diferentes autoridades gubernamentales para enfrentar adecuadamente los retos que se les presentan en un mundo cada día más conectado y dependiente de las TIC.

La investigación y la redacción de este informe fue resultado de la labor conjunta de la Organización de Estados Americanos y Symantec, con la colaboración y el apoyo adicionales de AMERIPOL, Microsoft, el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), la Corporación para la Asignación de Nombres y Números en Internet (ICANN) y el Grupo de Trabajo Antiphishing (APWG). La OEA y AMERIPOL recurrieron a su red de contactos oficiales con los gobiernos de la región y, en particular, a los organismos o instituciones nacionales responsables de la implementación de acciones vinculadas con la seguridad cibernética y el delito cibernético.[01] Symantec reunió información por medio de su red internacional, constituida por más de 41.5 millones de sensores, que registran miles de eventos por segundo. Los datos sobre *spam*, *phishing* (suplantación de identidad) y *malware* (programas maliciosos) que suministró Symantec se capturan mediante diversas fuentes, entre las que se incluye un sistema de más de 5 millones de cuentas señuelo y una red de detección de amenazas que procesa más de 8,400 millones de mensajes de correo electrónico por mes y más de 1,700 millones de solicitudes *web* diarias en 14 centros de datos. Otros colaboradores aportaron información según sus respectivas áreas de conocimientos y experiencia. Por ejemplo, en la investigación de la ICANN, se analiza la estabilidad de Internet en América; el informe del APWG enumera los ataques de *phishing* y *malware* perpetrados en la región, y la información proporcionada por Microsoft se centra en tendencias generales en materia de seguridad cibernética, con especial atención al *malware*. La investigación del LACNIC, en cambio, tiene como eje las implicaciones del sistema global de ruteo de Internet en lo que respecta a seguridad y resiliencia cibernética.

Los datos proporcionados por las autoridades gubernamentales, así como los recopilados por Symantec y otros brindaron información de utilidad en lo referente a las tendencias observadas en la región, los pasos que se adoptan para darles respuesta y las áreas en las que todavía existen brechas o deficiencias significativas.

01 Las diferentes autoridades gubernamentales aportaron información de manera voluntaria y tuvieron la posibilidad de indicar si esa información podía hacerse pública o debía mencionarse como proveniente de fuente anónima.

Resumen ejecutivo

También 2013 fue un año de importancia para las actividades relativas a la seguridad y el delito cibernético en América Latina y el Caribe. La brecha digital siguió reduciéndose, en un período en que la región volvió a registrar algunos de los índices de crecimiento de la conectividad más altos del mundo. Más usuarios, más dispositivos y sistemas, más redes y más servicios representaron más oportunidades y beneficios para más personas. Sin embargo, también significaron más amenazas y vulnerabilidades, más víctimas y mayores costos, financieros y de otros tipos.

Los gobiernos de la región se esforzaron por mantenerse al día con un contexto en evolución y lograron algunos avances notables, tanto a nivel regional como nacional. A nivel regional, a pesar de la existencia de obstáculos y complicaciones persistentes, las autoridades nacionales competentes, entre ellas los equipos de respuesta ante incidentes cibernéticoss (CSIRT, también denominados comúnmente CERT o CIRT) y los organismos policiales, compartieron más información y cooperaron a nivel técnico con mayor intensidad que en el pasado, a menudo con resultados positivos. Para muchos países, la cooperación en tiempo real en respuesta a incidentes o actividades delictivas que estaban teniendo lugar se volvió más frecuente, además de más eficiente y eficaz. Los socios regionales e internacionales siguieron desempeñando un papel clave en lo que respecta a reunir a los funcionarios gubernamentales con el fin de desarrollar capacidades, fortalecer relaciones y compartir conocimientos y experiencias, además de brindar asistencia a cada gobierno según sus necesidades específicas. Y si bien las iniciativas orientadas a elaborar estándares regionales oficiales no han dado frutos, no caben dudas de que se han elevado las expectativas acerca de lo que se espera de las autoridades nacionales para aumentar la seguridad del dominio cibernético.

En efecto, en 2013 muchos países lograron importantes avances en la elaboración de sus políticas y marcos jurídicos, y en el desarrollo de su capacidad técnica. Al menos cuatro gobiernos —Guyana, Jamaica, Trinidad y Tobago y Barbados— efectuaron progresos significativos en lo que respecta a establecer o poner en marcha un equipo u organismo nacional de respuesta ante incidentes cibernéticoss. Otros gobiernos han iniciado procesos tendientes al mismo fin. Si bien solo un país de América, Trinidad y Tobago, adoptó formalmente una Estrategia de Seguridad Cibernética Nacional, la OEA e instituciones asociadas empezaron a trabajar con otros tres países con ese objetivo. En el transcurso del año, entraron en vigor numerosas leyes, que fortalecieron los marcos jurídicos y permitieron a las autoridades nacionales dar mejor respuesta a actividades informáticas maliciosas o delitos que involucraron el uso de las Tecnologías de la Información y la Comunicación (TIC), así como investigarlos con más eficacia y procesar a sus autores.

Las inversiones en capacitación y desarrollo de capacidades mostraron resultados tangibles, pues las autoridades responsables de la gestión de incidentes o la investigación de delitos cibernéticos respondieron con más rapidez y eficacia, lo que permitió mitigar el impacto de los ataques y aprehender a más delincuentes. En varios de los informes por país, se destacan ejemplos de estos resultados.

Muchos países intensificaron sus actividades de concientización en 2013, al haber comprendido que el conocimiento —de los riesgos que entraña el uso de las TIC y de cómo minimizar y mitigar tales riesgos— es, sin duda, la más valiosa herramienta que las autoridades nacionales pueden desarrollar y utilizar para mejorar la seguridad cibernética y combatir el delito cibernético. Se implementaron iniciativas innovadoras de divulgación de información, campañas de concientización y programas

educativos dirigidos a todas las partes interesadas: personal estatal, empresas, bancos y otras organizaciones privadas, estudiantes y público en general. La campaña PARA.PIENSA.CONÉCTATE, llevada adelante por una variedad de actores, siguió cobrando impulso en América. En la actualidad, incluye a cinco gobiernos participantes y otros actores de la región, mientras que varias autoridades nacionales se encuentran analizando la posibilidad de sumarse.

A pesar de los importantes avances logrados, lo más importante que la experiencia de 2013 deja como lección es la necesidad de que todos los involucrados redoblen sus esfuerzos en lo que concierne a reformar leyes y políticas, desarrollar capacidad técnica, generar mayor conciencia, compartir información y cooperar con otras partes interesadas.

Persiste un notable desequilibrio en lo que respecta a la situación de cada país en términos de desarrollo vinculado con la seguridad cibernética. En algunos países, se han desarrollado avanzadas capacidades técnicas y de investigación integrados, y se encuentran en vigor las leyes necesarias para utilizar a pleno tales fortalezas. Otros, en cambio, se encuentran aún en el punto de partida o muy cerca de él, y todavía lidian con los retos que entraña determinar qué acciones poner en práctica, quiénes deben participar y cómo distribuir del mejor modo recursos humanos y financieros limitados. Estos gobiernos pueden aprovechar la experiencia y los conocimientos de sus pares más avanzados, por lo que es necesario desarrollar e intensificar iniciativas orientadas a fomentar y facilitar esa clase de cooperación horizontal y desarrollo de potencial. La OEA y otros actores regionales e internacionales pueden desempeñar un rol fundamental en ese sentido, y deben seguir adaptando las iniciativas de desarrollo de capacidad a las necesidades de cada país, intercambiar lecciones aprendidas y prácticas recomendadas en materia de desarrollo de seguridad cibernética, y seguir propiciando el establecimiento de asociaciones más sólidas para beneficio de los Estados que reciben asistencia.

Ni siquiera los países más avanzados de la región pueden correr el riesgo de adoptar una actitud de complacencia. Los datos proporcionados por las autoridades nacionales y recopilados por Symantec correspondientes a América Latina y el Caribe, muestran sin lugar a dudas incrementos significativos del volumen de delitos cibernéticos, ataques y otros incidentes en casi todos los países del hemisferio.

Los incidentes denunciados con mayor frecuencia dirigidos contra usuarios individuales involucraron *phishing*, seguido de robo de la identidad de una persona para cometer fraudes financieros o a través de las redes sociales. El último tipo de incidente parece ir de la mano de la expansión de las redes sociales y sus comunidades de usuarios, que en la actualidad existen en todos los Estados Miembros de la OEA en números crecientes, y se refleja en el aumento de la cantidad de denuncias de incidentes que involucran difamación, amenazas y *cyber-bullying* (acoso en la *web*). El incremento del uso de servicios bancarios electrónicos dio origen a un aumento paralelo de los actos de defraudación contra bancos y clientes, lo que ha provocado pérdidas financieras inmensas, que sin embargo no son denunciadas en toda su magnitud. El acceso no autorizado a los sistemas y a la información que contienen es otra área de riesgo significativa en la que las autoridades observaron un aumento de la cantidad de incidentes, que involucran, en particular, empresas privadas y pequeñas y medianas empresas (PyME). Ante esos escenarios, es cada vez más frecuente el uso de *ramsomware* (secuestro cibernético), por ejemplo Cryptolocker, con el fin de obtener dinero a cambio de restaurar archivos. Muchas autoridades informaron, asimismo, que registraban un aumento de la cantidad de ataques de denegación de servicio contra sitios *web* gubernamentales y privados. Resulta interesante, sin embargo, que varios países informaran una disminución del vandalismo de sitios *web* y otros actos de "*hacktivismo*", lo cual puede reflejar las acciones llevadas a cabo por los gobiernos para identificar a los autores de incidentes anteriores.

En general, como resultado del aumento del volumen de la actividad ilícita y de la sofisticación de las herramientas y técnicas pertinentes, se ha incrementado la presión que reciben los gobiernos para no quedarse atrás. El personal responsable de la detección, la respuesta y la investigación se esfuerza por mantenerse al día con las últimas tecnologías y herramientas delictivas, y por desarrollar y mantener su competencia en áreas especializadas como la ciencia forense digital, la detección de intrusiones y el análisis de *malware* y vulnerabilidades, entre otros.

A pesar de toda la atención que legítimamente se presta a los ciberataques e incidentes de seguridad más sofisticados que involucran *malware* y técnicas de *hackeo*, no puede pasarse por alto que la prevalencia de las TIC en todos los aspectos de nuestra vida también ha dado lugar al incremento de su empleo en muchos delitos tradicionales, tanto los perpetrados por individuos como por grupos delictivos organizados. La pornografía infantil y otras formas de explotación de niños y menores de edad sigue siendo la más vasta de las áreas de actividad delictiva en la web, a pesar de la enorme cantidad de iniciativas nacionales e internacionales orientadas a impedirla. El tráfico de armas y drogas y la trata de personas también resultan facilitados por las TIC e Internet. Esta situación ha generado la imperiosa necesidad de que las autoridades policiales y judiciales sean capaces de investigar y procesar delitos que tienen lugar en un ecosistema cibernético cada día más complejo, mediante el uso del análisis forense digital, la preservación de evidencia digital y la presentación de esa evidencia en los tribunales. Para desarrollar esa capacidad, sin embargo, es imprescindible contar con recursos financieros y humanos de los que pocos organismos policiales disponen en abundancia, en caso de tenerlos.

Las experiencias recientes también confirman que los gobiernos nacionales no pueden ocuparse por sí solos de garantizar la seguridad del dominio cibernético. Por ser las propietarias y operadoras de la mayoría de las infraestructuras críticas y sistemas de la región, y las proveedoras de la mayor parte de los servicios en línea, a las entidades del sector privado les corresponde igual responsabilidad en el fortalecimiento de la resiliencia cibernética y la lucha contra el delito cibernético. Las autoridades gubernamentales y los actores clave del sector privado deben redoblar sus iniciativas para propiciar el diálogo y el intercambio de información, desarrollar confianza mutua e identificar y aprovechar las oportunidades de colaboración. Establecer relaciones y mecanismos de intercambio de información y cooperación entre autoridades nacionales y empresas radicadas fuera de la región, por ejemplo en los Estados Unidos, plantea un desafío que deberá enfrentarse con particular urgencia.

Al mencionar sus motivaciones para intensificar los esfuerzos en materia de seguridad cibernética, muchas autoridades nacionales destacaron que la filtración de información gubernamental había sido un catalizador que precipitó acciones en todo el hemisferio. Amplios sectores de la sociedad han comprendido el papel que desempeña la seguridad cibernética en lo referente a garantizar la protección adecuada de la privacidad y las libertades individuales, en una era digital en rápida evolución. Si bien es esperable que las autoridades nacionales procuren proteger sus activos e información frente a la posible violación de su seguridad por parte de otros gobiernos, es vital que tales actividades no afecten la posibilidad de trabajar con otros países de manera más colaborativa y franca, ni alejen a los gobiernos de tal colaboración.

Considerada en conjunto, la trayectoria de las iniciativas en materia de seguridad y delito cibernético emprendidas por los gobiernos de América Latina y el Caribe fue positiva en 2013. Se efectuaron importantes avances y progresos, como resultado de los pasos concretos que adoptaron los gobiernos para impulsar su capacidad de proteger el propio domino cibernéticos, así como de disuadir y castigar los actos de delito cibernético. No obstante, resta mucho más por hacer aún, visto el indudable aumento de las actividades de quienes causan daño aprovechando las vulnerabilidades del dominio cibernético y los crecientes costos que esas actividades conllevan para todos nosotros.

Organización de los
Estados Americanos

Symantec™

TENDENCIAS DE SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE

Las tendencias más importantes de 2013

El ciberespionaje, las preocupaciones en materia de privacidad y el personal interno malintencionado fueron noticia y ocuparon un lugar destacado en las discusiones sobre seguridad cibernética en 2013. No obstante, varias violaciones de datos a gran escala hacia el final del año, pusieron de manifiesto que los delitos cibernéticos siguen proliferando y que la amenaza de los ciberdelincuentes sigue acechando a gobiernos, empresas y usuarios finales. Los delitos cibernéticos continuaron devengando grandes beneficios, mientras que la perspectiva de capturar a los *hackers* y estafadores en línea demostró ser limitada en todas las jurisdicciones. Estos factores fueron en parte responsables de los altos costos de los delitos cibernéticos en 2013. Si bien es difícil medir esos costos por motivos inherentes, se estima que ascendieron a por lo menos USD 113,000 millones, suma suficiente para comprar un iPad a toda la población de México, Colombia, Chile y Perú.[01] Solamente en Brasil, los costos de los delitos cibernéticos alcanzaron los USD 8,000 millones, seguidos por México con USD 3,000 millones y Colombia, con USD 464 millones.[02] A nivel mundial, una de cada ocho violaciones de datos dieron como resultado la exposición de 10 millones de identidades; además, la cantidad de ataques dirigidos se incrementó. Al mismo tiempo, la actitud laxa de los usuarios finales respecto de las redes sociales, junto con la mayor adopción de dispositivos móviles condujo al aumento de estafas y generó mayores oportunidades para los ciberdelincuentes, en un momento en que el uso de las redes sociales en dispositivos móviles desempeña un papel preponderante cada vez mayor en la vida cotidiana, en especial en América Latina y el Caribe.

Tomada como región, América Latina y el Caribe tienen la población de usuarios de Internet de más rápido crecimiento del mundo, con 147 millones de usuarios únicos en 2013, lo que representó un aumento de 12% respecto de 2012.[03] Los dispositivos móviles se están transformando rápidamente en el método preferido de acceso a Internet, especialmente para usar las redes sociales. Casi 95% de los usuarios de Internet en la región utilizan sitios de redes sociales de forma activa y las naciones de América Latina y el Caribe ocupan 5 de los primeros 10 puestos de mayor tiempo de uso de redes sociales.[04] Si bien hoy la región de América Latina y el Caribe representa sólo un pequeño porcentaje de los delitos cibernéticos perpetrados en el mundo, el aumento en el uso de Internet y de los ataques cibernéticos relacionados enfatiza la necesidad de desarrollar políticas y defensas eficaces en materia cibernética.

Este informe abarca la amplia gama de amenazas que afecta a la región de América Latina y el Caribe. Resalta varias tendencias clave e identifica las amenazas específicas que se pusieron de manifiesto a partir del análisis de sus datos realizado por Symantec y de los resultados de encuestas brindados por los Estados Miembro de la OEA.

El 2013 fue el año de las grandes violaciones a la seguridad cibernética

Además de la proliferación de violaciones de seguridad cibernética con fines financieros, los *hackers* se infiltraron en decenas de empresas y gobiernos, incluidas muchas instituciones de América Latina y el Caribe, para lograr acceso a información confidencial. Se produjeron 253 violaciones de datos a gran escala en 2013, lo que representó un aumento de 62% respecto de 2012.[05] Ocho de estas violaciones de datos expusieron 10 millones de identidades o más cada una, lo cual obligó a comerciantes minoristas, empresas financieras, de seguros y personas físicas, a invertir una gran cantidad de tiempo y recursos financieros para responder y recuperarse de esos ataques e implementar mecanismos de protección adicionales. En comparación, durante 2012 una sola violación de datos expuso más de 10 millones de identidades.[06]

En 2013, se utilizaban las violaciones de datos en Puntos de Venta (PoS) como el principal vector de ataque para robar la información de identificación personal (PII) de los clientes. El gráfico de la página siguiente detalla la arquitectura de una violación de datos en un PoS y presenta algunos de los métodos que utilizan los cibercriminales para ingresar a los sistemas de PoS de las empresas de manera ilegal.

Fig. 1

VIOLACIONES DE DATOS EN PUNTOS DE VENTA (PoS)

ETAPAS

Fuente: Symantec

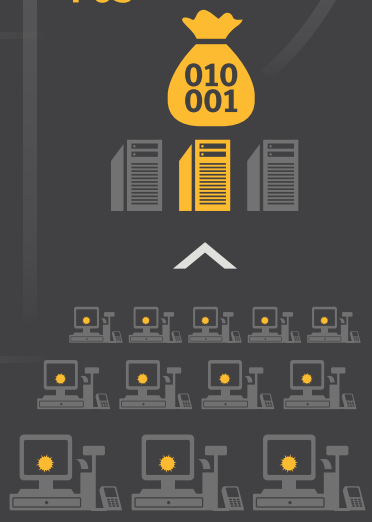
01 INFILTRACIÓN El atacante logra ingresar a la red corporativa mediante *spearphishing*, servidores vulnerables y otros métodos tradicionales

02 FUGA EN PUNTOS DE VENTA El atacante busca puntos de acceso a la red del punto de venta

03 HERRAMIENTAS DE ROBO DE DATOS El atacante instala *malware* en los sistemas del PoS para robar los datos de las tarjetas de crédito

04 PERSISTENCIA Y CAUTELA El *malware* roba los datos luego de cada transacción con tarjeta de crédito y, con el tiempo, acumula una gran cantidad de datos robados

05 PRUEBAS El atacante secuestra el sistema interno para su "servidor de pruebas" – y acumula datos de **miles de sistemas de PoS**



06 EXFILTRACIÓN Se exfiltran los datos obtenidos a un servidor externo, como un servidor de un tercero en la nube que ha sido comprometido

Fig. 2

Análisis de *emails* de tipo *spear-phishing* usados en los ataques dirigidos (global)

Fuente: Symantec

Tipo ejecutable	2013	2012
.exe	31.3%	39%
.scr	18.4%	2%
.doc	7.9%	34%
.pdf	5.3%	11%
.class	4.7%	<1%
.jpg	3.8%	<1%
.dmp	2.7%	1%
.dll	1.8%	1%
.au3	1.7%	<1%
.xls	1.2%	5%

- *Más de 50 % de los archivos adjuntos a los correos electrónicos usados en ataques tipo spear-phishing en 2013 contenían archivos ejecutables*
- *Se utilizaron documentos con formato PDF o Microsoft Word de forma regular. Estos documentos representaron 7.9% y 5.3% de los archivos adjuntos respectivamente. Sin embargo, estos porcentajes han disminuido respecto de 2012*
- *Los archivos Java con extensión .class representaron 4.7% de los archivos adjuntos utilizados en ataques de tipo spear-phishing*

En total, más de 552 millones de identidades se expusieron durante 2013 en todo el mundo, lo que permitió a distintos delincuentes acceder a información sobre tarjetas de crédito, fechas de nacimiento, números de documentos de identidad, domicilios particulares, historias clínicas, números de teléfono, información financiera, direcciones de correo electrónico, claves de acceso, contraseñas y otra clase de información personal.[07] Para comprender la magnitud del delito, podemos señalar que las tarjetas de crédito robadas pueden venderse por un valor de hasta USD 100 en el mercado negro, lo que hace de las violaciones de datos una actividad sencilla y de bajo riesgo para los ciberdelincuentes, pero sin duda rentable.[08]

Los ataques dirigidos crecen y evolucionan

El principal método de ataque desde principios de 2000 ha sido el uso de *malware* o programa malicioso para robar información sensible o confidencial. Un ataque dirigido utiliza *malware* orientado a un usuario o grupo de usuarios específico dentro de una organización en especial. Este *malware* puede distribuirse mediante un correo electrónico de tipo *spear-phishing* (ataques dirigidos) o una forma de infección a través de sitios *web* conocida como ataque "*watering-hole*". El *spear-phishing* es un correo electrónico diseñado con ingeniería social con el objeto de engañar a una persona o un pequeño grupo de personas y realizar un ataque dirigido. Un ataque "*watering-hole*", por su parte, requiere que los atacantes infiltren un sitio *web* legítimo visitado por sus víctimas, instalen un código malicioso y luego esperen que estas víctimas caigan en la trampa. Los ataques dirigidos en América Latina y el Caribe no sólo siguen creciendo sino también evolucionando.

Si bien el *spear-phishing* fue alguna vez el método preferido para instalar *malware*, los ataques "*watering-hole*" lo están reemplazando poco a poco en la región. Esto no significa que los ataques tipo *spear-phishing* estén en desuso. Si bien ha disminuido la cantidad total de correos electrónicos utilizados y víctimas por campaña de *spear-phishing*, en 2013 hubo un aumento de 91% en la cantidad de campañas.[09] Esto indica que los cibercriminales están realizando mayores esfuerzos y diseñando estos ataques para dirigirlos a víctimas potenciales en América Latina y el Caribe. Las tres fuentes principales de ataques de *phishing* en América Latina y el Caribe son Brasil, Colombia y Argentina. De hecho, estos tres países aportan 74% de todos los ataques de *phishing* en América Latina y 3.2% a nivel mundial.[10]

Estos enfoques "bajos y lentos" —las campañas duraron en promedio tres veces más que las de 2012, y pasaron de 3 a 8 días de duración— indican que la mayor conciencia de los usuarios y las tecnologías de protección han obligado a los cibercriminales que utilizan ataques tipo *spear-phishing* a mejorar sus métodos de ingeniería social para dirigir el ataque a sus víctimas potenciales de manera más precisa. También hemos notado la exitosa integración por parte de los cibercriminales de ataques virtuales y físicos en esquemas de ingeniería social.[11]

En 2013, más de 50% de los archivos adjuntos usados en los ataques de *spear-phishing* a nivel mundial contenían archivos ejecutables. Estos archivos son potencialmente peligrosos ya que pueden contener *malware* o pequeños programas para infectar la máquina de un usuario. También se utilizaron documentos con formato PDF o Microsoft Word de forma regular. Estos documentos representaron 7.9% y 5.3% de los archivos adjuntos, respectivamente.[12]

Fig.3

ATAQUE DIRIGIDO

ETAPAS CLAVE

Fuente: Symantec

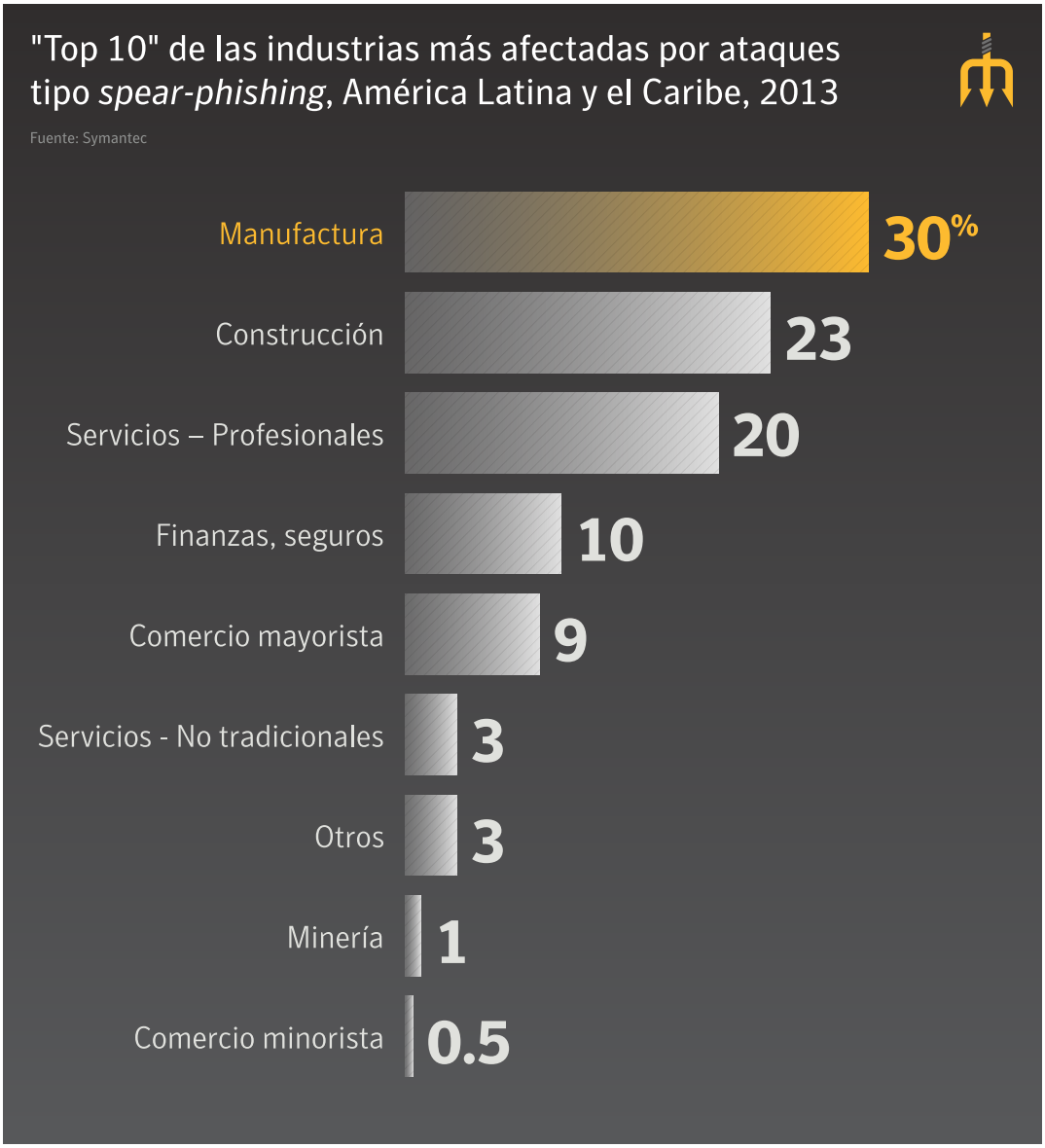
01 INCURSIÓN El atacante logra el ingreso a la organización víctima. En general, se realizan actividades de reconocimiento previo que permitan encontrar la táctica de ingeniería social adecuada.

02 DESCUBRIMIENTO Una vez que el atacante ha logrado el ingreso; procurará mantenerlo y descubrir a qué datos y otros recursos valiosos desea acceder.

03 CAPTURA Luego de descubrir e identificar los datos valiosos, el atacante encontrará la forma de recopilarlos antes de intentar exfiltrarlos.

04 EXFILTRACIÓN El atacante encontrará un mecanismo para robar los datos de la organización víctima. Para lograrlo, puede subir los datos a un servidor o sitio web remoto. Otros métodos más discretos pueden incluir la encriptación y esteganografía, para hacer el proceso de exfiltración aún más difícil de detectar, como esconder datos dentro de paquetes de petición de DNS.

Fig. 4



- *La industria manufacturera fue la más afectada en 2013, y representó 30% de todos los ataques perpetrados en América Latina*
- *La categoría de servicios profesionales incluye servicios contables y jurídicos, de ingeniería y de salud*
- *La categoría de servicios no tradicionales incluye servicios comerciales, de entretenimiento y reparaciones*

Caso de estudio: La Máscara [13]

Antecedentes

En general, se define a las campañas de ciberespionaje modernas por su nivel de sofisticación y profesionalismo. El grupo de ciberespionaje conocido como "La Máscara" no es la excepción. Según las investigaciones, este grupo opera desde 2007, y utiliza herramientas y técnicas innovadoras para comprometer, monitorear y exfiltrar datos de las víctimas infectadas. Utilizan *exploits* (códigos que aprovechan vulnerabilidades de seguridad) de alta gama y correos electrónicos cuidadosamente diseñados para atraer a víctimas desprevenidas. La Máscara cuenta con las herramientas necesarias para infiltrarse en todos los principales sistemas operativos, incluyendo Windows, Linux y Macintosh.

Cabe señalar que "La Máscara" utiliza herramientas específicamente diseñadas para atacar a víctimas de habla hispana. Por ejemplo, el *malware* está diseñado para buscar documentos en nombres de ruta en español, como "Archivos de Programas" en vez de "*Program Files*." Aparentemente, las víctimas potenciales residen principalmente en Europa y Sudamérica, y La Máscara parecería ser una de las primeras amenazas persistentes avanzadas (APT) creadas por hablantes hispanos o diseñadas para su uso en América Latina.[14]

La longevidad de la operación

Ésta, ha estado activa durante siete años, el acceso a las herramientas altamente sofisticadas, y la naturaleza precisa y selectiva de las víctimas indican que se trata de una estructura profesional, así como de un equipo de atacantes bien organizado y con recursos sustanciales.

Ataque a la víctima

La Máscara suele infectar a sus víctimas con un correo electrónico diseñado especialmente. Los archivos adjuntos generalmente tienen formato de documentos PDF o Microsoft Word, y utilizan como señuelo un CV (currículum) o contenido político para atraer a sus víctimas. A continuación, se incluyen algunos nombres de archivo adjunto utilizados:

- Inspirado por Islandia.doc
- DanielGarciaSuarez_cv_es.pdf
- cv-edward-horgan.pdf

Al abrir el documento, se muestra al destinatario del mensaje lo que parece ser un documento legítimo, sin embargo también se instala un troyano de acceso remoto (RAT), que permite acceso remoto total a la computadora afectada. Una vez infectado el equipo, La Máscara puede instalar herramientas adicionales que le permitan mejorar sus actividades persistentes de ciberespionaje.

Herramientas profesionales para el ciberespionaje

La Máscara cuenta con un conjunto de herramientas a su disposición. Una herramienta en especial diferencia a este grupo de las típicas ciberoperaciones. Backdoor.Weevil.B, una sofisticada herramienta de ciberespionaje de naturaleza modular; utiliza una arquitectura de complementos (*plug-in*) y una gran variedad de opciones de configuración.[15] Esta herramienta evoca a aquellas asociadas con otras campañas sofisticadas, como Duqu,[16] Flamer,[17] and MiniDuke.[18] Sin embargo, no hay pruebas que relacionen a La Máscara con estas campañas. La instalación predeterminada tiene casi 20 módulos desarrollados para cumplir funciones de intercomunicación, *network sniffing* (análisis del tráfico en la red), monitoreo de las actividades, exfiltración de datos y capacidades de *rootkit*.

La arquitectura de complementos permite cargar y descargar módulos adicionales según la necesidad. El troyano puede llevar un registro de la actividad en todos los navegadores principales y tiene una lista integral de las extensiones de archivo de donde puede recopilar información. Los documentos meta del troyano son:

01 Word, PDF, Excel

02 Archivos cifrados, claves PGP, claves de cifrado

03 Archivos de respaldo para dispositivos móviles

04 Archivos de correo electrónico

Luego, se puede utilizar el protocolo HTTPS para exfiltrar esta información de manera segura a servidores controlados por el atacante. El componente de robo de datos suministra pistas relativas a las víctimas potenciales de La Máscara. Busca documentos en nombres de rutas en español, por ejemplo "archivos de programa", lo que indica que sus víctimas utilizan sistemas operativos en español.

Cada vez son más comunes las campañas de ciberespionaje conducidas por equipos profesionales. En los últimos años, se han destacado gran cantidad de operaciones de espionaje de larga duración. Podemos citar, por ejemplo, a Flamer, MiniDuke y Hidden Lynx.[19] La Máscara se une a esta famosa lista y asimismo muestra que hoy estas campañas sofisticadas tienen como objetivo una mayor diversidad de víctimas. En coincidencia con estas campañas, han surgido empresas que desarrollan las herramientas necesarias para las campañas de espionaje. Empresas como Hacking Team y Gamma International ofrecen grupos de herramientas de acceso remoto que permiten desempeñar actividades sofisticadas de vigilancia. Todo esto pone en evidencia que el ciberespionaje está expandiendo sus barreras geográficas y técnicas.

Fig. 5

Algunos de los módulos de La Máscara

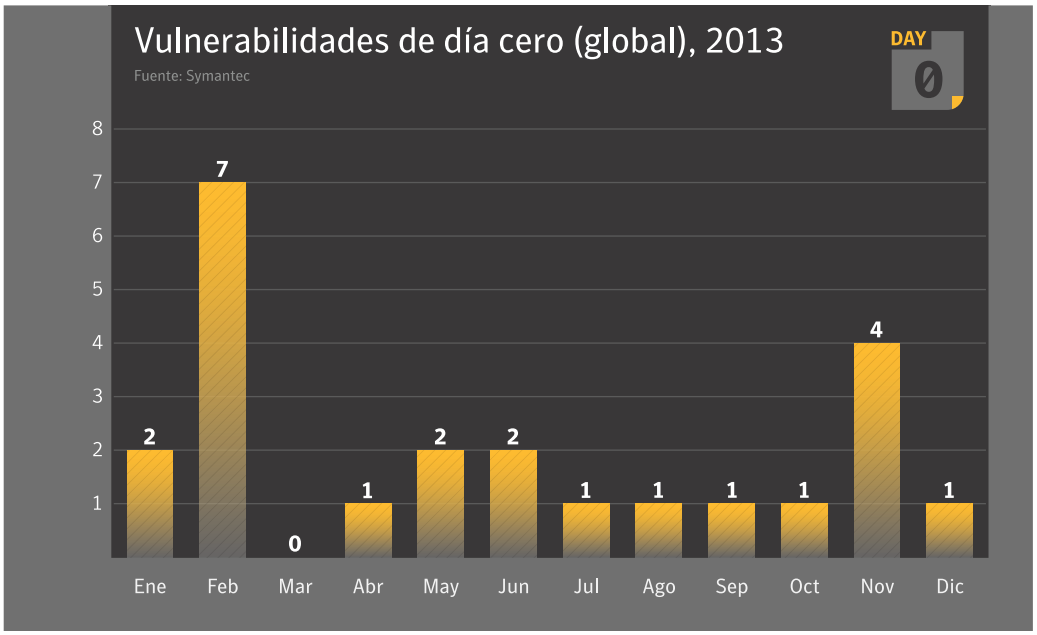
Las vulnerabilidades de día cero y los sitios *web* sin parches facilitaron los ataques de *watering-hole*

En 2013 los investigadores de seguridad descubrieron más vulnerabilidades de día cero que en cualquier otro año desde 2006. Las 23 vulnerabilidades de día cero que se descubrieron el año pasado representan un aumento de 61% en relación con 2012 y ascienden a un total que supera los dos años anteriores juntos.[20]

Las vulnerabilidades de día cero son vulnerabilidades contra las cuales ningún proveedor ha lanzado un parche todavía. La inexistencia de parches para las vulnerabilidades de día cero representa una amenaza tanto para organizaciones como para consumidores por igual, puesto que, en muchos casos, estas amenazas pueden evadir la detección puramente basada en firmas hasta tanto se lance un parche. Además, solo las vulnerabilidades de día cero brindan a los atacantes los medios para infectar a sus víctimas sin necesidad de utilizar adjuntos de correo electrónico, enlaces u otros métodos que puedan suscitar sospechas no deseadas. Los *hackers* simplemente aplican estos *exploits* en ataques de tipo *watering-hole*, evitando así la posibilidad de toparse con tecnologías *antiphishing* que les impidan continuar. Desafortunadamente, los sitios *web* legítimos pero con prácticas de gestión de parches deficientes han facilitado la perpetración de ataques *watering-hole*. En todo el mundo, 77% de los sitios *web* tenían vulnerabilidades explotables y uno de cada ocho sitios *web* presentaba una vulnerabilidad crítica.[21] Esto ofrece a los atacantes un sinnúmero de elecciones de sitios *web* donde ocultar sus programas maliciosos y entrampar a sus víctimas.

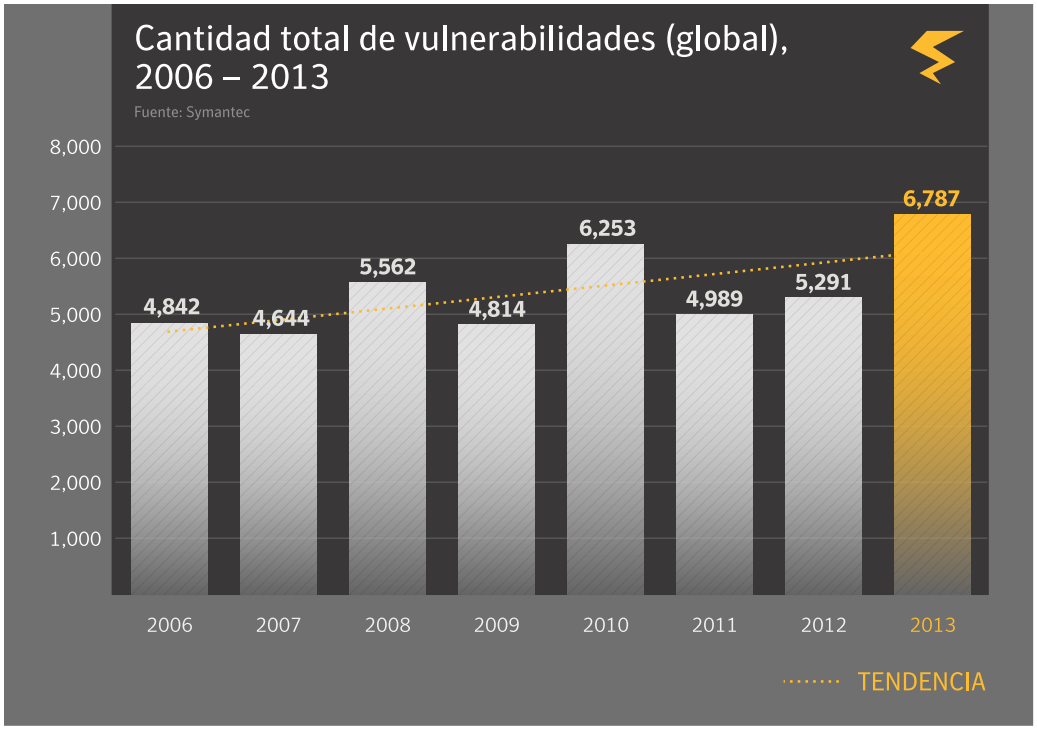
Los *hackers* más avanzados suelen dejar de explotar una vulnerabilidad de día cero una vez que esta se hace pública y, para evitar ser detectados, buscan emplear una vulnerabilidad alternativa. Pero ello no hace que deje de usarse. Los cibercriminales rápidamente incorporan a sus paquetes de herramientas estos *exploits* para vulnerabilidades de día cero, y esto nos amenaza a todos. Aunque los parches para las cinco vulnerabilidades de día cero más frecuentes estuvieron disponibles dentro de un período promedio de cuatro días, en 2013 se registraron al menos 174,651 ataques perpetrados aprovechando estas vulnerabilidades, ocurridos dentro de los primeros 30 días a partir de la publicación de la vulnerabilidad y la divulgación del parche. Los atacantes saben que suele haber una demora en la aplicación de los parches, lo cual genera un entorno muy ventajoso para los ataques.[22]

Fig. 6



- *Una vulnerabilidad de día cero es aquella que ha sido descubierta y explotada por los posibles atacantes antes de que se conozca su existencia y se publique un parche que las solucione*
- *En 2013, se documentaron 23 vulnerabilidades de día cero, comparadas con las 14 de 2012*
- *La cantidad pico de vulnerabilidades identificadas en un mes en 2013 fue de 7 (en febrero), comparadas con el pico mensual de 3 (en junio) en 2012*

Fig. 7



- *En 2013 se revelaron 6,787 vulnerabilidades, en comparación con las 5,291 de 2012*
- *En 2013 se registraron 32 vulnerabilidades en los sistemas SCADA (Supervisión, Control y Adquisición de Datos), en comparación con las 85 registradas en 2012 y las 129 en 2011*

Aumentaron los ataques con *ransomware* en la región y se volvieron más sofisticados

En 2013, los estafadores continuaron aprovechándose de *ransomware* (secuestro informático). A menudo, los atacantes se hacen pasar por agentes de las fuerzas de seguridad locales y así exigen el pago de una multa falsa, que suele oscilar entre USD 100 y 500, como condición para desbloquear una computadora que estaba supuestamente bloqueada, y que había sido usada por las autoridades durante una investigación. Estas amenazas aparecieron por primera vez en 2012, pero se intensificaron en 2013 y aumentaron 500% en todo el mundo ese mismo año.[23] América Latina y el Caribe, ciertamente, no han escapado a esta realidad. En abril de 2014, una propagación de *ransomware* llevó a la Policía de México a publicar un aviso formal.[24]

Los ataques de *ransomware* son sumamente rentables y con frecuencia se modifican para asegurar que sigan teniendo éxito. El paso siguiente de esta evolución fue el programa Ransomcrypt, conocido comúnmente como Cryptolocker. Este es el más prominente de los nuevos tipos de programas extorsivos. En lugar de hacerse pasar por un agente de la ley, el atacante solicita explícitamente una recompensa para descifrar archivos de usuarios que han sido atacados. Cryptolocker utiliza un cifrado RSA 2,048 de alto grado, que actualmente es imposible de descifrar. Salvo que un usuario haya hecho una copia de seguridad de sus datos antes del ataque de Cryptolocker, es probable que sus datos queden inaccesibles para siempre. Esta amenaza causa aún más daño a las empresas, pues también se afectan los archivos contenidos en unidades de redes compartidas o conectadas. Las investigaciones indican que, en promedio, 3% de los usuarios cuyas computadoras han sido infectadas pagan la recompensa, mientras que 97% restante pierde sus datos, o bien, debe contentarse con una copia de seguridad no actualizada.[25]

Retener archivos cifrados para obtener una recompensa no es una práctica totalmente nueva, pero, en el pasado, los delincuentes tenían dificultades para lograr el pago de la recompensa. Con el surgimiento de los métodos de pago *online*, Ransomcrypt tiene todo lo necesario para seguir creciendo en 2014. Los que están más expuestos al riesgo de perder datos, archivos o memorias

son las pequeñas empresas y los consumidores. La prevención y las copias de seguridad resultan cruciales para proteger a los usuarios contra este tipo de ataques.

Fig. 8 Ejemplo de ransomware dirigido a usuarios en Argentina

Fig. 9 Ransomware dirigido a usuarios en México

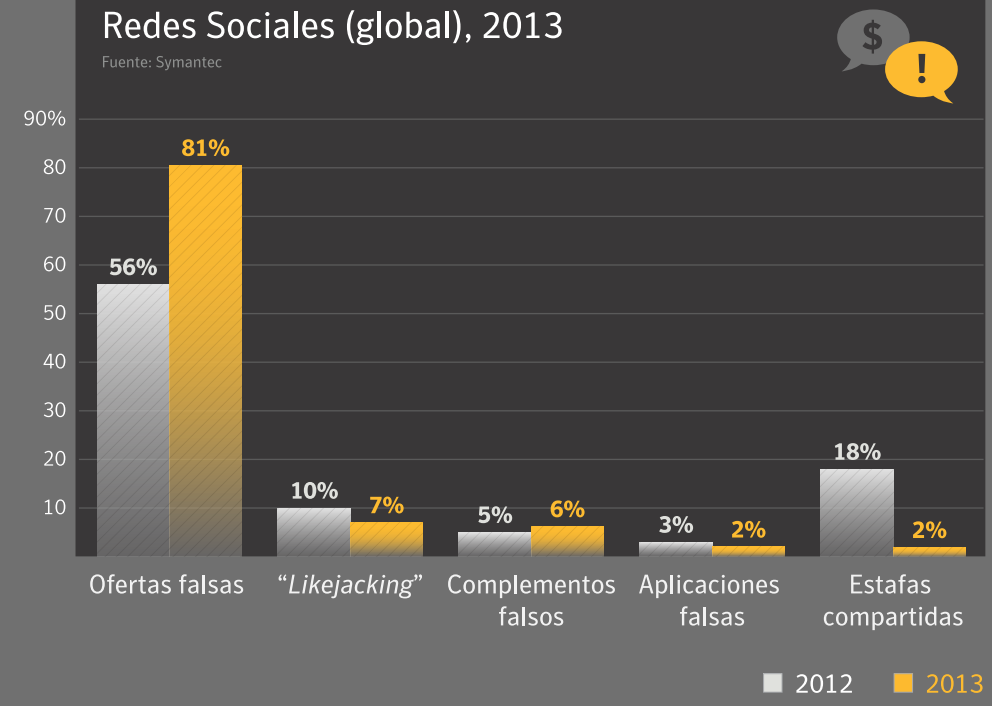
Prosperan en las redes sociales las estafas y el *malware* para dispositivos móviles

Si bien la preponderancia del *malware* móvil en todo el mundo sigue siendo baja en comparación con la de las computadoras portátiles y de escritorio, el año 2013 demostró que están dadas las condiciones para que aumenten significativamente las estafas y el *malware* destinados a los dispositivos portátiles. En 2013, una encuesta mundial a usuarios finales indicó que 38% de los usuarios de teléfonos celulares había experimentado delitos cibernéticos móviles en alguna de sus modalidades.[26] Los dispositivos perdidos o robados suelen precipitar actividades móviles maliciosas, aunque el comportamiento imprudente de los usuarios de teléfonos celulares los vuelve susceptibles a muchos tipos de ataques posibles.

En particular, los usuarios de teléfonos celulares demuestran un comportamiento imprudente cuando almacenan archivos sensibles *online* (52%), guardan información laboral y personal en las mismas cuentas de almacenamiento *online* (24%) y comparten contraseñas y claves de acceso con familiares (21%) y amigos (18%), lo cual pone en riesgo sus datos y los de sus empleadores.[27]

Sin embargo, solo 50% de esos usuarios toma las precauciones de seguridad más básicas, mientras que el resto descarta el uso de contraseñas o programas de seguridad en sus dispositivos móviles.[28]

Fig. 10



Ofertas falsas: Estas estafas invitan a los usuarios de las redes sociales a participar en un evento o grupo falso, con el incentivo de obtener tarjetas de regalo gratuitas, entre otros. Para participar, el usuario generalmente debe compartir sus credenciales con el atacante o enviar un texto a un número telefónico de tarificación adicional.

Estafas compartidas: Estas estafas cuentan con la ejecución por parte de las víctimas, quienes reciben videos que resultan muy atractivos, ofertas o mensajes falsos y los comparten con sus amigos, distribuyendo la estafa.

"Likejacking" (uso fraudulento del botón "Me gusta"): Los atacantes utilizan botones de "Me gusta" falsos que instalan *malware* al ser presionados por los usuarios y pueden publicar actualizaciones en las páginas de los mismos y así distribuir el ataque.

Estafas con complementos falsos: Se engaña a los usuarios para que descarguen a sus máquinas extensiones de navegadores falsas. Estas extensiones pueden parecer legítimas, pero al instalarlas roban información sensible de la máquina infectada.

Aplicaciones falsas: Se invita a los usuarios a suscribirse a aplicaciones que parecen estar integradas para el uso con una red social, pero en realidad se utilizan para robar credenciales o recopilar otros datos personales.

- *Las ofertas falsas representaron la mayor cantidad de ataques basados en medios sociales en 2013 —81%, en comparación con 56% de 2012*
- *Las estafas compartidas también descendieron en 2013 —de 18% en 2012 a 2% en 2013*
- *Las estafas basadas en "micro-blogging" representaron 1% del total de ataques detectados en la categoría de medios sociales, tanto para 2012 como 2013*

El ritmo al que se crean nuevas familias de *malware* disminuyó, puesto que los autores de estos programas maliciosos se abocaron a perfeccionar el *malware* existente. En 2012, cada familia de *malware* móvil tenía, en promedio, 38 variantes. En 2013, cada familia tenía, en promedio, 58.[29] Además, los eventos registrados en 2013 indican que los usuarios de dispositivos móviles son sumamente susceptibles a las estafas por medio de aplicaciones móviles. Parece ser que el *malware* móvil todavía no explotó, en parte debido a que los criminales potenciales tienen otros medios para lograr sus objetivos.

Los usuarios continúan siendo presas de estafas en los sitios de medios sociales, a menudo atraídos por una falsa sensación de seguridad que genera la presencia de tantas conexiones *online*. Las ofertas falsas, como las que simulan otorgar minutos de comunicación celular gratis, representaron el mayor número de incidentes maliciosos que afectaron a usuarios de Facebook en 2013 —81% en 2013 frente a 56% en 2012.[30] Pese a que 12% de los usuarios de redes sociales afirma que alguien consiguió entrar en su cuenta de una red social y asumió su identidad, un cuarto de esos usuarios continúa compartiendo sus contraseñas de acceso a las redes sociales y un tercio se conecta con personas que no conoce.[31]

En América Latina y el Caribe, casi 95% de los usuarios de Internet accede a sitios de redes sociales. Los países de América Latina y el Caribe representan cinco de los 10 países que más tiempo pasan en las redes sociales.[32] Puesto que el acceso a las redes sociales se realiza cada vez más mediante dispositivos móviles, es probable que todo comportamiento imprudente tenga consecuencias cada vez más graves para los usuarios y sus datos.

Copa Mundial de la FIFA 2014: objetivo tentador para los cibercriminales

Se espera que la Copa Mundial de la FIFA 2014, que se llevará a cabo en Brasil, sea uno de los sucesos deportivos más grandes de este siglo. Mientras que el mundo se reúne para celebrar y competir deportivamente, los delincuentes cibernéticos, por desgracia, han identificado vulnerabilidades y es posible que estén tramando ataques contra la infraestructura.[33] De hecho, miembros de grupos internacionales de *hackeo*, como Anonymous, recientemente amenazaron sitios *web* oficiales administrados por la FIFA, el Gobierno brasileño y patrocinadores corporativos de los juegos.

Ya se descubrieron varias operaciones de *malware*, ataques de *phishing* y estafas por correo electrónico relacionados con la Copa Mundial. Un ardid en particular involucra una publicidad fraudulenta denominada CIELO Brasil, que emplea la modalidad de *spear-phishing* (ataque dirigido a un grupo concreto de personas o empresas). Los usuarios son redirigidos a una página *web* donde se les solicita ingresar su nombre de usuario, fecha de nacimiento y código brasileño de identificación tributaria (CPF).

Otro ataque relacionado con la Copa del Mundo que descubrió este año Symantec fue una operación sofisticada de *malware* dirigida a instituciones financieras. Cuando el usuario hace clic en el correo electrónico infectado para descargar una "entrada gratis" para la Copa Mundial, se lo induce a descargar un archivo infectado denominado "eTicket.rar" que, a los ojos del usuario desprevenido, puede parecer inofensivo. Hecho esto, un archivo denominado "thanks.exe" (Infostealer.Bancos)[34] se aloja en el sistema y se ejecuta cada vez que se inicia Windows.

El troyano continuará ejecutándose en un segundo plano mientras evade las medidas de seguridad para robar información financiera confidencial, registrar los datos robados y enviarlos más tarde a un atacante remoto.

Los usuarios de América Latina y el Caribe deben estar en guardia antes y durante el campeonato para protegerse contra trampas de *malware* o *phishing* como las que se mencionaron aquí.[35] Además de la amenaza que representa la Copa Mundial, es probable que los Juegos Olímpicos de Río de Janeiro 2016 sean un objetivo destacado para los cibercriminales que emplean *malware, phishing*, estafas por correo electrónico y ataques a la infraestructura bancaria. En los Juegos Olímpicos de Invierno de Sochi 2014, así como en los Juegos Olímpicos de Londres 2012, se observaron tendencias cibernéticas similares, lo cual indica que durante la Copa Mundial y otros eventos deportivos importantes habrá actividades semejantes.

Fig. 11 Al hacer clic en el vínculo, se procede a la descarga maliciosa del malware Infostealer.Bancos.

Asaltos y troyanos bancarios

En toda América Latina y el Caribe han aumentado los incidentes relacionados con los asaltos y troyanos bancarios. Las amenazas actuales siguen concentradas en modificar sesiones bancarias e inyectar campos adicionales con la esperanza de robar información bancaria sensible o secuestrar la sesión. Algunos de los troyanos bancarios más comunes de este año incluyen Trojan.Tylon[36] y una variante del botnet Zbot llamada Gameover Zeus.[37] Infostealer.Bancos aparece con mucha frecuencia en América Latina y el Caribe. El informe "El Estado de los troyanos financieros: 2013" de Symantec concluyó que en los primeros tres trimestres de 2013 se triplicó el número de troyanos bancarios.[38] Aunque más de la mitad de estos ataques apuntaban a las principales 15 instituciones financieras, más de 1,400 instituciones fueron víctimas en 88 países de todo el mundo. Los ataques basados en navegadores siguen siendo moneda corriente, pero se utilizan también amenazas móviles para eludir la autenticación a través de mensajes de texto (SMS), que permiten a los atacantes interceptar mensajes de texto del banco de la víctima.

La forma más común de ataque sigue siendo un troyano financiero que realiza un ataque del tipo "hombre en el navegador" (MITB) en la computadora del cliente durante una sesión bancaria en línea. En un ataque MITB, el *malware* reside en el navegador *web* del dispositivo de una persona y se interpone entre el usuario y el sitio *web*, cambiando lo que ve el usuario y alterando la información de su cuenta y finanzas sin que éste lo note. Symantec analizó 1,086 archivos de configuración de 8 de los troyanos financieros más comunes. El *malware* se configuró para buscar URL, o direcciones *web*, que pertenecen a 1,486 organizaciones diferentes de todo el mundo.

También se observó un aumento en ataques basados en *hardware* en 2013. Además de los aún populares ataques de *skimming* (clonación de tarjetas) en toda América Latina y el Caribe, se descubrió un nuevo tipo de *malware* llamado Backdoor.Plotus que atacaba cajeros automáticos (ATM).[39] Este *malware* fue inicialmente descubierto en México, para luego diseminarse a otros países, y sus versiones en inglés aparecieron más tarde.

Caso de estudio: Los criminales ganan el premio mayor de los cajeros automáticos

Ploutus es una nueva forma de robar dinero de la cuenta bancaria de un individuo, utilizada inicialmente por los criminales en México. Los cajeros automáticos siempre fueron un objetivo común de los ladrones, pero el desafío que presentan es cómo sacar el dinero de la máquina. Si bien hay muchas maneras de lograr este cometido, un método cada vez más popular es el *skimming* en cajeros automáticos. Es el proceso de grabar los datos de la banda magnética de una tarjeta de crédito o débito para poder usarla más adelante de forma fraudulenta. No es la forma más fácil, pero produce los datos más viables para su posterior venta por parte de los estafadores.

Lo que más les gustaría a los criminales es que un cajero automático escupiera todo el efectivo con solo presionar algunos botones. Desafortunadamente para los bancos, parece que los sueños de los criminales podrían hacerse realidad. En investigaciones paralelas con otras firmas de seguridad, Symantec identificó este *malware* el 31 de agosto de 2013 y añadió un sistema de detección (Backdoor.Ploutus), en funcionamiento desde el 4 de septiembre de 2013.

Método de infección

Según fuentes externas, el *malware* se transfiere al cajero automático insertando físicamente un nuevo disco de arranque en la unidad de CD-ROM ubicada en la parte externa de la unidad. Luego, el disco de arranque transfiere el *malware*.

Impacto

Los criminales crearon una interfaz para interactuar con el *software* en un cajero automático afectado y ahora pueden retirar todo el dinero disponible de los contenedores que guardan los billetes, también conocidos como casetes. Un aspecto interesante para destacar es que los criminales también pueden leer toda la información que ingresaron los dueños de tarjetas en el teclado del cajero automático, permitiéndoles así robar información sensible sin usar ningún dispositivo externo.

Acciones que realiza Backdoor.Ploutus

- Generación de ID de cajero automático:
  Número generado en forma aleatoria y asignado al cajero automático afectado. Se basa en el día y mes actuales al momento de la infección
- Activación de ID de cajero automático:
  Establece un temporizador para entregar dinero. El *malware* entregará dinero solo dentro de las primeras 24 horas desde su activación
- Entrega de efectivo:
  Entrega dinero según la cantidad solicitada por los criminales
- Reinicio (Servicio):
  Reinicia el período de entrega de dinero

La lista de comandos mencionados anteriormente debe ejecutarse en orden, ya que el *malware* debe usar un ID de cajero automático que no haya expirado para entregar el dinero.

El código fuente contiene nombres de función en español que sugieren que el *malware* puede ser obra de codificadores de habla hispana.

El proceso de entrega comprometido

Queda claro que los criminales han realizado un proceso de ingeniería inversa con el *software* del cajero automático y han producido una interfaz que les permite interactuar con la máquina. Esta afirmación se basa en el código que revisaron los expertos en seguridad de Symantec. Este descubrimiento resalta el nivel creciente de cooperación entre los criminales tradicionales que atacan activos físicos y los cibercriminales. Dado el uso cada vez mayor de la tecnología en todos los aspectos de la seguridad, los criminales tradicionales se están dando cuenta de que para poder realizar asaltos exitosos ahora necesitan otro conjunto de habilidades que antes no eran esenciales. Los ladrones de bancos actuales necesitan profesionales de TI con experiencia dentro de su equipo para que los ayuden a realizar sus asaltos.

Y desde entonces los criminales han comenzado a subir la apuesta. Poco después de que se descubriera a Backdoor.Ploutus,[40] se descubrió una variante similar del *malware*, Backdoor.Ploutus.B. Esta variante de Ploutus era especialmente interesante porque permitía a los cibercriminales simplemente enviar un mensaje de texto SMS al cajero automático afectado y luego acercarse y recoger el dinero entregado. Puede parecer increíble, pero en la actualidad esta técnica se usa en varios lugares de todo el mundo.

Conclusiones

El panorama actual en materia de amenazas cibernéticas en América Latina y el Caribe muestra que los usuarios están sufriendo el impacto de amenazas que son tendencia a nivel mundial y de otras propias de cada región. Como agravante de este desafío, América Latina y el Caribe tienen la población de usuarios de Internet de más rápido crecimiento del mundo, con un aumento de 12 por ciento durante el último año. Este informe identificó las principales tendencias que impactan a la región:

01 Las violaciones de datos están aumentando

En 2013, denominado "El año de las grandes violaciones de la seguridad cibernética", más de 552 millones de identidades quedaron expuestas a causa de violaciones de datos, lo que puso en riesgo los datos de tarjetas de crédito, financieros, médicos y otros tipos de información personal de los consumidores. El origen principal de esta tendencia fueron las violaciones de datos mediante delitos cibernéticos y los actos de *hacktivismo*: las actividades de los *hackers* representaron 32 por ciento de todas las violaciones de datos registradas en 2013.

02 Continúan en crecimiento los ataques dirigidos

Los ataques contra personas particulares u organizaciones están evolucionando, ahora que los delincuentes cibernéticos adaptan las campañas de *spear-phishing* (robo de identidad con objetivos específicos) para hacerlas más disimuladas y suman a su grupo de recursos los ataques denominados *watering-hole* (que se valen de las visitas a una página *web*).

03 Las estafas en redes sociales están a la alza

En 2013, los delincuentes cibernéticos se propusieron obtener los datos que compartimos en Internet a través de las redes sociales, y a medida que este tipo de sitios se vuelven cada vez más interconectados, la seguridad de nuestros datos e información personal en Internet cobra una importancia sin precedentes.

04 Troyanos bancarios y robos

En toda América Latina y el Caribe, la cantidad de incidentes que involucran troyanos bancarios aumentó considerablemente. El *malware* dirigido a cajeros automáticos, descubierto por primera vez en México, se ha extendido a otros países de América, especialmente en países hispanohablantes.

05 Los eventos de gran convocatoria son atractivos para los delincuentes

La Copa del Mundo de la FIFA ya es un vector importante para los delincuentes cibernéticos, que realizan incontables operaciones de *malware*, trucos de *phishing* y estafas por correo electrónico relacionadas con el campeonato. Acontecimientos globales tales como conciertos y eventos deportivos suelen ser atractivos para los delincuentes cibernéticos, y la Copa Mundial 2014 no es excepción. De hecho, durante las Olimpíadas de Invierno 2014 de Sochi y las Olimpíadas de Verano 2012 de Londres, muchas campañas dirigidas por correo electrónico usaron temas olímpicos para atraer a víctimas potenciales; un mensaje estaba vinculado a una peligrosa campaña de *malware* denominada "Darkmoon".[41]

Referencias

01 Symantec Corporation, *Reporte Norton 2013* (octubre 2013), 8. Disponible en: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

02 Symantec Corporation, *Reporte Norton 2013* (Colombia). Disponible en: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

03 Jason Kohn, "The Internet is Booming in Latin America, Especially Among Younger Users," *Cisco Blogs*, 17 de octubre de 2013. Disponible en: http://blogs.cisco.com/cle/the-internet-is-booming-in-latin-america-especially-among-younger-users/

04 Richard Simcott, "Social Media Fast Facts: Latin America," *Social Media Today*, 3 de abril de 2014. Disponible en: http://socialmediatoday.com/richard-simcott/2317236/social-media-fast-facts-latin-america

05 Symantec Corporation, *Informe anual sobre amenazas* 19 (April 2014), 40. Disponible en: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf Véase también el Índice de Cibercrimen de Norton

06 Ibíd. en 40.

07 Ibíd. en 40.

08 Symantec Corporation, "Underground Economy Servers – Goods and Services Available for Sale," Symantec Security Response, 2010. Disponible en: http://www.symantec.com/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

09 Symantec Corporation, *Informe anual sobre amenazas* 19, 25.

10 ISTR 19, en 33.

11 Symantec Corporation, "Francophoned – A Sophisticated Social Engineering Attack," *Symantec Security Response*, 28 de agosto de 2013. Disponible en: http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack

12 Symantec Corporation, *Informe anual sobre amenazas – Datos por región*, (abril 2014).

13 Stephen Doherty, "The Mask," *Symantec Security Response Blog*, 10 de febrero de 2014. Disponible en: http://www.symantec.com/connect/blogs/mask

14 Matthew Hilburn, "'Mask' Malware Called 'Most Advanced' Cyberespionage Operation," Voice of America, 13 de febrero de 2014. Disponible en: http://www.voanews.com/content/mask-careto-called-most-advanced-cyber-espionage-operation/1850889.html

15 *Véase* "Backdoor.Weevil.B," *Symantec Security Response*, 10 de febrero de 2014. Disponible en: http://www.symantec.com/security_response/writeup.jsp?docid=2014-021017-4904-99

16 *Véase* "W32.Duqu: The Precursor to the Next Stuxnet," *Symantec Security Response*, 11 de octubre de 2011. Disponible en: http://www.symantec.com/connect/http%3A/%252Fwww.symantec.com/connect/blogs/w32_duqu_precursor_next_stuxnet

17 *Véase* "Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East," *Symantec Security Response*, May 28, 2012. Disponible en: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east

18 *Véase* "Backdoor.Miniduke," *Symantec Security Response*, 27 de febrero de 2013. Disponible en: http://www.symantec.com/security_response/writeup.jsp?docid=2013-030119-2820-99

19 Symantec Corporation, "Hidden Lynx – Professional Hackers for Hire," *Symantec Security Response Blog*, 23 de enero de 2014. Disponible en: http://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire

20 *Symantec Informe anual sobre amenazas* (informe sobre las amenazas a la seguridad en Internet de Symantec) 19, en 38.

21 Ibíd. en 6.

22 Ibíd. en 6.

23 Ibíd. en 48.

24 "Mexican Police Issue 'Ransom Ware' Virus Warning", *Associated Press*, 10 de abril de 2014. Disponible en: http://www.41nbc.com/story/d/story/mexican-police-issue-ransom-ware-virus-warning/39517/Zt2c0Ra-hkmr8YT_vK1Wcg

25 Brian Krebs, "Inside a 'Reveton' Ransomware Operation", *KrebsOnSecurity*, 12 de agosto de 2013. Disponible en: http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

Referencias

26 Symantec Corporation, *Reporte Norton 2013*, (octubre de 2013), 7. Disponible en: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

27 *Symantec Informe anual sobre amenazas* 19, en 6.

28 *Reporte Norton 2013*, en 8.

29 Ibíd. en 6.

30 Ibíd. en 6.

31 *Reporte Norton* 2013, en 8.

32 *Véase* Simcott, 3 de abril de 2014.

33 Esteban Israel, "Hackers Target Brazil's World Cup for Cyber Attacks", *Reuters*, 26 de febrero de 2014. Disponible en: http://www.reuters.com/article/2014/02/26/us-worldcup-brazil-hackers-idUSBREA1P1DE20140226

34 *Véase* "Infostealer.Bancos", *Symantec Security Response*, 17 de julio de 2003. Disponible en: http://www.symantec.com/security_response/writeup.jsp?docid=2003-071710-2826-99

35 *Véase* Sean Butler, "Fraudsters and Scammers Kick Off Their Campaigns for the 2014 FIFA World Cup", *Symantec Security Response Blog*, 3 de febrero de 2014. Disponible en: http://www.symantec.com/connect/blogs/fraudsters-and-scammers-kick-their-campaigns-2014-fifa-world-cup

36 Kevin Savage, "Trojan.Tylon Risk Assessment," *Symantec Security Response Team*, 16 de noviembre de 2013. Disponible en: http://www.symantec.com/security_response/writeup.jsp?docid=2012-111612-5925-99.

37 *Véase* "Trojan.Zbot," Symantec Security Response, 10 de enero de 2010. Disponible en: http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

38 Symantec Corporation, "The State of Financial Trojans 2013," *Symantec Security Response Team*, 17 de diciembre de 2013. Disponible en: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_state_of_financial_trojans_2013.pdf

39 Daniel Regalado, "Criminals Hit the ATM Jackpot," *Symantec Security Response Team*, 11 de octubre de 2013. Disponible en: http://www.symantec.com/connect/blogs/criminals-hit-atm-jackpot

40 Daniel Regalado, "Texting ATMs for Cash Shows Cybercriminals' Increasing Sophistication," *Symantec Security Response Blog*, 24 de marzo de 2014. Disponible en: http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication

41 Symantec Corporation, "Sochi Olympics Terrorism Fears Used as Bait for Targeted Darkmoon Campaigns", *Blog de Symantec Security Response*, 28 de febrero de 2014. Disponible en: http://www.symantec.com/connect/blogs/sochi-olympics-terrorism-fears-used-bait-targeted-darkmoon-campaigns

Organización de los
Estados Americanos

Symantec

MEJORES PRÁCTICAS

Mejores prácticas

01
Utilizar estrategias de defensa profunda

Emplee activamente sistemas defensivos múltiples, superpuestos y de soporte mutuo para protegerse contra fallas de punto único en cualquier tecnología o método de protección específico. Esto debe incluir la implementación de *firewalls* actualizados con regularidad, así como antivirus de puertas de enlace, sistemas de detección o protección contra intrusiones (IPS), escaneos de vulnerabilidad de sitios *web* con protección contra *malware* y soluciones de seguridad de puertas de enlace *web* en toda la red.

02
Monitorear para detectar intentos de incursión en la red, vulnerabilidades y abuso de marca

Reciba alertas sobre nuevas vulnerabilidades y amenazas en las plataformas de los diversos proveedores para tomar medidas de reparación proactivas. Detecte casos de abuso de marca mediante alertas de dominio e informes sobre sitios *web* ficticios.

03
Un antivirus en los *endpoints* no alcanza

En los *endpoints*, es importante tener instaladas las últimas versiones de *software* antivirus, pero esto por sí solo no brindará una protección completa. Se debe implementar y usar un producto integral para seguridad en extremos que tenga capas adicionales de protección, incluyendo:

- Prevención contra intrusión en extremos que impida el aprovechamiento de vulnerabilidades sin parche, proteja contra ataques de ingeniería social y evite que el *malware* llegue a los *endpoints*
- Protección del explorador para evitar ataques complejos basados en la *web*
- Soluciones de reputación basadas en archivos y en la *web* que proporcionen una calificación de riesgo y reputación de cualquier aplicación y sitio *web* para impedir la ejecución de *malware* polimórfico y de mutación veloz
- Funciones de prevención conductual que observen la actividad de las aplicaciones e impidan la ejecución de *malware*
- Configuración del control de las aplicaciones que impida que éstas y los complementos *(plug-ins)* del explorador descarguen contenido malicioso no autorizado
- Configuración del control de los dispositivos que impida y limite los tipos de dispositivos USB que se utilizarán

04
Proteger sus sitios *web* contra "*Man In The Middle*" (ataques de intermediarios) e infecciones de *malware*

Evite comprometer su relación de confianza con sus clientes tomando las siguientes medidas:

- Configurar "*SSL Always On*" (protección SSL en su sitio *web* desde el inicio hasta el cierre de sesión)
- Escanear su sitio *web* en forma diaria para detectar *malware*
- Establecer el marcador seguro para todas las *cookies* de la sesión
- Evaluar periódicamente su sitio *web* para detectar vulnerabilidades (en 2013, uno de cada 8 sitios web escaneados tenía vulnerabilidades)
- Optar por Certificados SSL con Validación Extendida, que muestra a los usuarios del sitio *web* la barra de direcciones del explorador en verde
- Mostrar marcas de confianza reconocidas en ubicaciones de gran visibilidad en su sitio *web* para demostrar a sus clientes su compromiso con la seguridad

05
Proteger sus claves privadas

Asegúrese de obtener sus certificados digitales de una autoridad reconocida y confiable que demuestre excelentes prácticas de seguridad. Se recomienda a las organizaciones:

- Usar infraestructuras independientes de Firma de Prueba y Firma de Versión
- Proteger las claves en dispositivos de *hardware* seguros, criptográficos y a prueba de alteraciones
- Implementar seguridad física para proteger sus activos contra robos

06
Usar encriptación para proteger datos sensibles

Se recomienda implementar y hacer cumplir una política de seguridad que exija que todo dato sensible sea encriptado. El acceso a la información sensible debe ser restringido. Esto debe incluir una solución de Protección Contra Pérdida de Datos (DLP). Asegúrese de que los datos de los clientes también estén encriptados. Esto sirve no sólo para impedir violaciones de datos sino que además puede ayudar a mitigar los daños provocados por las posibles fugas de datos desde dentro de una organización. Use la Prevención Contra Pérdida de Datos para ayudar a prevenir las violaciones de datos: Implemente una solución de DLP capaz de descubrir dónde reside la información sensible, monitorear su uso y protegerlos contra pérdidas. Debe implementarse la prevención contra pérdida de datos para monitorear el flujo de información a medida que va saliendo de la organización hacia la red, y el tráfico hacia dispositivos externos o sitios *web*.

- La solución de DLP debe configurarse para identificar y bloquear acciones sospechosas de copiado o descarga de datos sensibles
- También debe utilizarse para identificar activos de datos confidenciales o sensibles en sistemas de archivos de red y computadoras

07
Asegurarse de que todos los dispositivos autorizados con acceso a las redes de la empresa tengan protecciones de seguridad adecuadas

Si se aplica una política de 'Traiga su propio dispositivo' (BYOD), asegúrese de que haya un perfil de seguridad mínimo para todo dispositivo autorizado a acceder a la red.

08
Implementar una política de medios extraíbles

Cuando sea práctico, restringir los dispositivos no autorizados, tales como discos duros externos portátiles y otros medios extraíbles. Tales dispositivos pueden introducir *malware* y facilitar las infracciones de propiedad intelectual, ya sea de manera intencional o no. Si los dispositivos de medios externos están permitidos, automáticamente escanearlos en caso de virus ya que se conectan a la red, también usar una solución de prevención de pérdida de datos para monitorear y restringir la copia de información confidencial a dispositivos de almacenamiento externo sin encriptar.

09
Tomar medidas enérgicas de actualización y aplicación de parches

Haga actualizaciones, parcheos y migraciones desde exploradores, aplicaciones y complementos de exploradores obsoletos e inseguros. Siempre tenga las últimas versiones disponibles de las definiciones de prevención de virus e intrusiones utilizando los mecanismos de actualización automática de los proveedores. La mayoría de los proveedores de *software* trabajan con esmero para parchar las vulnerabilidades de *software* explotadas; sin embargo, los parches sólo pueden ser eficaces si se adoptan en el campo. Siempre que sea posible, conviene automatizar las implementaciones de parches para mantener la protección contra vulnerabilidades en toda la organización.

10
Aplicar una política de contraseñas eficaz

Asegúrese de que las contraseñas sean sólidas, con un mínimo de 8-10 caracteres de largo y con una combinación de letras y números. Recomiende a los usuarios evitar reutilizar las mismas contraseñas en distintos sitios *web* y compartir sus contraseñas con otras personas, práctica que debería estar prohibida. Las contraseñas se deben cambiar con regularidad, al menos cada 90 días.

11
Hacer copias de seguridad regularmente

Es recomendable crear y mantener copias de seguridad (*backups*) de los sistemas críticos y de los extremos con regularidad. Si ocurriera una emergencia de seguridad o de datos, se debe poder acceder fácilmente a las copias de seguridad para minimizar el tiempo de inactividad de los servicios y garantizar la productividad de los empleados.

12
Restringir los archivos adjuntos de correo electrónico

Configure los servidores de correo para bloquear o eliminar mensajes que contengan archivos adjuntos que suelen usarse para difundir virus, por ejemplo archivos .VBS, .BAT, .EXE, .PIF y .SCR. Las empresas deben examinar las políticas relativas a los archivos .PDF autorizados a incluirse como datos adjuntos. Asegúrese de que los servidores de correo estén bien protegidos por *software* de seguridad, y de que los mensajes se escaneen de forma exhaustiva.

13
Asegurarse de contar con procedimientos de respuesta a infecciones e incidentes

- Tenga siempre a mano los datos de contacto de su proveedor de soluciones de seguridad, sepa a quién va a llamar y qué pasos va a seguir si tiene uno o más sistemas infectados
- Asegúrese de contar con una solución de copias de seguridad y restauración para recuperar datos perdidos o comprometidos si ocurriera un ataque exitoso o una pérdida de datos grave
- Aproveche las funciones de detección *post* infección de los cortafuegos y soluciones de seguridad de puertas de enlace *web* y extremos para identificar sistemas infectados
- Aísle las computadoras infectadas para prevenir el riesgo de infectar otros equipos de la organización, y recupere los datos usando medios confiables de copias de seguridad
- Si los servicios de red son víctimas de un código malicioso o alguna otra amenaza, hay que deshabilitar o bloquear el acceso a esos servicios hasta aplicar un parche

14
Educar a los usuarios acerca de los protocolos básicos de seguridad

- No abra datos adjuntos si no esperaba recibirlos o si no provienen de una fuente conocida y confiable, y no ejecute *software* descargado de Internet (si se permiten dichas acciones), salvo que la descarga haya sido escaneada para detectar virus y *malware*
- Se debe tener cuidado al hacer clic en URL en mensajes de correo electrónico o programas de redes sociales, incluso cuando provienen de fuentes confiables y amigos
- Implemente soluciones con complementos de reputación de URL en exploradores *web* que muestren la reputación de los sitios *web* desde las búsquedas
- Descargue únicamente *software* (si está permitido) compartido por la empresa, o directamente del sitio web del proveedor
- Si los usuarios de Windows ven una advertencia que indica que están "infectados" luego de hacer clic en una URL o de usar un motor de búsqueda (infecciones de antivirus falsos), se debe enseñar a los usuarios a cerrar o salir del explorador pulsando Alt-F4 o CTRL+W o utilizando el administrador de tareas

Organización de los
Estados Americanos

INFORMES POR PAÍS DE LA OEA

Antigua y Barbuda

★ St. John's

Población: **88,000**
Cobertura de Internet: **59%**
Suscriptores de banda ancha fija: **4.6%**

Varios organismos gubernamentales desempeñan un rol de liderazgo al promover la seguridad cibernética y combatir el delito informático en Antigua y Barbuda. La Oficina de Política Nacional de Control de Drogas de la Casa Blanca (ONDCP) representa el punto de contacto nacional para trabajar con organizaciones internacionales como la OEA, y el Ministerio de Información ha sido designado como el representante líder del gobierno para los asuntos relacionados con la seguridad cibernética en general. Asimismo, el Laboratorio de Investigaciones Cibernéticas Regional (RCIL), situado en el cuerpo de policía de Antigua y Barbuda, es responsable de procesar las pruebas digitales de causas penales e investigar las denuncias relacionadas con los delitos cibernéticos en Antigua y Barbuda y la región del gran Caribe.

En tanto que el Gobierno de Antigua y Barbuda no ha establecido formalmente un equipo de respuesta a incidentes de seguridad cibernética (CSIRT) a nivel nacional, se han celebrado reuniones de consulta con las posibles partes interesadas para debatir las cuestiones relacionadas con esta actividad y estas iniciativas continúan en curso. De manera similar, en tanto que las autoridades nacionales han tomado medidas para desarrollar una estrategia y una política nacional de seguridad cibernética, ninguna ha sido adoptada hasta ahora. El año 2013, sin embargo, se ha destacado por las mejoras significativas en la estructura legislativa del país mediante la aprobación de la Ley de Transacciones Electrónicas, la Ley de Evidencia Digital, la Ley Contra Delitos Electrónicos y la Ley de Protección de Datos.

Hasta ahora, no se ha adoptado ninguna campaña de concientización formal en lo que respecta a la seguridad cibernética, no obstante el Ministerio de Información, junto con la Iniciativa Conecta Antigua y Barbuda (Connect Antigua Barbuda Initiative), actualmente intenta desarrollar una campaña orientada a dictar pequeños cursos destinados a los empleados públicos sobre concientización para la seguridad de los correos electrónicos. Asimismo, se planea realizar varios anuncios de servicios públicos sobre cuestiones relacionadas con seguridad cibernética.

Los organismos del sector privado no están obligados a informar los incidentes relacionados con seguridad cibernética a las autoridades nacionales, y tampoco se han implementado las estructuras o los memorándums de entendimiento necesarios para facilitar este intercambio de información o esta cooperación. Sin embargo, el gobierno se ha esforzado en demostrar su voluntad para trabajar con el sector privado al tratar de comprometer la participación de los organismos clave, entre ellos, de telecomunicaciones, financieros, infraestructura crítica, servicios públicos, proveedores de Internet y otras partes interesadas, en varias reuniones sobre seguridad cibernética organizadas por el gobierno. La cooperación con otros países se ha fortalecido, dado que el RCIL trabaja activamente con varios gobiernos de la región. No obstante, la falta de capacidad de respuesta a incidentes o de un organismo líder de respuesta a incidentes a nivel nacional ha inhibido el compromiso con otros países en ese sentido.

En el país no existen programas de grado especializados en seguridad cibernética, si bien Antigua and Barbuda International Institute of Technology, que se especializa en asignaturas sobre tecnología de la información, en varios cursos incluye contenidos relacionados con seguridad.

Dado que no existe un organismo oficial encargado de responder a los incidentes cibernéticos y que la mayoría de estos incidentes no se denuncian, las autoridades nacionales no se encuentran en

condiciones de evaluar los cambios en la frecuencia o tipo de incidentes o los ataques que afectan a las personas, las empresas o las instituciones en el país. En 2013, el RCIL sólo recibió una pequeña cantidad de denuncias por cuentas de correo personales *hackeadas*. En el caso que captó la atención de la prensa, varias personas fueron extorsionadas después de un acceso de terceros a su cuenta. Sin embargo, ante la falta de denuncias, especialmente del sector privado, las autoridades nacionales no están en condiciones de precisar las tendencias o los incidentes de seguridad cibernética de importancia ocurridos en el país.

En el futuro, el éxito de las iniciativas actuales para mejorar la postura con relación a la seguridad cibernética a nivel nacional en Antigua y Barbuda dependerá en gran medida de varios factores clave, entre los que se incluyen: el nivel de aceptación y apoyo de las autoridades y ministerios, el grado de participación de diferentes partes interesadas a nivel nacional para el desarrollo de una política de seguridad cibernética y la disponibilidad de los recursos financieros para el lanzamiento del CSIRT a nivel nacional.

Argentina

★ Buenos Aires

Población: **41,350,000**
Cobertura de Internet: **55.8%**
Suscriptores de banda ancha fija: **10.9%**

El organismo líder a cargo de la seguridad cibernética en Argentina es el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) que forma parte de la Oficina Nacional de Tecnología de Información (ONTI), dependiente del Gabinete de Ministros. La investigación de los delitos cibernéticos y las actividades conexas es llevada a cabo principalmente por la Policía Federal Argentina (PFA), a través de su División de Delitos Tecnológicos. El Gobierno de Argentina también ha desarrollado políticas nacionales de seguridad de la información, y su estrategia nacional de seguridad cibernética ya ha sido elaborada y está siendo considerada para su aprobación.

Dentro del marco del ICIC (www.icic.gov.ar) se fundó el primer CERT (equipo de respuesta a emergencias informáticas) a nivel nacional en 1994, y en 2011, se lo designó formalmente como parte de la Oficina Nacional de Tecnología de la Información (ONTI), en donde se expandió para brindar servicios adicionales. Actualmente, los cuatro objetivos principales de ICIC-CERT son los siguientes: servir como repositorio de información relevante relacionada con los incidentes, herramientas y técnicas de seguridad cibernética; promover la coordinación entre los administradores de redes para todas las instituciones públicas a nivel nacional, a fin de prevenir, detectar, gestionar y recuperarse de los incidentes relacionados con la seguridad que afecten sus redes; centralizar la generación de informes respecto a incidentes que afecten las redes gubernamentales y facilitar el intercambio de información a fin de abordarlos de manera más eficaz; e interactuar con otros equipos de respuesta ante incidentes en el país y la región.

La División de Crímenes Tecnológicos de la PFA es la unidad responsable de las investigaciones referentes a delitos cibernéticos.

Las empresas del sector privado no están obligadas por ley a proporcionar información relacionada con los incidentes a las autoridades nacionales. No obstante, las autoridades han informado que existen

mecanismos establecidos para facilitar el intercambio de información por parte de las empresas privadas, como los proveedores de Internet (ISP) o de servicios de correo electrónico, cuando existe una clara base legal y judicial para la investigación. La actual legislación relacionada con los delitos informáticos se aprobó en 2008 y ha permitido realizar investigaciones y procesamientos exitosos en varios casos de importancia. No obstante, las autoridades indicaron que sus esfuerzos para hacer pleno uso de la ley al combatir los delitos cibernéticos han sido obstaculizados, en cierto modo, por los desafíos que surgen de la naturaleza de muchos delitos informáticos, que no tienen fronteras y están en constante evolución.

Las iniciativas lideradas por el gobierno para crear conciencia respecto a las diversas cuestiones y los desafíos relacionados con la seguridad cibernética se han centrado, en gran medida, en debates y conversaciones mantenidos en zonas densamente pobladas. A su vez, los esfuerzos a nivel de autoridades locales se han centrado en el desarrollo de centros de capacitación y unidades operativas equipadas correctamente. El ICIC también ha desarrollado una iniciativa llamada "Internet Sano", que apunta a promover el uso responsable de las TIC e Internet. Y la Dirección Nacional para la Protección de Información Personal, dependiente del Ministerio de Justicia y Derechos Humanos, ha desarrollado un segundo programa de concientización denominado "Contigo en la *web*".

En la actualidad, varias instituciones de educación superior en Argentina ofrecen programas de certificación y de grado en una amplia variedad de aspectos relacionados con la seguridad cibernética, incluyendo el análisis forense digital. Asimismo, se informó que el Instituto Nacional de Administración Pública (INAP) ofrece capacitación y cursos sobre temas relacionados con seguridad cibernética.

Aunque no se cuenta con registros detallados y cifras concretas disponibles para su distribución pública, las autoridades nacionales han observado durante 2014 un aumento en determinados delitos informáticos y otras actividades informáticas maliciosas, entre los que se incluyen: suplantación de identidad y fraudes por medio de las redes sociales, el correo electrónico o la banca electrónica, mediante el uso de ingeniería social o *keylogger* (registrador de pulsaciones de teclas) y otro *malware* (programas maliciosos); vandalismo de sitios *web*; y amenazas persistentes avanzadas (APT). Sin embargo, no existe información disponible que indique qué sector de la población ha sido el más afectado o perjudicado.

El Gobierno argentino se entrena de forma continua con el propósito de prepararse ante las amenazas cibernéticas emergentes. Desde 2012 se han llevado a cabo Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos (ENRIC), los cuales se realizan de forma anual. Este año, el ejercicio será realizado conjuntamente por la ONTI/ICIC, el Ministerio de Defensa y la Armada Argentina. Otros talleres sobre tecnologías emergentes de seguridad cibernética se llevan a cabo de forma regular para garantizar que los técnicos argentinos permanezcan al día sobre las últimas tendencias.

Las autoridades gubernamentales identificaron tres impedimentos principales a sus iniciativas en curso relacionadas con la seguridad y los delitos cibernéticos, específicamente: la falta constante de concientización entre las partes interesadas en todos los niveles, problemas y cuestiones relacionados con la privacidad, y financiación insuficiente.

Barbados

★ Bridgetown

Población: **276,000**
Cobertura de Internet: **73.3%**
Suscriptores de banda ancha fija: **23.09%**

El último año se ha destacado por los avances notables en el área de seguridad cibernética en Barbados y las iniciativas importantes continúan en diversas etapas de desarrollo. En el Gobierno de Barbados, dos autoridades nacionales han tomado un rol de liderazgo, la Unidad de Telecomunicaciones del Ministerio de Energía y Telecomunicaciones, que se encuentra en proceso de crear un CIRT nacional, y la Unidad de Delito Informático de la Policía Real de Barbados.

Aunque aún no se encuentra en funcionamiento, el CIRT actualmente se encuentra en la etapa de implementación que, a la fecha, ha incluido paneles de debate para crear conciencia respecto a sus tareas y actividades de capacitación en el futuro. Esto último implicó el entrenamiento del personal en sistemas y teorías de seguridad cibernética. Actualmente, no existe ninguna política o estrategia relacionada con seguridad cibernética aplicable a nivel nacional, aunque se ha confirmado un proyecto. El Gobierno de Barbados colabora con otros gobiernos caribeños, así como también con la Unión de Telecomunicaciones del Caribe (CTU) y la Organización de Telecomunicaciones del Commonwealth (CTO) en la organización de varias charlas consultivas relacionadas con la creación de un "modelo de gobernanza cibernética" del Commonwealth que sería adoptado e implementado por los países del Commonwealth para crear una norma compartida. Desde 2010, la Unidad de Telecomunicaciones de la Oficina del Primer Ministro ha asumido una iniciativa de concientización pública que apunta a proteger a los niños en el ciberespacio, que ha culminado recientemente en una sociedad con una empresa del sector privado para promocionar la campaña "Think Click Surf" (Pensar, cliquear y navegar). Finalmente, se alienta al personal clave del gobierno a asistir oportunamente a los eventos sobre políticas y prácticas relacionadas con seguridad cibernética.

Aunque las empresas del sector privado no están obligadas por ley a informar determinados incidentes cibernéticos específicos al gobierno, esta situación puede cambiar con la Ley de Protección de Datos, que actualmente se encuentra en la etapa de proyecto. La ley intenta abordar las cuestiones relacionadas con la generación de informes sobre violaciones de seguridad e incluye la determinación de plazos para informar incidentes.

Las autoridades del gobierno informan que una mayor cooperación constituye una prioridad clave y los funcionarios participan en todos los foros regionales correspondientes y en las iniciativas en curso a nivel nacional para comprometer a las empresas privadas y establecimientos educativos (University of the West Indies) en la concientización y el desarrollo de estrategias para gestionar la seguridad cibernética en Barbados. Se espera que el lanzamiento del CIRT nacional hacia fines de este año genere la articulación de un enfoque más orientado al fortalecimiento de mecanismos de cooperación a nivel nacional y regional. La cooperación con la ITU ha sido fundamental para el proceso de creación del CIRT nacional hasta la actualidad y se espera que se mantenga como una asociación de base para el gobierno.

En Barbados no existen programas de grado relacionados con la seguridad cibernética, aunque el campus local de la University of the West Indies ofrece varios cursos sobre diferentes aspectos de la seguridad cibernética y diversas empresas privadas organizan seminarios y talleres sobre este tema.

Aunque todavía no se cuenta con cifras concretas, el gobierno informa que la Unidad de Telecomunicaciones se encuentra recopilando datos sobre ataques cibernéticos e incidentes en los departamentos de gobierno que pronto permitirán un análisis crítico de los tipos de ataques y su frecuencia, así como también la clase de técnicas de mitigación empleadas y su eficacia. Se ha informado que varios incidentes ocurridos a principios de 2014 afectaron a varios departamentos gubernamentales y han sido comunicados a la oficina del Primer Ministro, que dispuso de ayuda para gestionar y mitigar el impacto de estos incidentes en sus objetivos.

La falta de financiamiento ha sido identificada como el impedimento más significativo para el avance de la seguridad cibernética en Barbados.

Belice

★ Belmopan

Población: **340,000**
Cobertura de Internet: **25%**
Suscriptores de banda ancha fija: **3.1%**

En tanto que el Gobierno de Belice actualmente no cuenta con una política o estrategia oficial en materia de seguridad cibernética, dos autoridades nacionales, el Ministerio de Seguridad Nacional y el Departamento de Policía de Belice (BPD), comparten la autoridad para administrar las cuestiones relacionadas con seguridad cibernética a nivel nacional. El BPD se ocupa del manejo de los delitos cibernéticos o los temas relacionados ad hoc y la Unidad de TI (PITU) asume el liderazgo con la colaboración, según sea requerida, de la Dependencia Especial para Seguridad e Inteligencia (SB). Cuando la investigación de un delito informático u otro incidente requiere la cooperación o el intercambio de información con otras organizaciones de seguridad o inteligencia tanto regionales como internacionales, la SB se ocupa de manejar estas comunicaciones. No existe un CIRT nacional ni una política o procedimiento establecidos para responder ante los incidentes cibernéticos. La Unidad de TI del BPD, sin embargo, ha organizado un "ICT *Road Show*" anual por todo el país para promocionar una mayor concientización en las cuestiones relacionadas con Internet y seguridad cibernética en el público en general.

Las iniciativas del BPD para abordar el delito informático han generado resultados positivos, pero aún presentan obstáculos ante la falta de un marco legal adecuado que permita procesar a los culpables, así como también la necesidad de contar con mayores recursos, entre ellos, personal, capacitación, equipamiento, *software* y espacio de oficinas.

El Ministerio de Seguridad Nacional, específicamente el punto medular para el Comité Interamericano contra el Terrorismo-OEA (CICTE-OAS), actualmente trabaja para establecer el Comité Directivo de ICT en el Ministerio, con el doble objetivo de desarrollar una estrategia de seguridad cibernética a nivel nacional y revisar y fortalecer el marco legislativo relacionado con los delitos cibernéticos. Asimismo, las autoridades de gobierno recientemente han comenzado a trabajar para desarrollar una "Política de Innovación Nacional para ICT". En tanto que esta política apuntará principalmente a las cuestiones relacionadas con la administración electrónica, incluirá un componente que se ocupe de la seguridad cibernética y la protección de infraestructuras críticas.

Aunque las instituciones del sector privado no están obligadas por ley a informar los incidentes cibernéticos a las autoridades nacionales, el BPD ha trabajado para establecer relaciones de cooperación con varias empresas del sector privado y ha brindado apoyo y asistencia cuando se le ha solicitado. La cooperación con las autoridades de otros países ha sido limitada. Sin embargo, el BPD junto a otros miembros de la Comunidad del Caribe (CARICOM) ha coordinado los asuntos relacionados con la seguridad cibernética en el período previo a la Copa Mundial de *Cricket* de 2007 y ha brindado asistencia a las autoridades de Estados Unidos al recuperar datos de las computadoras utilizadas por los delincuentes involucrados en el tráfico de personas, así como también, en la investigación de las personas que tuvieran conexiones sospechosas con terroristas u otras redes delictivas.

Aunque actualmente no llevan registro de las estadísticas oficiales, el Gobierno de Belice ha informado un aumento notable de los incidentes relacionados con seguridad cibernética durante el último año y cita informes no formales del sector privado, incluso de las empresas de telecomunicaciones y otros propietarios y operadores de infraestructura crítica que, de manera anecdótica, confirman un aumento de los ataques cibernéticos. Los incidentes que involucran a las instituciones financieras no se han informado tan abiertamente a las autoridades nacionales, tal vez para no llamar la atención a sus clientes de manera indeseada. Es decir, dichas instituciones actualmente prefieren manejar internamente los asuntos relacionados con seguridad cibernética.

Las autoridades nacionales muestran un conocimiento de las tendencias y los desafíos relacionados con la seguridad cibernética en América Latina y el Caribe y las vulnerabilidades de sus propios sectores industriales y financieros, así como también, las infraestructuras críticas, como las telecomunicaciones y los servicios públicos. Este conocimiento impulsa las iniciativas actuales de creación de capacidades y desarrollo de políticas a nivel nacional, incluso aquellas que apuntan a la adopción de una estrategia a nivel nacional, la reforma del sistema jurídico y la creación del CIRT nacional.

Bolivia

★ La Paz y Sucre

Población: **10,517,000**
Cobertura de Internet: **34.2%**
Suscriptores de banda ancha fija: **1.05%**

En Bolivia, dos autoridades nacionales son responsables de las acciones gubernamentales tendientes a desarrollar un régimen de seguridad cibernética propio. La primera es el Instituto de Investigaciones Técnico Científicas de la Universidad Policial (IITCUP), el principal organismo encargado de investigar delitos cibernéticos, cuyo objetivo central es el procesamiento y análisis de evidencia digital. El personal del departamento de análisis forense digital está a cargo de esa labor. Sus miembros han sido capacitados en Estados Unidos, Argentina y Perú y participan regularmente en otros cursos y eventos nacionales e internacionales, en carácter de instructores o asistentes. En el último año el IITCUP ha centrado sus esfuerzos en fortalecer su capacidad de realizar análisis forense digital.

La segunda autoridad nacional es la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), que depende de la Vicepresidencia de la República y de la Presidencia de la Asamblea Nacional. Entre otras cosas, la ADSIB está elaborando planes para la implementación del gobernanza electrónica y el uso de *software* gratuito, que resolverán una variedad de importantes cuestiones relacionadas con la seguridad cibernética. Si bien aún no existe un equipo de respuesta a incidentes

cibernéticos (CIRT), la ADSIB se encuentra abocada a la labor de generar una capacidad nacional de respuesta a incidentes a partir de su equipo actual de personal capacitado y competente. Se espera que este equipo comience a operar en 2014. La ADSIB también ha organizado un seminario de capacitación acerca de la protección de sitios *web* contra ataques cibernéticos.

Las autoridades gubernamentales impulsaron la creación del primer punto de intercambio de tráfico de Internet (IXP) en Bolivia, al parecer motivada por las revelaciones de Snowden en los Estados Unidos.

Si bien el IITCUP cuenta con canales para solicitar información y cooperación a las entidades del sector privado, refiere que el principal obstáculo para investigar y procesar delitos cibernéticos es la continua falta de mecanismos formales para obtener acceso a esa información de manera oportuna cuando se la solicita a redes sociales y otros operadores. Y, dada la cooperación relativamente limitada entre el IITCUP y otras autoridades nacionales y entidades del sector privado, estas últimas suelen ocuparse de su propia seguridad y gestión de incidentes. De forma similar, las entidades del sector privado no deben denunciar incidentes ante la ADSIB, la que no brindó información respecto de la situación actual en cuanto a colaborar o compartir información entre ambas partes. Sin embargo, la ADSIB ha logrado establecer una cooperación más fructífera con entidades homólogas en otros países. Un especial incidente de seguridad denunciado dio como resultado la coordinación directa con el CIRT nacional de Argentina, ICIC-CERT, para atender y resolver una situación relacionada con el *phishing* (suplantación de identidad) y un posible ataque a una empresa de importancia fundamental para los intereses nacionales de Bolivia. La gestión eficaz de este incidente fue considerada un gran éxito del gobierno.

Si bien el IITCUP tiene su propio protocolo de seguridad interna consolidado, informa que no existen protocolos o procedimientos comunes entre otros organismos gubernamentales. Y, si bien en teoría cada institución debería adoptar sus propios protocolos según lo requerido, muchas aún no han establecido procedimientos de seguridad de la información o las redes.

El IITCUP informa que muchas universidades en Bolivia ofrecen cursos relacionados con la seguridad cibernética, incluidos cursos de análisis forense digital, y que algunos miembros de su personal toman estos cursos de capacitación con frecuencia. Sin embargo, la mayoría de los cursos son generales y teóricos, e incorporan escasa formación práctica.

Ambas autoridades informan que no se han tomado medidas significativas para generar conciencia en materia de seguridad en el ámbito gubernamental, el sector privado o la sociedad en general.

Si bien la ADSIB no cuenta con datos cuantitativos acerca de la frecuencia o tipos de incidentes cibernéticos en Bolivia, el IITCUP ha observado un aumento exponencial en esta clase de incidentes en los últimos años y menciona un incremento de al menos 60% en 2013, en comparación con el año anterior. Según el IITCUP, los grupos más afectados han sido los usuarios particulares, seguidos por el gobierno. De acuerdo con los informes de la ADSIB, los incidentes importantes del último año también han incluido el robo de datos, disturbios civiles y modificaciones a los usuarios raíz de sitios clave. El IITCUP observó que los medios más comunes de ataque o explotación eran amenazas, extorsión y secuestro de menores a través de las redes sociales, y ataques y vandalismo de sitios *web* de instituciones gubernamentales. El IITCUP informó que se abrieron aproximadamente 150 casos relacionados con delitos cibernéticos en el último año. Cabe destacar un caso que involucró el uso de Facebook para contactar y ofrecer oportunidades laborales falsas a mujeres menores de edad. El perpetrador del incidente persuadía a las mujeres de encontrarse con él, las fotografiaba en situaciones comprometedoras y luego las extorsionaba mediante amenazas de publicar estas fotografías. Las autoridades lograron atraparlo, reunir y procesar evidencia obtenida de diferentes computadoras y dispositivos electrónicos, y obtuvieron un veredicto de culpabilidad.

De cara al futuro, tanto el IITCUP como la ADSIB mencionan la necesidad de una mayor cooperación entre organismos estatales, así como de mayor capacitación y asistencia para respaldar las iniciativas de desarrollo de la capacidad emprendidas por esos organismos.

Brasil

★ Brasilia

Población: **201,033,000**
Cobertura de Internet: **49.8%**
Suscriptores de banda ancha fija: **9.2%**

El Gobierno de Brasil ha desarrollado capacidades avanzadas en materia de seguridad cibernética y disuasión de delitos cibernéticos, y cuenta con una gran cantidad de instituciones y organismos en el área. La Policía Federal (DPF) es el principal organismo responsable de investigar todos los delitos perpetrados en el país y como tal, es la principal autoridad en materia de delitos cibernéticos, a través de su Servicio de Represión de Delitos Cibernéticos (SRCC). Asimismo, mantiene un segundo grupo de tareas especializado en la lucha contra los delitos relacionados con la pornografía infantil en Internet, GECOP, si bien se planea su pronta integración con el SRCC. Cuando la naturaleza de un delito informático en especial lo amerita, se da participación al personal de otras unidades del DPF y de otras instituciones. En el caso de un delito cometido contra una persona física, el cuerpo de Policía Civil del estado donde el delito fue perpetrado asume un papel activo y entrega al DPF las pruebas requeridas para conducir una investigación internacional.

Para la preparación de este informe, no se nos suministró información pertinente acerca de las políticas en materia de seguridad o de respuesta a incidentes.

El DPF mantiene un sólido régimen de seguridad interna y externa para garantizar la resiliencia cibernética e integridad de sus sistemas de información en red, incluida una unidad técnica para investigar y resolver infracciones de seguridad interna, el uso de salas equipadas con altos niveles de seguridad y la disponibilidad de conexiones y suministro de energía redundantes para los servidores que alojan los servicios y la información más importantes. El DPF acata los lineamientos establecidos por el Comité de Gestión de TIC (tecnologías de la información y la comunicación) del gobierno brasileño.

El personal del SRCC y otros funcionarios responsables de la investigación de delitos cibernéticos reciben una capacitación regular sobre aspectos específicos de cibernética forense para permanecer actualizados y utilizar las herramientas y técnicas pertinentes con eficiencia.

Las autoridades nacionales, especialmente dentro del Departamento de Seguridad de la Información y Comunicaciones (DSIC), del Gabinete de Seguridad Institucional (GSI) de la Presidencia de la Nación, han desarrollado e implementado campañas de concientización para promover el uso inteligente y responsable de Internet por parte de los ciudadanos.

Si bien las entidades del sector privado no están legalmente obligadas a brindar a las autoridades nacionales información relativa a incidentes, las autoridades informaron que la cooperación entre ambos sectores es habitual y sólida. Como ejemplo, podemos mencionar un acuerdo entre el DPF y Microsoft, en virtud del cual Microsoft brinda al DPF la información de registro de los usuarios de sus servicios, cuando éste se lo solicita a través de un formulario electrónico. Las autoridades también señalaron que Brasil cuenta con un sector, importante y productivo, dedicado a desarrollar *software* de seguridad cibernética personalizado para entidades privadas, como bancos, y para instituciones públicas

Las autoridades mencionaron varias tendencias observadas en 2013, si bien no se proporcionaron datos precisos. Estas tendencias incluían el aumento de las denuncias al DPF de delitos cibernéticos y actividades relacionadas, que según suponen las autoridades obedecería principalmente a la reciente entrada en vigencia de una ley que modifica el Código Penal para incluir los delitos cibernéticos.

La forma de delito informático más común denunciada fue el fraude bancario electrónico, que afecta a los usuarios y proveedores de servicios bancarios por Internet. Según las autoridades, el sector comercial ha sufrido el mayor impacto. Las empresas más afectadas son aquellas que venden productos o servicios por Internet, al igual que los bancos mencionados anteriormente y las empresas emisoras de tarjetas de crédito. En 2013 las autoridades informaron el arresto de 91 personas por actividades relacionadas con delitos cibernéticos.

Si bien las autoridades no mencionaron un incidente de especial importancia para ser incluido en el informe, se resaltó el destacado aumento de las denuncias de fraude bancario electrónico como una de las principales tendencias, con costos potencialmente significativos.

En términos de los impedimentos a la mejora de la seguridad cibernética y la lucha contra los delitos cibernéticos, las autoridades hicieron referencia a la necesidad de avanzar en la penalización de ciertos delitos y a la falta de requerimientos que obliguen a los proveedores de servicios de Internet (ISP) a guardar los datos de sus usuarios y entregar esa información a las autoridades en caso de un incidente o investigación sin necesidad de una orden judicial. Sin embargo, se informó que el congreso nacional está analizando un proyecto de ley para resolver esta última cuestión.

Chile

★ Santiago

Población: **16,841,000**
Cobertura de Internet: **61.4%**
Suscriptores de banda ancha fija: **12.4%**

Varios organismos dentro del gobierno chileno comparten responsabilidades relativas a la promoción de la seguridad cibernética y la lucha contra los delitos cibernéticos. El Ministerio del Interior y Seguridad Pública, la Secretaría General de la Presidencia y la Subsecretaría de Telecomunicaciones tienen un papel clave en materia de seguridad cibernética. Los Carabineros, o la policía nacional, son los encargados de las cuestiones relativas a los delitos cibernéticos, a través de su Departamento de Investigación de Organizaciones Criminales (OS-9). La Sección de Delitos de Alta Complejidad es parte de la estructura operativa del OS-9 y lidera las investigaciones relativas a las TIC o a la recolección y análisis de evidencia digital. El Departamento de Criminología de los Carabineros (LABOCAR) también mantiene un laboratorio informático dedicado a realizar un análisis de computadoras y dispositivos incautados durante las investigaciones de amenazas, *grooming* (captación de menores con fines sexuales), *phishing* (suplantación de identidad) y otras actividades ilícitas.

Si bien no existe ninguna estrategia o política oficial en material de seguridad cibernética a nivel nacional, en los últimos años las autoridades chilenas han estado trabajando en el desarrollo de una capacidad nacional de respuesta y gestión de incidentes cibernéticos. En este emprendimiento, han adoptado un enfoque bastante singular ya que, en lugar de concentrarse en la creación de un único Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) nacional o un organismo similar, han concentrado sus esfuerzos en el desarrollo de procedimientos y mejores prácticas estandarizados en materia de gestión de incidentes y seguridad cibernética en general. Estos procedimientos y mejores prácticas se encuentran delineados en el Decreto Supremo Número 1299, Programa para la Mejora de la Gestión de Sistemas de Seguridad de la Información. Si bien el gobierno cuenta con

un CSIRT desde 2004, llamado CSIRT-CL, no se trata de una entidad institucional formal sino de una función y estructura operativa mantenida por el Ministerio del Interior y Seguridad Pública. Sus metas incluyen ofrecer respaldo en materia de delitos cibernéticos a la Red de Conectividad del Estado y otras entidades del gobierno central, y promocionar la cooperación nacional e internacional, así como la concientización y el fortalecimiento de leyes y políticas nacionales. El CSIRT-CL ha colaborado de forma activa con otros CSIRT nacionales de la región en respuesta a incidentes y ha formado parte de iniciativas de capacitación de personal de otros Estados Miembros de la OEA. Además del trabajo del CSIRT-CL, el gobierno habilita e incentiva a las empresas privadas para que brinden servicios de gestión de incidentes, tanto a otras empresas privadas como a instituciones públicas. El personal de OS-9, LABOCAR y CSIRT-CL recibe capacitación técnica en investigación cibernética y gestión de incidentes por parte de expertos en la materia. Por otro lado, la capacitación brindada por los proveedores de un *hardware* o *software* determinado que se está utilizando constituye una formación adicional que garantiza la administración y uso adecuados del dispositivo o programa. Y cuando se necesita un conocimiento específico del que carece el personal actual, por ejemplo si el OS-9 requiere una persona con conocimientos de ingeniería de *software* especializada en delitos cibernéticos, se contrata un especialista. La Universidad de Chile y otras instituciones académicas de primer nivel ofrecen carreras de grado y de posgrado en seguridad cibernética y delitos cibernéticos.

A fin de promover la resiliencia de sus sistemas y la integridad de los datos dentro de su propia institución, los Carabineros utilizan un plan y un *software* de recuperación ante desastres que garantizan el rápido reinicio de las operaciones ante un desastre natural o provocado por el hombre. Y los administradores de sistemas y gerentes de seguridad de la institución verifican de forma regular los procesos, políticas y procedimientos relacionados con la recuperación de la información y la continuidad de la infraestructura de TI. Se han establecido políticas y procedimientos de seguridad para garantizar que los usuarios dentro de la institución colaboren con la gestión segura de los sistemas de información. Estas políticas y procedimientos incluyen pedir a los usuarios que cambien sus contraseñas de forma periódica y prohibir la instalación de programas de intercambio de archivos (P2P) en las computadoras laborales. Asimismo, se llevan a cabo evaluaciones de riesgo y se dictan cursos de capacitación para el personal de forma regular. Además, gracias a un sistema interno de Intranet, que incluye una página *web* interna, los usuarios pueden comunicarse y acceder a información dentro de un entorno seguro y con acceso controlado, lo que garantiza que cualquier persona sólo tiene acceso a las bases de datos pertinentes a sus funciones laborales. Los usuarios que desean acceder al sistema de forma remota, deben utilizar una red privada virtual (VPN) segura, que constituye una capa adicional de protección.

La legislación chilena no obliga a las empresas privadas a compartir información relativa a incidentes con las autoridades nacionales, a menos que se requiera esta información como parte de una investigación penal oficial. Sin embargo, las autoridades nacionales procuran de forma activa desarrollar y mantener canales con entidades clave del sector privado, cuya cooperación es esencial para llevar a cabo investigaciones o gestión de incidentes eficaces. Se informó que estos canales en general son a nivel operativo y personal y que, si bien pueden facilitar y acelerar el flujo de información, no cuentan con el beneficio de las estructuras o mecanismos institucionales que pueden facilitar, normalizar y legitimar estos intercambios.

El Ministerio de Educación ha desarrollado y está implementando, en asociación con varias entidades del sector privado, una campaña a largo plazo llamada “Internet Segura”, para concientizar y promover una cultura de seguridad cibernética.

Las autoridades informaron que no cuentan con suficiente información para ofrecer una evaluación cuantitativa respecto al aumento o disminución de los incidentes o delitos cibernéticos en 2013. Sin embargo, sí informaron que, según los datos disponibles, los tipos más comunes de incidentes señalados a las autoridades nacionales en el año estaban relacionados con actividades de *phishing*, *malware* o programas maliciosos y el *hackeo* de páginas *web* gubernamentales por parte de *hacktivistas*, actividad que aparentemente fue 30 veces superior en 2013. Sin embargo, entre estos incidentes, el *phishing* parecería representar el mayor porcentaje de delitos cibernéticos en el país. El *grooming* (captación de menores con fines sexuales) y las amenazas contra personas constituyen otros incidentes denunciados con frecuencia. Las autoridades policiales han observado que los grupos

etarios a los que pertenecen las víctimas parecen ser un factor constante para cada tipo de delito informático o actividad ilícita. Por ejemplo, los incidentes de captación de menores con fines sexuales, legalmente clasificados como "abuso sexual indebido", generalmente afectan a niños entre 6 y 15 años de edad, independientemente de su situación socio-económica o académica.

Las autoridades informaron que no existen registros de la cantidad exacta de casos de delitos cibernéticos abiertos en 2013, o de la cantidad de personas condenadas por ellos. Sin embargo, resaltaron varios casos importantes en 2013. En un caso conocido como Operación Minerva, algunas personas afiliadas a un movimiento *hacktivista* desarrollaron un *malware* que implementaron mediante *phishing*, que les permitió infectar las computadoras de gran cantidad de funcionarios gubernamentales y obtener acceso no autorizado a datos. Las autoridades finalmente lograron detectar la actividad maliciosa, llevaron a cabo un análisis forense para establecer la naturaleza y origen de la amenaza, e identificaron a las personas responsables. En otro incidente, un funcionario gubernamental de alto nivel jerárquico del área de seguridad, recibió amenazas de muerte a través de Twitter. Gracias a una investigación conducida por el OS-9, se identificó al responsable, quien fue arrestado.

Las autoridades chilenas mencionaron dos impedimentos principales a los esfuerzos para mejorar la seguridad cibernética y luchar contra los delitos en el ciberespacio. El primero es la necesidad de desarrollar una mayor conciencia entre los responsables de la toma de decisiones de mayor jerarquía en relación con la urgencia de las amenazas cibernéticas y los pasos a seguir para atenderlas. El segundo impedimento relacionado es la falta de comprensión de la magnitud de los costos que acarrean los delitos cibernéticos y las vulnerabilidades cibernéticas, tanto para el sector público como privado, y la importancia de desarrollar un enfoque estratégico e integrado que delinee los roles y responsabilidades de todas las partes interesadas.

Colombia

★ Bogotá

Población: **47,130,000**
Cobertura de Internet: **49%**
Suscriptores de banda ancha fija: **8.2%**

Las iniciativas en materia de seguridad y delitos cibernéticos que lleva a cabo el Gobierno de Colombia están regidas principalmente por el documento CONPES 3701, una política nacional relativa a la seguridad cibernética y ciberdefensa que se ha utilizado durante varios años. La política define principios rectores, describe roles y responsabilidades, y destaca campos prioritarios para la acción e inversión por parte de autoridades gubernamentales. Fue sobre la base de este documento que se creó el Centro Cibernético Policial (CCP) especializado dentro de la Policía Nacional de Colombia, bajo la Dirección de Investigación Criminal e INTERPOL (DIJIN). El CCP es la principal unidad designada en Colombia para investigar delitos cibernéticos en todo el país, y el Departamento de Estado de los Estados Unidos (DS/ATA) y el FBI, así como los Gobiernos de España y Francia, brindaron capacitación en investigación cibernética y análisis forense digital a su personal. CONPES 3701 también especifica el mandato de ColCERT, el organismo nacional a cargo de la respuesta a incidentes cibernéticos y de la coordinación entre las partes interesadas en el ámbito nacional. Numerosos ministerios y organismos comparten un amplio abanico de responsabilidades relacionadas con asuntos cibernéticos bajo el liderazgo de estas dos entidades relevantes. La Ley 1273, promulgada en 2009, constituye el eje del marco legislativo nacional del país en materia de seguridad cibernética y delitos cibernéticos.

Para fomentar la resiliencia de los sistemas internos y la integridad de la información, la Policía Nacional ha desarrollado sus sistemas internos para la gestión de la seguridad de la información en cumplimiento con la norma ISO 27001. Esto provocó el desarrollo de su propia aplicación para gestionar los activos cibernéticos y la seguridad de la información del sistema, conocida como SINAI. Para informar al personal y a otros usuarios sobre políticas y procedimientos pertinentes se emplean comunicados internos. Además, como medidas de seguridad adicionales, la Policía Nacional mantiene su propio equipo de respuesta a incidentes cibernéticos (CSIRT) y también encomendó la creación de un sitio alternativo para albergar aplicaciones y bases de datos consideradas cruciales para su institución.

En cuanto a la cooperación y el intercambio de información entre el sector privado y las autoridades gubernamentales, existe una norma específica, el Decreto 1704 (2012), que establece los requisitos que deben cumplir los proveedores de redes y servicios de telecomunicaciones a fin de respaldar, de manera eficaz y oportuna, el trabajo de las autoridades nacionales. Además, las autoridades nacionales procuraron forjar relaciones con entidades clave del sector privado con el objeto de incrementar aún más la cooperación y el intercambio de información.

La cooperación internacional ha sido sólida, puesto que las autoridades nacionales colaboraron, de modo directo, con organismos homólogos de otras regiones en la respuesta a ataques cibernéticos o delitos cibernéticos. Un ejemplo de esto fue la participación activa de las autoridades colombianas en una iniciativa multinacional, bajo el auspicio del Grupo de Trabajo Latinoamericano sobre Delitos Tecnológicos de INTERPOL, cuyo objeto era identificar y arrestar a los usuarios de foros *online* donde se intercambiaba y distribuía material sobre delitos sexuales contra niños y adolescentes. Entre los países que colaboraron, se encuentran Argentina, Brasil, Chile, Costa Rica, Ecuador, Uruguay, Venezuela y España.

Cabe destacar que el gobierno invitó recientemente a una Comisión Internacional de Expertos a venir al país y realizar una evaluación exhaustiva de la seguridad cibernética en Colombia. El equipo estaba formado por expertos de Canadá, España, Estados Unidos, Reino Unido, República Dominicana, Estonia, Israel, Corea del Sur y Uruguay, así como por representantes de la OEA, el Consejo de Europa (COE), el Foro Económico Mundial (WEF), INTERPOL, las Naciones Unidas (ONU), la Organización de Cooperación y Desarrollo Económicos (OCDE) y la Universidad de Oxford. Se hizo hincapié en las políticas de seguridad cibernética, la respuesta a incidentes y su gestión, los marcos normativos y la cooperación internacional, la legislación e investigación en materia de delitos cibernéticos y la ciberdefensa. Los expertos se reunieron con funcionarios oficiales y observaron operaciones en numerosas instituciones gubernamentales, e intercambiaron información e ideas con actores involucrados en iniciativas nacionales de seguridad cibernética. Después de la visita, se elaboró un paquete integral de observaciones y recomendaciones, que se presentó a las autoridades colombianas de mayor rango para su consideración y aprovechamiento.

Las universidades y otras instituciones educativas colombianas ofrecen un amplio abanico de programas académicos y de capacitación sobre todos los temas relacionados con la seguridad cibernética y los delitos cibernéticos, entre ellos, la seguridad de redes y el análisis forense digital.

Frente al mayor acceso de los ciudadanos colombianos a las nuevas tecnologías de la información y la expansión del dominio cibernético, las autoridades observaron un incremento paralelo y sistemático de la transición de las actividades delictivas del mundo físico al mundo virtual. En Colombia, este fenómeno fue sumamente evidente en el ámbito del fraude electrónico, que afecta a usuarios y entidades del sistema bancario colombiano. Cada vez más, los incidentes que se reportan involucran el uso de *keyloggers* (registradores de teclas), *spyware* y otros programas maliciosos semejantes. La misma dinámica se vio reflejada en el campo del suplantación de identidad, donde los autores del hecho se vuelcan a delitos cada vez más sofisticados, como *ransomware* (secuestro informático) y el uso del programa malicioso Cryptolocker para atacar a la comunidad de pequeñas y medianas empresas (PyME), así como a empresas más grandes.

Los datos recopilados por la Policía Nacional revelan estadísticas interesantes en relación al crecimiento del uso de las TIC y el aumento consiguiente de incidentes y delitos cibernéticos. Se informaron las siguientes cifras para 2013: 448.983 seguidores en Twitter; 256,987 visitantes al sitio web www.ccp.gov.com; 16,789 páginas *web* bloqueadas por pornografía infantil; 2652 nuevas alertas de

amenazas cibernéticas; 422 personas detenidas por delitos cibernéticos y un total de 4,290 reclamos recibidos por la Policía Nacional en relación con incidentes asociados a las TIC (lo cual representa un aumento de 1,194 quejas respecto del año anterior).

En 2013, el CCP respondió a 1,647 ataques o incidentes cibernéticos, de los cuales 62% involucró a ciudadanos particulares y 21%, a entidades del sector bancario. El resto de los incidentes involucró a una combinación casi igual de entidades pertenecientes a los sectores de gobierno, fuerzas de seguridad, comunicaciones, energía, salud y educación.

Las autoridades colombianas identificaron tres tendencias específicas del delito cibernético. La primera es el mayor uso de códigos maliciosos, *phishing* (suplantación de identidad) y el robo de información que afectan a usuarios e instituciones que operan en el creciente sector de la banca virtual. Las autoridades afirman que esta situación fue perpetuada por una débil cultura de la seguridad y una correspondiente falta de concientización de los usuarios en materia de seguridad por parte de las empresas. La segunda tendencia genera incidentes que afectan la seguridad cibernética, entre ellos, el acceso no autorizado a la información o la fuga de esta, la interceptación de datos, el acceso abusivo a los sistemas, la denegación de servicio (DoS) y vandalismo de sitios *web*. La tercera tendencia observada se refiere al mayor uso de Internet, las redes sociales, el correo electrónico y la Internet profunda por delincuentes comunes y el crimen organizado. Esto comprende el cobro masivo ilegal de dinero (por ejemplo, pirámides cibernéticas), el uso de divisas virtuales como mecanismo para lavar dinero y negocios ilícitos que involucran el tráfico de armas, las drogas, la pornografía infantil, etcétera.

La Policía Nacional informó un marcado aumento de la cantidad de personas arrestadas por haber cometido delitos cibernéticos y otros actos ilegales semejantes en 2013, que ascendió a los 422 arrestos frente a 323 en 2012, y 252 en 2011. Además, las autoridades colombianas se refirieron a la mencionada Operación Pureza II - dirigida contra distribuidores de pornografía infantil y delitos similares, que se llevó a cabo bajo el auspicio de INTERPOL y en colaboración con organismos de las fuerzas de seguridad y otras entidades de numerosos países, como ejemplo de un triunfo formidable en sus continuos esfuerzos para reducir el delito cibernético.

Las autoridades informaron que el principal impedimento para aumentar la seguridad cibernética del país es la persistente ausencia de una cultura de la información y la seguridad cibernética entre los ciudadanos usuarios y las empresas por igual. También destacaron la falta de políticas de uso de las TIC con soporte en Internet y su capacidad limitada para actuar en este ámbito, puesto que las sedes de la mayoría de los proveedores y operadores de servicios de Internet se encuentran fuera del territorio nacional y las relaciones de cooperación son acotadas.

Costa Rica

★ San José

Población: **4,667,000**

Cobertura de Internet: **47.5%**

Suscriptores de banda ancha fija: **9.3%**

La autoridad principal en materia de seguridad cibernética de Costa Rica es el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICIT). No obstante, también se encargan de estos asuntos numerosos organismos e instituciones, entre ellos: el Gobierno Digital/Secretaría Digital; la Dirección de Firmas Digitales; la Sección de Delitos Cibernéticos del Poder Judicial; la Agencia para la Protección de Datos (Prodhab); el Banco Central; el centro CSIRT-CR y la Superintendencia de Telecomunicaciones.

Hace más de una década, se creó la Sección de Delitos Cibernéticos de la rama de investigación del Poder Judicial, con el objeto de supervisar y asistir en la investigación de delitos que involucren el uso de TIC y pruebas digitales. En 2012, se creó el centro CSIRT-CR, dependiente del Ministerio de Ciencia, Tecnología y Telecomunicaciones, a fin de responder a los incidentes cibernéticos que afecten a organismos gubernamentales, así como mitigarlos. El centro CSIRT-CR también tiene a su cargo articular los diferentes organismos estatales, instituciones autónomas, empresas y bancos para identificar amenazas, reducir al mínimo los riesgos y mejorar la cooperación y el intercambio de información sobre asuntos relacionados con la seguridad cibernética.

El gobierno adoptó una Estrategia Digital Nacional. No obstante, su objetivo principal es definir una visión para el uso integrado de tecnologías por parte del Estado y se limita a identificar la seguridad cibernética como una prioridad. En la actualidad, no hay ninguna estrategia o política en materia de seguridad cibernética que regule las iniciativas asociadas de las autoridades nacionales.

En lo que respecta a la formación y el desarrollo de capacidades, el personal de la Sección de Delitos Cibernéticos recibió capacitación de organismos homólogos de los Estados Unidos y Canadá, en aspectos de investigación y análisis forense digital, y otros cursos de capacitación de mucha utilidad, dictados por otras organizaciones regionales, incluida la OEA. Además, el personal del CSIRT-CR recibió capacitación técnica de socios externos, entre ellos, la OEA y expertos en respuesta a incidentes de otros Estados Miembros de la OEA.

En el ámbito institucional, ya se tomaron medidas para mejorar la resiliencia del sistema y la integridad de la información. A diario se hace una copia de seguridad de los datos de los servidores a las unidades SAN (red de área de almacenamiento) y se dispone de sistemas de seguridad para las computadoras de la red y las bases de datos que contienen. La política de seguridad establece que solo algunos servidores centrales designados pueden conectarse a las bases de datos de la red.

El marco legislativo de Costa Rica incluye una ley de firmas digitales, en la que se definen políticas relativas a la certificación por el Gobierno de certificadores registrados, y a los formatos oficiales para los documentos electrónicos con firma digital. Otra ley (No 8,968) aborda la protección de la información personal y define la forma en que las empresas deben manejar la información personal que recaben, restringiendo el uso de dicha información. Más recientemente, las autoridades costarricenses aprobaron una nueva ley de delitos cibernéticos (No 9,048), que comprende reformas importantes al Código Penal y tipifica nuevos delitos cibernéticos. Si bien Costa Rica fue invitada a adherir el Convenio de Budapest, y a pesar de las continuas iniciativas de algunas autoridades nacionales, orientadas a avanzar en ese frente, el país todavía no lo ha hecho.

Las entidades del sector privado no tienen obligación legal de intercambiar información con las autoridades nacionales en caso de incidentes, y los vínculos y mecanismos necesarios para facilitar tal cooperación son limitados e informales. Gracias a la creación del CSIRT-CR y a sus posteriores iniciativas orientadas a involucrar a posibles socios, tanto del sector público como privado, se hicieron algunos avances en este frente, pero la cooperación no es sistemática y es, a menudo, insuficiente.

Las autoridades costarricenses continúan vinculadas activamente a socios internacionales para actuar en varios frentes. En 2013, el Ministerio de Ciencia, Tecnología y Telecomunicaciones organizó un Simposio Regional de Seguridad Cibernética, junto con la OEA y el Network Information Center (NIC, Centro de Información de Redes) del país. El simposio reunió a funcionarios de toda la región y a representantes del mundo académico y del sector privado, con el objeto de examinar las oportunidades de continuar desarrollando las capacidades nacionales en materia de seguridad cibernética. Se brindó capacitación técnica al personal del CSIRT-CR, NIC Costa Rica, el Poder Judicial, el Banco Central, el Instituto Costarricense de Electricidad (ICE) y numerosos propietarios y operadores de infraestructura. Una segunda iniciativa similar se llevó a cabo en la primavera de 2014, junto con muchas de las mismas instituciones y organizaciones asociadas, donde participaron funcionarios de los Estados Unidos, Panamá, México, Perú, Honduras y Argentina. Los debates se centraron en temas como la seguridad de redes, el *hackeo* legítimo, las normas internacionales para combatir los delitos cibernéticos y las herramientas y técnicas relacionadas con el análisis forense digital. En otra muestra de asociación internacional eficaz, el Gobierno de Costa Rica informó que recibe asistencia técnica del Ministerio de Ciencia del Gobierno de Corea del Sur, así como del Instituto Coreano para el Desarrollo de una Sociedad de la Información (KISDI) y la Agencia Coreana de Internet y Seguridad (KISA). La asistencia técnica comprendió recomendaciones para la revisión y aplicación de una política costarricense en materia de seguridad cibernética nacional.

Si bien numerosas instituciones educativas de Costa Rica ofrecen cursos sobre seguridad y delitos cibernéticos, actualmente solo dos ofrecen títulos de grado o especializaciones. El Centro de Formación en Tecnologías de Información y Comunicación (CENFOTEC) ofrece una especialización en seguridad cibernética: Ingeniería en Seguridad de TIC, mientras que la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT) ofrece una especialización en seguridad cibernética, que comprende cursos de *hackeo* legítimo, análisis forense digital y criptografía.

No existen campañas gubernamentales oficiales de concientización sobre seguridad o delitos cibernéticos. Es cierto que las autoridades nacionales organizan charlas y cursos de capacitación sobre el tema para las partes interesadas, pero no hay una iniciativa orientada a informar al público en general acerca de las amenazas que existen en el ciberespacio. Dentro de los organismos de gobierno se llevan a cabo unas pocas actividades de concientización, en las que la Unidad de Gestión de cada organismo debe informar a todos los usuarios sobre las políticas, procedimientos y responsabilidades que les corresponden, entre ellas, la seguridad de cuentas y el uso adecuado de la información contenida en los sistemas.

Respecto de las tendencias que se observan, las autoridades nacionales informan que, aunque se ha recabado alguna información, la cantidad de casos reportados sigue siendo relativamente limitada y faltan datos concretos. Las autoridades mencionaron varios ataques esporádicos contra sitios *web* del gobierno perpetrados por grupos *hacktivistas* el año pasado, aunque pocos fueron oficialmente reportados por la institución afectada. En toda la nación, durante el año pasado, se reportaron a las autoridades alrededor de seiscientos casos de *phishing* (suplantación de identidad), *pharming* (estafa a través de ingeniería social y sitios fraudulentos) o incidentes relacionados, lo cual dio lugar a la apertura de trescientos procesos formales por parte de los organismos de investigación. Otros incidentes involucraron alguna forma de violación de comunicaciones electrónicas, como el acceso no autorizado a cuentas de usuarios. Sobre la base de la limitada información disponible, las autoridades identificaron a las instituciones gubernamentales y entidades comerciales como los dos grupos más afectados.

En julio de 2013, ocurrió un incidente importante que afectó a una institución nacional. La red de telecomunicaciones del ICE (empresa eléctrica nacional) sufrió un ataque de denegación de servicio (DoS) que se originó en Rusia, que implicó casi 25 millones de intentos para acceder al sitio en un período de 48 horas. El incidente fue detectado por el propio centro interno de la institución (CSIRT-

ICE), que notificó al CSIRT-CR, que a su vez se contactó con USCERT y sus socios en Europa. Gracias a la asistencia prestada, el incidente se mitigó por completo alrededor de doce horas después del reporte inicial.

Las autoridades estatales destacaron varios impedimentos centrales que atentan contra el fortalecimiento de la seguridad cibernética de Costa Rica. La falta de una cultura y conciencia de seguridad cibernética, incluida la adhesión de los usuarios a las normas relativas a buenas prácticas, se identificó como quizás el único impedimento importante. Asimismo, las autoridades señalaron la necesidad de actualizar las normas existentes relativas a la tecnología en el contexto de su uso, así como de brindar una mejor capacitación a las autoridades del Estado (incluso del Poder Judicial), a fin de fomentar y respaldar estas nuevas normas.

Las autoridades informaron que, dentro del gobierno, prevalece un enfoque fragmentado sobre las cuestiones de seguridad cibernética y delitos cibernéticos, por lo que cada institución trabaja como una isla independiente en lugar de hacerlo de forma coordinada o de acuerdo con una estrategia general. Si bien algunos organismos públicos crearon sus propios mecanismos y políticas en relación con la seguridad cibernética, estos deben estar más alineados y normalizados en todo el gobierno. Los crecientes requerimientos que recibe la Sección de Delitos Cibernéticos exigen un aumento correlativo de los recursos financieros y humanos para poder afrontar este volumen de trabajo.

En lo que respecta al sector privado, las autoridades informaron que la falta de leyes o normas claras relativas a la retención de registros de ISP entorpece innecesariamente su capacidad de adquirir la información requerida para la investigación. Además, se afirmó que las entidades del sector privado deberían trabajar más —incluso invertir más recursos— a fin de mejorar la seguridad en la prestación de servicios y sistemas online, inclusive mediante medidas de protección de datos de autenticación más eficaces.

Dominica

★ Roseau

Población: **71,000**
Cobertura de Internet: **55.2%**
Suscriptores de banda ancha fija: **11.9%**

El año pasado, se logró un avance importante en los esfuerzos para desarrollar el régimen de seguridad cibernética nacional de Dominica, gracias al fruto de una colaboración continua entre el Ministerio de Seguridad Nacional, Inmigración y Trabajo, y el Ministerio de Información, Telecomunicaciones y Empoderamiento de la Ciudanía. El gobierno adoptó un modelo para el desarrollo de la seguridad cibernética que se presenta como una guía. El mismo facilita los esfuerzos del rubro desde un enfoque integral y multisectorial. Si bien el país todavía no cuenta con una política nacional ni con una estrategia en términos de seguridad cibernética, se ha comenzado a trabajar con la Organización de los Estados Americanos (OEA), la Iniciativa del Commonwealth contra la Ciberdelincuencia (CCI) y el Consejo Europeo para desarrollar una política nacional a gran escala y para fortalecer la legislación contra la ciberdelincuencia. Los dos ministerios mencionados anteriormente han tomado un rol de liderazgo en el desarrollo de las capacidades del Gobierno, que incluye el trabajo hacia la creación de un Equipo de Respuesta ante Incidentes Cibernéticos nacional (CIRT) y una unidad equipada con los elementos necesarios como para investigar delitos mediante tecnologías de la información.

Actualmente, todas las denuncias de ciberdelincuencia, o actividades relacionadas, están a cargo del Departamento de Investigaciones Criminales de la Policía del Commonwealth de Dominica, que depende del Ministerio de Seguridad Nacional, Inmigración y Trabajo. A pesar de que la Policía no cuenta con una infraestructura forense cibernética, existe una gran cantidad de leyes contra la ciberdelincuencia, entre ellas la Ley contra Crímenes Electrónicos, que todavía no se han implementado y que harán que los estatutos legales de Dominica se pongan en el mismo nivel que las normas internacionales.

El Gobierno todavía no ha realizado acciones de concienciación de manera sistemática, aunque algunas instituciones financieras han hecho circular avisos de toma de conciencia en vista de la creciente ola de actividades criminales como el *phishing* (suplantación de identidad) y otros ataques. Debido a que no existe una entidad que pueda rastrear o manejar los incidentes cibernéticos, no se cuenta con información sobre los tipos y cantidades de incidentes y su impacto a nivel gubernamental o nacional. Las entidades del sector privado no tienen la obligación de informar los incidentes cibernéticos a las autoridades nacionales y lidian con estos sin participación del Gobierno.

Los esfuerzos para desarrollar sociedades regionales e internacionales se han acelerado en 2013 y 2014. Si bien todavía resta finalizar las asociaciones formales, Dominica ha sido anfitrión de eventos patrocinados por la OEA, la CCI, la Comisión Europea, la Unión de Telecomunicaciones del Caribe (CTU) y el Grupo de Operadores de Red del Caribe (CaribNOG). En el país, todavía no se ofrece capacitación académica ni existen programas de estudio relacionados con la seguridad cibernética, aunque no es infrecuente que los dominiqueses obtengan títulos sobre seguridad de la información por parte de universidades del exterior ubicadas en el Caribe, Europa o Estados Unidos. No obstante, luego de obtener los títulos, estos ingenieros capacitados buscan empleo en el exterior, algo que se repite en muchos países del Caribe. En estos momentos, para Dominica es una prioridad establecer un programa de retención de profesionales capacitados en las tecnologías de la información.

Las autoridades nacionales informaron que la falta de una política nacional y un marco estratégico, y la ausencia de iniciativas de desarrollo de las capacidades y de concientización son los mayores impedimentos para el avance de la seguridad cibernética en Dominica. También se informó que la necesidad de aumentar los esfuerzos para desarrollar las capacidades en el país se fortaleció debido a la fuga de información sensible por parte del Gobierno de Estados Unidos el año pasado.

En vistas al futuro, el Gobierno de Dominica continuará su colaboración con socios regionales e internacionales para desarrollar todavía más las capacidades del país en términos de seguridad cibernética. Se buscará la asistencia de la OEA y de otros socios internacionales para desarrollar las capacidades relacionadas con la creación y ampliación de la capacidad de respuesta ante incidentes a nivel nacional y para fortalecer las sociedades externas del país a fin de lograr cooperación y compartir información. Las autoridades también están trabajando para acceder al Convenio sobre cibercriminalidad de Budapest y establecer vínculos internacionales para combatir mejor la ciberdelincuencia. Por último, Dominica explora la posibilidad de establecer un Centro de Seguridad cibernética que se ubicará en el Dominica State College, en sociedad con agencias internacionales como la OEA, el COMSEC, la Comisión Europea, el Banco Mundial, el Banco Interamericano de Desarrollo (BID) y la Unión Internacional de Telecomunicaciones (UIT). Estas instalaciones serán un centro regional para entrenamiento y desarrollo de las capacidades.

República Dominicana

★ Santo Domingo

Población: **9,745,000**
Cobertura de Internet: **45%**
Suscriptores de banda ancha fija: **4.3%**

Los esfuerzos del Gobierno de la República Dominicana para mejorar la seguridad cibernética involucran a múltiples agencias que trabajan de forma coordinada a través de la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT). Esta Comisión tiene cinco funciones centrales. La primera es asegurar la coordinación y cooperación entre todas las agencias nacionales de la Policía, el Ejército y el poder judicial responsables que están comprometidas en responder, investigar y procesar actos de ciberdelincuencia. La segunda es coordinar y cooperar con otros gobiernos nacionales, instituciones internacionales y otras partes interesadas para prevenir y reducir la frecuencia de las actividades cibercriminales en la República Dominicana y en el mundo. La tercera es definir las políticas, establecer directivas y desarrollar estrategias y planes de seguridad cibernética para ser presentados ante el poder ejecutivo. La cuarta es promover la adopción e implementación de tratados y convenciones internacionales relacionadas con el tema. Y la quinta y última es asegurar que el Gobierno esté representado por la institución y las personas adecuadas en todas las organizaciones internacionales involucradas en la lucha contra la cibercriminalidad y en la promoción de la seguridad cibernética.

En términos de investigaciones de actos de ciberdelincuencia, se crearon dos entidades específicas: el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) en la Policía Nacional, y la División de Investigación de Delitos Cibernéticos (DID) en el Departamento Nacional de Investigaciones (DNI). La Ley 53-07, cuyo objetivo es respaldar el trabajo de estas agencias, establece como delitos una amplia variedad de actividades cibernéticas y brinda un marco para que el Gobierno pueda prevenirlas y sepa cómo responder ante ellas. No obstante, no existe una estrategia o política nacional sobre seguridad cibernética a gran escala, ni tampoco se estableció un CIRT o que cuenta con capacidades de respuesta ante incidentes similares.

Desde su creación, la DICAT comenzó una campaña de prevención de riesgos cibernéticos que consiste en una serie de charlas que se brindan en instituciones educativas y en entidades privadas y públicas. También se realizó una campaña de concientización en las redes sociales con el objetivo de prevenir la ciberdelincuencia. Otras instituciones estatales también han trabajado para informar a la población acerca de los riesgos cibernéticos y para dar consejos sobre buenas prácticas. Estas instituciones incluyen el Instituto Dominicano de las Telecomunicaciones (INDOTEL), que cuenta con un programa denominado “Internet Sano” (http://www.internetsano.do/). Para tratar las carencias en enseñanza de temas relacionados con la seguridad cibernética en las universidades del país, las autoridades del Gobierno se encuentran trabajando en asociación con el Instituto Tecnológico de Santo Domingo (INTEC) para desarrollar capacitaciones y programas de certificación relacionados con este tema.

El sector privado no está obligado a informar acerca de incidentes cibernéticos a las autoridades nacionales. No obstante, se establecieron mecanismos judiciales para solicitar de manera oficial este tipo de información por parte de entidades en el país. También se han mejorado los métodos para compartir información mediante el desarrollo de sociedades colaborativas entre el Gobierno y el sector privado, producto de los importantes esfuerzos previos realizados para generar conciencia y llegar a posibles socios del sector privado.

La cooperación con otros países también aumentó considerablemente. Se han llevado a cabo investigaciones conjuntas con autoridades de los gobiernos de España y Colombia, y los funcionarios trabajaron activamente en varias operaciones multilaterales exitosas. Como miembro de la Convención de Budapest y de varias de las redes 24-7 del G8, la Interpol y la OEA, la República Dominicana logró avances importantes en el desarrollo de mecanismos de cooperación efectiva con autoridades de otros países. De hecho, los funcionarios dominicanos afirman que el acceso del país a la Convención de Budapest y la importante ayuda obtenida para el desarrollo de las capacidades por parte de socios internacionales como la OEA fortalecieron considerablemente la postura del país en términos de seguridad cibernética. No obstante, el Gobierno informó que el mayor obstáculo para incrementar la seguridad cibernética e investigar de manera exitosa la ciberdelincuencia es la dificultad con la que se encuentra al intentar obtener información pertinente de otros países, especialmente de proveedores de servicios de internet y de operadores de redes sociales con base en los Estados Unidos.

Las autoridades nacionales informaron que el número de usuarios de internet de la República Dominicana continúa aumentando a un ritmo constante, al igual que la cantidad de personas que son víctimas de ataques y explotación. Las estadísticas con las que se cuenta muestran un aumento en los incidentes cibernéticos en el país de siete a diez por ciento (7-10%) anual en estos últimos tres años. Las víctimas son individuos, empresas y hasta el propio Gobierno. Estos son algunos de los incidentes más comunes que se han denunciado: clonación de tarjetas de crédito, difamación mediante correos electrónicos y redes sociales, *phishing* (suplantación de identidad) y estafas telefónicas. También se encontraron numerosos ataques y actos de vandalismo de sitios gubernamentales llevados a cabo por grupos de *hacktivistas*.

Las autoridades han anunciado que se abrieron 654 causas relacionadas con ciberdelincuencia en 2013, lo cual dio como resultado 300 procesos judiciales. También se anunció que se han desmantelado con éxito grupos de *hacktivistas* que operaban en el país, luego de una investigación conjunta de seis meses de duración realizada entre la Policía Nacional, el Ministerio Público, la Interpol y las autoridades de otros cuatro países, que dio como resultado la detención de seis personas afiliadas a Anonymous Dominicana y a un anexo de Anonymous con base en la República Dominicana.

Los investigadores y funcionarios responsables del análisis forense digital dentro de la DICAT reciben capacitación a diario para mantener y mejorar sus habilidades. Las autoridades del Gobierno afirman que mejorar las oportunidades de entrenamiento y desarrollo de las capacidades de su personal es una prioridad clave de cara al futuro.

Ecuador

★ Quito

Población: **15,779,000**
Cobertura de Internet: **35.1%**
Suscriptores de banda ancha fija: **5.3%**

Si bien ningún ministerio ni agencia están designados como entidades responsables de la seguridad cibernética en el Ecuador, una gran cantidad de autoridades nacionales y organizaciones comparten la responsabilidad de promoverla y combatir la ciberdelincuencia. La Secretaría Nacional de la Administración Pública, mediante su Dirección de Arquitectura Tecnológica y Seguridad de la Información, fomenta el uso y la implementación de una plataforma de Gobierno electrónico y supervisa la gestión de la seguridad de la información mediante la promulgación de disposiciones, decretos y acuerdos a nivel ministerial. La Secretaría de Inteligencia, mediante su Subsecretaría de Contrainteligencia e Infocomunicaciones y el Centro de Operaciones Tecnológicas Estratégicas, implementa medidas de seguridad dentro de las entidades gubernamentales centrales y es responsable de la formación de una unidad nacional de respuesta ante incidentes. La Superintendencia de Telecomunicaciones también es responsable de la formación y posterior operación de un CSIRT nacional, cuyo nombre tentativo es EcuCERT, mediante su Secretaría de Tecnologías de la Información. La responsabilidad principal en la investigación de la ciberdelincuencia y de las actividades criminales que involucren TIC recae en la Unidad de Investigación del Delito Cibernético de la Policía Judicial, que depende de la Policía Nacional. En algunos casos, la Unidad de Investigaciones Cibernéticas de la Procuraduría General del Estado está involucrada en las investigaciones.

Aunque todavía no se estableció un CSIRT nacional, ya se han desarrollado y están en marcha políticas y procedimientos para la seguridad cibernética y para la respuesta ante incidentes. Por ejemplo, el Decreto 166 de la Secretaría Nacional de la Administración Pública establece que todas las entidades de la Administración Pública deben cumplir con los estándares técnicos para la seguridad de la información. Además, la organización implementó el uso de firmas digitales y creó 47 departamentos. Cada uno cuenta con un oficial de TI dedicado.

A pesar de los esfuerzos pasados y actuales del gobierno para atraer a otros CSIRT nacionales y a organizaciones activas en América, y para lograr la participación del Ecuador en el Grupo de Trabajo de América Latina contra el Delito cibernético en la Interpol, la creación y el desarrollo de sociedades internacionales sigue siendo un área que debe mejorarse.

La Unidad de Investigación del Crímenes Tecnológicos comenzó a crear espacios para lograr una cooperación interinstitucional mejorada entre entidades del sector público y del sector privado, dentro del país y a nivel internacional. Se puso énfasis en la promoción del intercambio de la información y la cooperación, particularmente en la investigación del fraude electrónico y la pornografía infantil.

Estas son algunas otras iniciativas clave: participación dentro de la Asamblea Nacional para identificar reformas necesarias al nuevo Código Orgánico Integral Penal para definir y tipificar los ciberdelitos en Ecuador; desarrollo y administración de una página en Facebook (www.facebook.com/CibercrimenPJ.EC) para generar conciencia y prevenir la ciberdelincuencia mediante la publicación de quejas, alertas de seguridad, campañas de información, asistencia técnica y consejos de seguridad cibernética para los ciudadanos; participación en el Comité de Seguridad de la Asociación de Bancos Privados del Ecuador para compartir experiencias y coordinar investigaciones; y la organización de conferencias y debates en universidades, escuelas secundarias y primarias sobre ciberdelincuencia y seguridad cibernética ciudadana.

En relación con las campañas de concientización, la Secretaría de Inteligencia también creó un proyecto denominado "Promoción de una cultura de inteligencia" cuyo objetivo es justamente generar conciencia mediante la democratización y el aumento de la participación ciudadana.

Si bien actualmente no existen cursos sobre análisis forense digital y otros aspectos de la investigación de delitos que involucren las TIC, la Policía Nacional está diseñando un plan de estudios para brindar capacitación en diferentes centros de entrenamiento nacionales de la Policía orientado a agentes de investigación y detectives de la Policía Judicial La Unidad de Investigación del Delito cibernético ya recibe capacitación técnica por parte de instituciones de educación superior dentro del país y por parte de organizaciones internacionales. Aunque las autoridades nacionales no desarrollaron *software* ni herramientas relacionadas con la seguridad, existen actualmente una gran cantidad de propuestas por parte del sector académico y privado para estos desarrollos.

En Ecuador, se identificaron dos impedimentos principales para reducir la ciberdelincuencia. El primero es la falta de leyes sobre ciberdelincuencia adecuadas que criminalicen actividades específicas y que definan penas. La segunda es la constante falta de conciencia y de recursos educativos para ciudadanos en relación con el uso responsable de Internet y de las TIC, y el uso adecuado de las medidas de seguridad que brindan las redes sociales, los proveedores de servicios de correo electrónico, los sitios de *microblogging*, etcétera.

La legislación que está siendo considerada actualmente abarcaría una amplia variedad de temas clave, como por ejemplo: el comercio electrónico, y el acceso ilegal y los ataques contra la información y la integridad de los sistemas; la interceptación ilegal de información; la falsificación de información; el fraude electrónico e informático; la pornografía infantil y la explotación sexual; la protección de la propiedad intelectual; y la cooperación internacional, entre otros.

En 2013, se registró un aumento exponencial en la cantidad de quejas cibernéticas de los ciudadanos en las autoridades nacionales. La información disponible en el Sistema Automático de Trámite Judicial Ecuatoriano (SATJE) indica que 93% de los incidentes denunciados se dirigieron a la Fiscalía Nacional; 4% de las denuncias restantes se realizaron en la Policía Nacional; y 3% se realizan mediante una línea telefónica habilitada para denuncias del Ministerio del Interior. Los casos reportados por los ciudadanos estaban relacionados con ataques de interceptación ilegales sobre la integridad de la información, dispositivos de abuso de sistemas, ciberfalsificación, fraude informático, pornografía infantil y delitos contra la propiedad intelectual. Por otra parte, la cantidad de casos presentados y acumulados en el periodo 2008-2013 aumentó 203% y 458%, respectivamente.

Dentro de los procesos registrados por la Unidad de Investigación del Delito cibernético de la Policía Nacional en 2013, la mayoría de los casos (casi 80%) estuvo relacionada con la apropiación indebida mediante técnicas como el *skimming* (clonación de tarjetas), el *phishing* y la explotación de sistemas de pago en línea. La Policía Nacional informa que, en la segunda mitad de 2013, el país experimentó un aumento importante en la cantidad de incidentes de fraude electrónico, en los que el público general fue el grupo más afectado con 58,94% de todos los incidentes denunciados. Los ciudadanos también fueron víctimas de otro rango de actividades y delitos que involucran el uso de las TIC, como homicidios, esquemas piramidales, extorsiones, interceptaciones de comunicaciones y accesos no autorizados a sistemas de información. Las entidades del sector bancario son otro de los grupos más importantes en donde se detectaron incidentes, según los datos de la Policía Nacional, con 38.48% y una gran cantidad de denuncias sobre fraudes mediante métodos como el *phishing*, el *skimming* y el *bitching*. Y 2.58% de las denuncias recibidas fueron por delitos que tenían que ver con ataques a niños y menores, como la pornografía, *grooming* (captación de menores con fines sexuales), acoso sexual y *cyber-bullying*.

A finales de 2013, se alertó a las autoridades nacionales acerca de una posible amenaza de un ataque masivo, o "Hackatón", cuyo objetivo era la Secretaría de Inteligencia. Aunque el ataque nunca se concretó, la Secretaría de Inteligencia informó a otras partes interesadas nacionales y, como muestra de cooperación, se tomaron las acciones necesarias para fortalecer las posibles vulnerabilidades. Si bien no se han conocido otros incidentes específicos que hayan tenido impacto importante, se resolvieron con resultados positivos una gran cantidad de casos de fraude electrónico y pornografía infantil, a pesar de que las autoridades se vieron sorprendidas por el grado de sofisticación de las

técnicas utilizadas. Aunque los culpables fueron condenados y sentenciados por delitos relacionados con fraude electrónico y pornografía infantil, la actual falta de legislación adecuada en materia de seguridad cibernética impidió que las autoridades enjuiciaran a estas personas por ciberdelincuencia.

El Salvador

★ San Salvador

Población: **6,635,000**
Cobertura de Internet: **25.5%**
Suscriptores de banda ancha fija: **3.8%**

Existen dos ministerios que comparten la responsabilidad de la seguridad cibernética y la prevención del delito cibernético en El Salvador. El Ministerio de Justicia y Seguridad Pública es el líder designado para asuntos de seguridad cibernética, mientras que la responsabilidad de la investigación de cibercrímenes depende principalmente de la Unidad de Delitos Cibernéticos de la Policía Nacional Civil. Este organismo se encuentra actualmente en proceso de convertirse en una nueva Unidad de Delito cibernético. Se estableció un CIRT nacional, con la sigla SALCERT, y ya está en funcionamiento. Aunque aún no se ha establecido alguna política o estrategia nacional para la seguridad cibernética, ya se encuentra una en proceso de desarrollo.

Actualmente, la Policía Nacional Civil está formalizando una asociación con la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) para recibir capacitación relacionada con el delito cibernético a fin de reforzar sus capacidades existentes, desarrolladas, hasta ahora, mediante cursos en línea autodidácticos e interacción informal con autoridades con autoridades homólogas de la región.

Se han implementado mecanismos jurídicos que permiten a la Policía Nacional Civil solicitar la cooperación de empresas privadas cuando se requiera información para combatir el delito cibernético. Sin embargo, en algunos casos la ley exige que estas solicitudes se realicen a través de la Oficina del Fiscal General, responsable de las investigaciones criminales. Actualmente, la Presidencia está evaluando la propuesta de una nueva legislación con el nombre de Ley Especial contra el Delito cibernético.

El gobierno emplea una estrategia para la recuperación de datos y la continuidad operacional dentro de sus propias instituciones basada en el uso de dos sitios de almacenamiento remoto en tiempo real, un sitio primario y uno secundario, en los que almacena información de las bases de datos de red. Cuando los datos están almacenados en la computadora de un usuario y no en uno de los dos sitios de almacenamiento remoto, se utiliza *software* forense para recuperarlos. Dentro de cada institución individual se utilizan *firewalls* para filtrar paquetes de información maliciosos, con el respaldo del sistema Advance Security de Oracle para seguridad de la base de datos. El acceso externo a través de una VPN (Red Privada Virtual) está protegido por contraseña. Asimismo, el gobierno manifiesta que se utilizan medidas de seguridad adicionales, no descritas en este documento, de forma rigurosa en todas sus instituciones. Los usuarios individuales reciben un manual de políticas de seguridad cibernética que les provee instrucciones explícitas sobre el uso responsable y autorizado de sistemas de información administrados por el gobierno.

Las autoridades citan una serie de impedimentos para la mejora de la seguridad cibernética y combatir el delito cibernético en El Salvador. Los principales obstáculos son los límites de presupuesto y la falta de soporte de los ISP (proveedores de servicios de Internet) para brindar información acerca de los

usuarios sospechosos de haber cometido un delito cibernético. De un modo similar, el gobierno no mantiene relaciones de cooperación con compañías establecidas fuera de El Salvador que proveen servicios de Internet relevantes, tales como proveedores de servicios de correo electrónico, redes sociales o dueños de sitios web. Otras importantes deficiencias identificadas son la falta de un marco de trabajo legislativo integral para combatir el delito cibernético y la necesidad de más capacitación para investigadores y fiscales, además de la necesidad de brindar más oportunidades a los miembros de la Unidad de Delito Cibernético Emergente de participar en foros regionales e internacionales de desarrollo de capacidades. Finalmente, las autoridades resaltaron la falta de iniciativas de educación o concientización destinadas a informar mejor a los usuarios de Internet y TIC acerca de los riesgos y buenas prácticas para reducir sus vulnerabilidades.

Se ha informado una serie de actividades ilícitas a la Policía Nacional en los últimos años. Las autoridades comunicaron que se abrieron 72 casos de delito cibernético en 2013, que llevaron a 5 condenas. Además, desde la creación de la División de Delitos Cibernéticos en 2011, se documentaron otros 51 casos de pornografía infantil, 26 casos relacionados con amenazas o intimidación, 23 caso de diseminación ilegal de información y 15 casos de acoso sexual.

Y mientras que las leyes actuales no penalizan el *hackeo* como un delito de por sí (aunque en algunos casos se considera una forma de fraude de comunicaciones o violación de medidas de seguridad), las técnicas de *hackeo* se emplean para ganar acceso no autorizado a cuentas de correo electrónico y redes sociales, lo que sirve de base para cometer otras actividades ilícitas tales como extorsión, diseminación ilegal de información, etc. Sin embargo, dado que las técnicas utilizadas para perpetrar estos últimos delitos no están penalizadas, no hay estadísticas disponibles que permitan evaluar un aumento de uso.

En un caso destacable, un depredador sexual estaba contactando víctimas jóvenes a través de redes sociales, ganándose su confianza y luego incitándolos a crear y compartir fotografías y videos sexualmente explícitos. Se alertó a la Policía Nacional y se realizó una investigación que llevó a descubrir evidencia en la computadora del culpable. Luego, por primera vez en El Salvador, se enjuició al individuo y se lo condenó por depredación sexual de menores.

A futuro, las autoridades gubernamentales se concentrarán en la sanción de las Leyes Especiales contra Delitos Cibernéticos, la creación de una estrategia y política nacional en materia de seguridad cibernética, y el mayor desarrollo de la capacidad del personal responsable de la administración de incidentes e investigación de cibercrímenes, campañas de concientización y consolidación de las asociaciones internacionales.

Granada

★ St. George's

Población: **103,000**
Cobertura de Internet: **42%**
Suscriptores de banda ancha fija: **13.7%**

La agencia líder en materia de seguridad cibernética y prevención del delito cibernético en Granada es la Fuerza de Policía Real de Granada, y específicamente su Departamento de Tecnologías de la Información y la Comunicación (TIC). Si bien el gobierno no tiene una estrategia de seguridad cibernética a nivel nacional y no ha creado un CIRT nacional ni otro marco de trabajo para tratar incidentes cibernéticos, está en el proceso de desarrollar una campaña de concientización a través de la Comisión Reguladora de Telecomunicaciones. Y en 2013, la legislatura aprobó la Ley contra Delitos Cibernéticos número 23, que otorga al gobierno una mayor capacidad para procesar cibercriminales.

Las entidades del sector privado no están obligadas a brindar información sobre incidentes cibernéticos a las autoridades nacionales, y el gobierno no trabaja en forma activa con entidades del sector privado en asuntos de seguridad cibernética. Las autoridades nacionales informaron que la colaboración con otros países es fructífera, aunque se realiza en forma no oficial. Una sociedad entre el gobierno y la ITU e IMPACT incluyó una evaluación de la postura del país en materia de seguridad cibernética y realizó recomendaciones sobre los pasos que el gobierno puede tomar a futuro. En la actualidad, las instituciones académicas del país no ofrecen programas de grado u otros cursos relacionados con la seguridad cibernética.

Las autoridades nacionales informan que no han visto un aumento en el número de incidentes cibernéticos u otra actividad cibernética ilícita en el último año, y no tienen registro de que hayan ocurrido otros incidentes cibernéticos relevantes. Las autoridades del gobierno identificaron la falta de un CIRT nacional como el principal impedimento para el progreso de la seguridad cibernética de Granada.

Guatemala

★ Ciudad de Guatemala

Población: **15,440,000**
Cobertura de Internet: **16%**
Suscriptores de banda ancha fija: **1.8%**

Múltiples autoridades nacionales comparten la responsabilidad de las actividades en materia de seguridad cibernética y prevención del delito cibernético dentro del Gobierno de Guatemala, en el grado de competencia designado oficialmente. El Equipo de Respuesta a Incidentes de Seguridad Cibernética de Guatemala, CSIRT-gt, sirve eficazmente como el principal punto de contacto y organismo de coordinación nacional para asuntos relacionados con seguridad cibernética. La oficina del Viceministro de Gobernación es responsable de aumentar la capacidad del país para combatir el crimen organizado. Además, la Dirección de TI, dependiente del Viceministerio de TIC dentro del Ministerio de Gobernación, también cumple funciones determinadas en relación con la seguridad cibernética. Sin embargo, no existe un único organismo del estado responsable de las investigaciones de cibercrímenes o esfuerzos relacionados, y todavía no hay una estrategia o política nacional oficial en materia de seguridad cibernética, aunque se informó que actualmente hay una en desarrollo.

Cabe destacar que si bien el CSIRT-gt (www.csirt.gt) se creó en términos prácticos, no se estableció oficialmente por ley, y opera esencialmente como un servicio pro bono ofrecido por sus afiliados del sector público. Recientemente, se estableció en el país otro CSIRT (CERT-Cyberseg) y ahora se encuentra operando. Sin embargo, es una entidad del sector privado y no tiene responsabilidad a nivel nacional.

El marco legislativo actual en materia de seguridad cibernética y delito cibernético se estableció en 2009, cuando el Congreso Nacional aprobó una Ley de Delitos Cibernéticos orientada a brindar una base para prevenir y castigar los cibercrímenes y proteger la confidencialidad, integridad y disponibilidad de datos y tecnologías de la información. Actualmente, se están realizando esfuerzos para actualizar el marco legislativo, además de promover modificaciones reglamentarias y jurídicas para permitir la creación y operación del CSIRT nacional dependiente del Ministerio del Interior.

Las entidades del sector privado no están obligadas por ley a brindar información sobre incidentes específicos a las autoridades nacionales, y actualmente no hay acuerdos formales entre ambas partes respecto a dicha cooperación. La única excepción son las instituciones financieras bajo la supervisión de la Superintendencia de Bancos (SIB), que deben informar cuando se ven afectadas por un incidente de seguridad cibernética. Las autoridades reconocieron que la falta de cooperación general con el sector privado se debe en gran medida a la ausencia de una estrategia nacional en materia de seguridad cibernética, además de la falta de un marco jurídico para procesar la mayoría de las actividades que pueden considerarse cibercrímenes. Cuando las autoridades del gobierno requieren información sobre incidentes cibernéticos, la solicitan directamente a la entidad en el sector privado en cuestión, aunque no se brindó información sobre las tasas de cumplimiento de estas solicitudes.

La cooperación entre las autoridades de Guatemala y sus autoridades homólogas fuera del país es limitada y generalmente se produce en situaciones informales para propósitos específicos, entre personas u oficinas que han establecido contacto a través de la participación en talleres regionales u otras actividades. Esta colaboración se limita principalmente a entidades en Centroamérica y el Caribe.

Las autoridades informaron que las universidades e instituciones académicas de Guatemala ofrecen programas y cursos relacionados con la seguridad cibernética, incluyendo un programa de postgrado en seguridad cibernética en una universidad específica. Sin embargo, no se brindó información adicional.

En la actualidad, el Gobierno de Guatemala no mantiene ninguna iniciativa de concientización sobre seguridad cibernética oficial u organizada. No obstante, el personal individual que desarrolla diferentes tareas en el área de seguridad cibernética lleva a cabo sus propios esfuerzos para crear conciencia y promover una cultura de mayor seguridad, por ejemplo a través de blogs y entrevistas a diarios locales.

Las autoridades nacionales informaron que han observado varias tendencias importantes en el último año. Estas tendencias incluyen los siguientes aumentos aproximados en la frecuencias de actividades específicas: *skimming* (clonación de tarjetas) 100%; clonación de tarjetas de crédito/débito – 50%; distintas formas de fraude en línea/por correo electrónico (ej. estafa nigeriana, "ofertas de concursos", etc.) – 100%; *spam* – 200% (probablemente debido a la ausencia de una ley que restrinja su uso); y acceso no autorizado a sistemas de información – 100%. Además, las autoridades han observado un aumento en los ataques DDoS, percepción que se ve respaldada por información provista por el CSIRT privado (CERT-Cyberseg). Sin embargo, no queda claro si de hecho existe una tendencia creciente o si simplemente los sensores del CERT-Cyberseg están detectando más incidentes. Las autoridades también han reconocido que los números informados sobre incidentes de clonación de tarjetas de crédito/débito pueden ser bajos, ya que sospechan que los bancos se resisten a compartir toda la información disponible por miedo a que esto tenga un impacto negativo sobre su reputación y participación en el mercado. Se informó al menos un incidente en el que se supo que el banco había sufrido pérdidas considerables como resultado de una operación ilícita de este tipo, pero no se hicieron públicos los números exactos ni otra información específica.

Si bien no se ha informado de investigaciones o condenas específicas, las autoridades resaltan como éxito en el último año el progreso que han logrado con el desarrollo de CSIRT-gt como recurso para instituciones del sector público y privado, y punto focal para el alcance y la asistencia de socios regionales e internacionales. De un modo similar, algunas autoridades consideran un éxito la creación del CERT-Cyberseg, el primer CERT privado del país, y mencionan que en algunas ocasiones este equipo se ha coordinado con el CSIRT-gt para responder a incidentes relacionados con estafas en línea, spam, intentos de infiltración y ataques DDoS en pequeña escala.

Las autoridades de Guatemala han resaltado muchos impedimentos en la promoción de una mayor seguridad cibernética en su país. El primero de estos impedimentos es la ya mencionada falta de una estrategia y política nacional en materia de seguridad cibernética. Como resultado, las entidades del Estado siguen trabajando en una forma fragmentada y específica. La falta de un marco jurídico para penalizar determinadas actividades como cibercrímenes y brindar una base para investigarlas y procesarlas reviste igual importancia. Las autoridades también han enfatizado la ausencia de una cultura de la seguridad cibernética y la falta de conciencia en todos los niveles, lo que vuelve más vulnerables a los usuarios individuales e impide al gobierno adoptar las medidas necesarias para asegurar las infraestructuras críticas y de la información del país. Finalmente, se mencionó nuevamente que deben actualizarse los regímenes reglamentarios y jurídicos para permitir la formación oficial del CSIRT nacional y dotarlo de los recursos humanos y financieros que le permitirán desarrollar una capacidad de respuesta eficaz ante incidentes nacionales.

Guyana

★ Georgetown

Población: **798,000**
Cobertura de Internet: **33%**
Suscriptores de banda ancha fija: **3.7%**

El Gobierno de Guyana ha logrado varios avances considerables en materia de seguridad cibernética durante el año pasado. El más importante fue la creación del Equipo Nacional de Respuesta a Incidentes Cibernéticos de Guyana o GNCIRT (www.cirt.gy) en agosto de 2013. Si bien el GNCIRT todavía se encuentra desarrollando sus políticas, procedimientos y capacidades, ya está en funcionamiento y ha sido designado como la autoridad responsable de manejar los incidentes cibernéticos a nivel nacional. La investigación de los delitos cibernéticos sigue siendo responsabilidad del Departamento de Investigaciones Criminales de la Fuerza Policial de Guyana. Actualmente, el Gobierno de Guyana no posee una política o estrategia general de orientación para la seguridad cibernética. Sin embargo, bajo el liderazgo del GNCIRT, formado por cuatro personas, se planea desarrollar este año una iniciativa nacional de concientización sobre seguridad cibernética, la cual posiblemente se base en la campaña "PARA.PIENSA.CONÉCTATE.". Asimismo, las autoridades nacionales informan que se encuentran trabajando para crear un marco normativo que abarque la seguridad cibernética de una manera más estratégica, integral y proactiva.

Las entidades del sector privado no están obligadas por ley a informar al gobierno acerca de los incidentes cibernéticos, si bien las autoridades nacionales consideran que el trabajo en conjunto con el sector privado para apoyar las innovaciones en seguridad cibernética es de alta prioridad. Sin embargo, actualmente se está considerando obligar a los organismos gubernamentales a informar acerca de estos incidentes, para fomentar un manejo más efectivo de la seguridad cibernética y la recolección de estadísticas precisas y detalladas sobre los incidentes cibernéticos.

Se puede ver una mayor la colaboración con las autoridades homólogas de otros países, principalmente gracias a la membresía del GNCIRT en la red CICTE-OEA y el fortalecimiento de los contactos con el personal de otros CIRT nacionales en América, mediante la participación en las conferencias y capacitaciones del CICTE-OEA. Aun así, todavía se debe fortalecer el nivel de organización, la colaboración y alianza entre los equipos CIRT. En la actualidad, no se ofrecen programas de grado sobre seguridad cibernética ni programas de estudio relacionados en las instituciones académicas del país.

Desde la creación del GNCIRT en agosto de 2013, el país ha experimentado numerosos incidentes de seguridad cibernética que van desde el vandalismo de sitios *web* del gobierno para cometer fraudes con tarjetas de crédito a una estafa que sufrió un importante hombre de negocios. Si bien las autoridades no tienen datos concretos que indiquen un aumento o descenso cuantitativo en la cantidad de incidentes, ha habido un claro crecimiento de la cantidad de incidentes informados por el público. La mencionada estafa al importante empresario capturó particularmente la atención de la prensa ya que esta persona, cuya identidad sigue siendo desconocida, fue engañada para que depositara sus pagos en cuentas bancarias fraudulentas. En febrero de 2013, hubo otro incidente de gran repercusión en el que 10 sitios *web*, entre ellos siete sitios del Gobierno de Guyana, fueron vandalizados por *hackers* internacionales, quienes más tarde presumieron de sus hazañas en sus páginas de Facebook y en los sitios *web* de *hackers*. En el caso del segundo incidente, el GNCIRT pudo coordinar con los otros organismos gubernamentales afectados y la compañía privada de alojamiento *web*, y respaldarlos. En el curso de sus actuaciones, brindó un análisis diario de la situación al ministro del gobierno responsable de la seguridad nacional.

Según los informes del gobierno, los mayores desafíos que enfrenta el progreso de la seguridad cibernética de Guyana en el futuro incluyen la falta de personal dotado de las aptitudes requeridas en seguridad cibernética, las insuficientes oportunidades de capacitación para desarrollar la capacidad de seguridad cibernética y el hecho de que, si bien ésta se encuentra entre las prioridades nacionales, todavía no se la considera un imperativo de primer nivel para la seguridad.

Haití

★ Puerto Príncipe

Población: **10,671,000**
Cobertura de Internet: **9.8%**
Suscriptores de banda ancha fija: **N/A**

El Gobierno de Haití ha identificado la seguridad cibernética como una prioridad y está tomando las medidas necesarias para mejorar su capacidad nacional de manejo de ciberamenazas y lucha contra los delitos cibernéticos, aunque aún queda mucho trabajo por hacer. No existe ninguna política ni estrategia nacional oficial en materia de seguridad cibernética, ni tampoco un organismo del Gobierno de Haití responsable de manera oficial de responder a los ataques cibernéticos o delitos cibernéticos. Sin embargo, se le ha asignado a una unidad de gobernanza electrónica dentro del gabinete del Primer Ministro (Primature) la responsabilidad de trabajar con las demás demás dependencias públicas y partes interesadas en el desarrollo de capacidades y un marco para la seguridad cibernética a nivel nacional. Hace poco, esta unidad creó un grupo de trabajo en asociación con la autoridad nacional de telecomunicaciones (CONATEL), la policía nacional y la Secretaría de Seguridad Nacional, con el objetivo de fomentar la agenda nacional en materia de seguridad cibernética.

Actualmente, se involucra a ciertos organismos según los casos, muchas veces con el respaldo de autoridades extranjeras que ofrecen su cooperación. Por ejemplo, la Dirección Central de la Policía Judicial (Direction Centrale de la Police Judiciaire - DCPJ) ha tomado la iniciativa en la investigación de ataques cibernéticos identificados. Junto con el coordinador nacional de la unidad de gobernanza electrónica, CONATEL ha comenzado una campaña de concientización que consiste en una serie de eventos destinados a informar a las personas encargadas de tomar decisiones y demás partes interesadas nacionales. Otro objetivo de esta campaña es evaluar las oportunidades existentes para luchar contra las vulnerabilidades y delitos cibernéticos y aquellos relacionados con las TI. A principios de 2014, un enfoque clave ha sido el desarrollo del equipo de trabajo de múltiples partes interesadas con diversos objetivos, entre ellos: la formulación de una estrategia nacional, el trabajo con miembros del parlamento para redactar y aprobar las leyes necesarias, la creación y desarrollo de un CIRT nacional, el trabajo conjunto con la DCPJ en la investigación de delitos y ataques cibernéticos y el fortalecimiento de las alianzas con el sector privado y la comunidad internacional. Las autoridades gubernamentales han buscado activamente aprovechar la capacitación y el soporte técnico disponible que ofrecen los aliados regionales e internacionales, incluida la OEA, la UIT y las entidades de las comunidades de Europa y del Caribe. Asimismo, actualmente se están considerando nuevas leyes propuestas relacionadas con las firmas electrónicas, los servicios públicos en línea y el comercio electrónico, de conformidad con el objetivo de armonizar la legislación nacional pertinente con la de los demás países en el Caribe. A fin de mejorar las capacidades de respuesta y la cooperación entre organismos, el CONATEL y diversos actores del sector privado han recomendado que se cree cuanto antes un CIRT nacional.

Si bien el sector privado no está obligado por ley a informar a las autoridades nacionales acerca de los incidentes cibernéticos y no existen vínculos o alianzas oficiales entre el gobierno y dicho sector, sí existe cierto grado de cooperación informal y extraoficial. El año pasado, CONATEL llevó a cabo una encuesta que sugirió que los operadores bancarios y de telecomunicaciones en general están bien informados sobre el tema de la seguridad cibernética y que las empresas más grandes tienen equipos de seguridad interna. Las entidades que informaron que asignan un nivel de prioridad menor a la seguridad cibernética atribuyeron este hecho a la falta de recursos o a la falta de preocupación sobre los costos probables de las ciberamenazas. El mencionado equipo nacional de trabajo buscará involucrar a las partes interesadas clave del sector privado y tendrá como objetivo central lograr una mayor cooperación y compartir la información.

En términos de desarrollo de capacidades, si bien algunas instituciones académicas de Haití ofrecen programas de estudio sobre seguridad cibernética o temas relacionados, la mayoría no lo hace y no existen programas de grado formales sobre seguridad cibernética en el país. La mayoría de los especialistas en seguridad cibernética haitianos han estudiado en el extranjero, muchos de ellos en Francia, y ahora trabajan en áreas que van desde la seguridad de la información a la legislación cibernética y la guerra de la información, si bien no cuentan con una comunidad de colegas o una estructura de soporte técnico, tal como existen en otros países.

Las autoridades haitianas informan que el único y mayor impedimento para el progreso de la seguridad cibernética es la falta de recursos financieros y afirman que, a pesar de su predisposición a adoptar las políticas, los planes o los procedimientos requeridos para mejorar su seguridad cibernética, los niveles del presupuesto actual hacen que esto sea muy difícil, sino imposible. No obstante, se está logrando algún progreso. Las operaciones que se llevaron a cabo a principios de 2014 permitieron la captura de 69 criminales, 11 de los cuales fueron luego condenados por delitos cibernéticos.

Las autoridades gubernamentales informan un marcado aumento de la cantidad de incidentes cibernéticos conocidos, la mayoría de los cuales incluyen las redes sociales y el robo o uso indebido de la identidad e información de los usuarios. Uno de estos incidentes que atrajo la atención pública involucró el acceso no autorizado y uso indebido de la cuenta de correo electrónico de un miembro del Parlamento.

Las autoridades reconocen que la falta de un marco nacional de seguridad cibernética coloca a Haití en una situación de vulnerabilidad ante los ataques cibernéticos y el delito, y la convierte en un posible refugio para los criminales cibernéticos. Por ello, las autoridades manifiestan un fuerte compromiso a futuro para trabajar en el desarrollo de las capacidades del país en materia de seguridad cibernética, tanto a nivel interno como en colaboración con todos los aliados interesados. El momento es perfecto para crear una política en materia de seguridad cibernética. Desde el Gobierno hasta el sector privado, los actores clave hacen hincapié en la necesidad de un equipo de respuesta.

Jamaica

★ Kingston

Población: **2,715,000**

Cobertura de Internet: **46.5%**

Suscriptores de banda ancha fija: **4.3%**

El organismo principal para los asuntos relacionados con la seguridad cibernética en Jamaica es el Ministerio de Ciencias, Tecnología, Energía y Minería (MSTEM). La investigación de los delitos cibernéticos es competencia de la Unidad Forense de Comunicaciones y Delincuencia Cibernética (CFCU) de la Fuerza Policial de Jamaica (JCF). El Ministerio de Seguridad Nacional y la Oficina del Fiscal General también tiene un rol de influencia en los esfuerzos actuales para crear un régimen nacional de seguridad cibernética.

En especial, el gobierno ha establecido un Equipo de Trabajo Nacional de Seguridad cibernética (NCSTF) compuesto por una gran parte de los representantes de las partes interesadas del sector público y privado, así también como del sector académico y de la sociedad civil. Al NCSTF se le otorgaron varias tareas centrales. Estas asignaturas incluyen: asistir en la creación de un marco que ayude a generar confianza en el uso del ciberespacio y la protección y seguridad de los recursos relacionados; fomentar una mayor colaboración entre todas las partes interesadas; establecer un programa de educación pública y de concientización, y formular una estrategia para desarrollar, incrementar y retener talentos cibernéticos de gran calidad para el equipo de trabajo nacional.

Si bien el gobierno aún no ha adoptado una política o estrategia nacional sobre seguridad cibernética, el mencionado NCSTF ha comenzado un proceso para desarrollar una bajo el liderazgo de MSTEM y con la ayuda de la OEA. Ya se ha creado el primer borrador de una estrategia, que está en proceso revisión por parte de las autoridades pertinentes y se espera que esté terminada hacia fines del primer semestre de 2014.

El Gobierno también se encuentra en el proceso de establecer un CSIRT nacional para ayudar en la protección de la infraestructura cibernética en línea de Jamaica, mediante la coordinación de tareas destinadas a prevenir las ciberamenazas, y responder a ellas. Se ha preparado un informe de evaluación y las Especificaciones de los Requerimientos de Usuario del CSIRT, con la ayuda de la Alianza Internacional Multilateral contra las Ciberamenazas de la Unión Internacional de Telecomunicaciones (UIT-IMPACT). Las autoridades gubernamentales esperan que el CSIRT esté en funcionamiento en algún momento de 2014.

Jamaica no tiene actualmente ninguna campaña de concientización en materia de seguridad cibernética; sin embargo, la creación e implementación de una es un objetivo estratégico clave del borrador actual de la estrategia sobre seguridad cibernética. Asimismo, actualmente hay iniciativas de entidades del sector privado y público, por ejemplo de las instituciones financieras y la JCF respectivamente, que buscan generar conciencia sobre áreas específicas de seguridad cibernética.

En respuesta al aumento de incidencias de delitos cibernéticos, en enero de 2013 se creó un Comité Selecto Conjunto de las dos cámaras del Parlamento, compuesto por once miembros, para considerar e informar sobre el funcionamiento de la Ley de Delitos Cibernéticos. Las cámaras del Parlamento adoptaron las recomendaciones realizadas por el Comité respecto a las enmiendas a la Ley y actualmente se está trabajando para implementarlas. Dichas enmiendas incluyen el aumento de las penas por delitos definidos conforme a la Ley y la penalización de acciones que perjudican las investigaciones y actividades tales como el fraude informático, la falsificación y la comunicación malintencionada.

En mayo de 2014, el Tribunal Superior entendió en una causa que dio como resultado el procesamiento exitoso de un delito informático y actualmente se están procesando otros tres casos en los tribunales, con cargos definidos por la Ley de Delitos Cibernéticos.

Actualmente se llevan a cabo capacitaciones y actividades relacionadas con el desarrollo de capacidades orientadas al personal clave del gobierno; la policía y los fiscales reciben capacitación sobre los aspectos clave de la seguridad y delitos cibernéticos y los funcionarios de gestión de sistemas de la información de todo el gobierno reciben capacitación sobre seguridad en redes.

Hoy en día, las entidades privadas no están obligadas por ley a informar a las autoridades gubernamentales sobre asuntos relacionados con el hackeo o los ataques cibernéticos. Sin embargo, existe una cooperación entre la policía y las entidades privadas, mediante la cual la policía se compromete a investigar los incidentes o atentados que puedan sufrir las entidades. El borrador de la estrategia nacional identifica como objetivo principal la definición de medidas y mecanismos destinados a lograr una mayor cooperación y compartir información entre el sector público y privado.

Si bien a la fecha no se ha producido ningún incidente importante o detectado una amenaza que requieran la colaboración con otros países, se reconoce la posibilidad de que se produzca un incidente del estilo, lo que ha promovido la creación de un CSIRT nacional y la adopción de otras medidas, contempladas en el borrador de la estrategia.

En cuanto a la disponibilidad de la capacitación académica en seguridad cibernética, Jamaica se encuentra relativamente en una mejor posición que la mayoría de sus vecinos de la región del Caribe. Dos de sus principales universidades (Northern Caribbean University y University of the West Indies) ofrecen títulos en cibernética con algún grado de especialización en seguridad de la información y seguridad de redes, así también como un programa de estudios más avanzado en criptografía. Otras instituciones (University of Technology y University College of the Caribbean) exigen a los alumnos de la carrera de Ciencias Cibernéticas que completen un programa de estudios sobre seguridad cibernética y de TI.

Con respecto a las tendencias observadas, las autoridades nacionales informaron un aumento de 15% en incidentes cibernéticos en 2013, en comparación con el año anterior. Las actividades más predominantes informadas incluyen el fraude en línea en transacciones con terceros, difamación y extorsión por Internet. A pesar de que aumentó la denuncia de dichos incidentes a las autoridades gubernamentales, sólo se pudo encontrar a aproximadamente 5% de los autores de los delitos, principalmente debido al nivel mínimo de apoyo recibido por parte de las entidades de otras jurisdicciones.

Las autoridades nacionales han identificado varios desafíos clave que Jamaica enfrenta en el área de seguridad cibernética, entre ellos: la falta de una estrategia oficial de seguridad cibernética para garantizar un marco coherente; la falta de un CSIRT/CERT nacional; personal insuficiente en la CFCU para investigar los incidentes de delitos cibernéticos de manera oportuna, y un escaso nivel de conciencia sobre los imperativos en materia de seguridad cibernética y los efectos de los delitos cibernéticos. No obstante, tal como lo demuestra la información provista, se están tomando activamente las medidas necesarias para abordar cada uno de estos desafíos en el corto y mediano plazo y se espera una mejoría.

México

★ México D.F.

Población: **118,419,000**
Cobertura de Internet: **38.4%**
Suscriptores de banda ancha fija: **10.5%**

La Policía Federal de México es la principal autoridad operacional en lo que respecta a iniciativas relativas a la seguridad y el delito cibernético en México, pero muchas otras instituciones gubernamentales también desempeñan un rol activo. Dentro de la Policía Federal, la División Científica mantiene una unidad responsable de coordinar actividades para investigar, prevenir y procesar toda conducta considerada delictiva que utiliza medios electrónicos y cibernéticos. Además de desarrollar una amplia gama de actividades relacionadas con la seguridad de la tecnología cibernética, la información y las comunicaciones a nivel nacional, esta unidad también utiliza técnicas de investigación especiales como el monitoreo de la actividad pública en Internet, el uso de la figura de usuario simulado y operaciones encubiertas. La División Científica también es la sede del principal equipo de respuesta a incidentes de seguridad cibernética (CSIRT) con responsabilidad a nivel nacional, el CERT-MX. Si bien el CERT-MX no tiene un sitio *web* propio, sus datos de contacto pueden encontrarse en el sitio *web* del Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST).

Además, para que las partes interesadas más relevantes participen en la promoción de la agenda nacional de seguridad cibernética, se creó el Comité Especializado en Seguridad de la Información (CESI) con la misión de desarrollar una Estrategia Nacional de Seguridad de la Información (ENSI), que guiará todas las acciones que emprendan las entidades del gobierno federal para prevenir, identificar, neutralizar o contrarrestar riesgos y amenazas a la seguridad de la información. La ENSI fue creada a partir del reconocimiento de la necesidad de acciones concretas, claramente articuladas y coordinadas para fortalecer las capacidades del Estado en materia de seguridad de la información, seguridad cibernética, delito cibernético, ciberdefensa y protección de infraestructuras. A través del CESI, las autoridades también desarrollaron un Protocolo de Colaboración entre el CERT-MX y las diversas dependencias del gobierno central mexicano, para abordar y responder ante los incidentes cibernéticos que podrían hacer peligrar las infraestructuras críticas del país.

El personal de la División Científica recibió y continúa recibiendo capacitación especializada brindada por el Sistema de Desarrollo Policial (SIDEPOL) de México, y por muchas otras organizaciones de seguridad y policiales en países que incluyen Colombia, Estados Unidos, Holanda y Japón. Se hace hincapié en que las actividades de formación recibidas por el personal garanticen su capacitación de acuerdo con las responsabilidades específicas que les corresponden, y que sus conocimientos y habilidades estén lo más actualizadas posible. La capacitación relativa a las investigaciones y análisis forenses digitales se centra en la cadena de custodia, la identificación y confiscación de evidencia digital, los sistemas analíticos telefónicos, los análisis forenses digitales y los análisis forenses de dispositivos celulares. Asimismo, algunos miembros del personal recibieron capacitación de organizaciones no gubernamentales tales como el Centro Nacional y el Centro Internacional para Niños Desaparecidos y Explotados (NCMEC e ICMEC, respectivamente).

Para garantizar la continuidad de las operaciones y la garantía de los datos a nivel de la institución, se hace un respaldo de la información y se aplican técnicas de recuperación de datos en dispositivos individuales según las necesidades. Además, todas las instituciones gubernamentales principales deben cumplir con los requisitos de la norma ISO 207001 relativos al sistema de gestión de seguridad de la información.

Las solicitudes de cooperación con entidades del sector privado suelen estar gestionadas por el área de Representación Social del Ministerio Público. El CERT-MX también se comunica y coopera en forma directa con entidades financieras privadas. Uno de los principales objetivos de la ENSI es aumentar e institucionalizar la cooperación y el intercambio de información entre todos los sectores de la sociedad –públicos y privados– de manera más integrada.

El CERT-MX ha logrado importantes avances en la promoción del establecimiento de CSIRT propios de cada organización en muchas instituciones federales, y está incentivando la creación de proyectos similares en industrias clave del sector privado para lograr que la respuesta ante incidentes cibernéticos sea más eficaz y coordinada.

Las autoridades mexicanas han desarrollado relaciones de colaboración activas con otros gobiernos y organizaciones internacionales, trabajando con entidades policiales nacionales y con CSIRT, y a través de organizaciones internacionales como FIRST y la Organización de Estados Americanos (OEA/CICTE).

Los esfuerzos del gobierno por generar conciencia sobre seguridad cibernética incluyeron la organización de varias conferencias para instituciones gubernamentales y educativas (de nivel primario a universitario), y tareas de divulgación entre ciudadanos y otras entidades públicas y privadas.

Las autoridades gubernamentales mencionaron un gran número de impedimentos para reducir el delito cibernético y aumentar la seguridad cibernética en México. Uno de ellos es la constante falta de legislación que permita a las entidades policiales actuar en forma inmediata para enfrentar las amenazas a la seguridad y los delitos cibernéticos. La capacidad limitada de las entidades policiales para actuar en muchas instancias debilita las investigaciones, perpetúa la sensación de impunidad entre los grupos criminales organizados y les permite implementar las últimas tecnologías y técnicas para cometer delitos. El otro gran impedimento identificado es la constante falta de conciencia entre la población general sobre seguridad cibernética, incluidos riesgos y prácticas recomendadas.

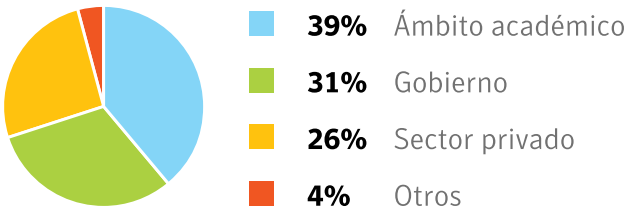
Según los datos que mantiene la División Científica de la Policía Federal, hubo un aumento de 113% en incidentes de seguridad cibernética en 2013 comparado con el año anterior. Además, los datos preliminares sobre 2014 hasta ahora sugieren un aumento incluso más pronunciado en incidentes detectados: nada menos que 300% más que en 2013. Cabe destacar que el marcado aumento en el corriente año se atribuye principalmente a las mejoras de los procesos de identificación de incidentes a nivel nacional y en la generación de nuevos vectores de ataque.

De los incidentes denunciados ante la Policía Federal Mexicana, y sin incluir incidentes que involucraron a ciudadanos particulares, aproximadamente 31% fueron contra instituciones gubernamentales, 26% contra entidades del sector privado, 39% contra organizaciones académicas y 4% contra otras entidades. Los incidentes de acceso lógico no autorizado aumentaron aproximadamente 260%, las infecciones de *malware* aumentaron 323% y los incidentes de *phishing* aumentaron un 409%, mientras que los ataques de denegación de servicio disminuyeron 16%.[01]

También se observaron aumentos considerables de los incidentes relativos a amenazas persistentes avanzadas (APT) contra medianas empresas y el uso de código malicioso a fin de *hackear* información de usuarios para luego intentar extorsionarlos. Este último tipo de incidentes también provocó un aumento en el uso de *malware* que utiliza encriptaciones de seguridad complejas para atacar a los servidores de pequeñas y medianas empresas (PyME), lo que tiene un impacto cada vez mayor en el sector productivo.

Entidades afectadas por los delitos informáticos

Fuente: Gobierno de México



01 Esta información fue proporcionada por el Gobierno de México. Además, estas estadísticas sólo abarcan casos en que se inició una investigación oficial sobre cibercrimen, a pedido de la entidad afectada.

Los incidentes de seguridad cibernética más denunciados incluyeron el uso de *malware*, *phishing*, *hackeos* y vandalismo y las intrusiones en sistemas. Los incidentes de fraude y extorsión más denunciados incluyeron los fraudes de comercio electrónico, las estafas nigerianas, los fraudes de banca electrónica y la extorsión. Además, las denuncias de quejas particulares incluyeron la difamación, las amenazas, el robo de contraseñas, la suplantación de identidad y el acoso.

Un caso particularmente digno de mención involucró el uso de un *ransomware* (secuestro informático) disimulado con el nombre "Protección Contra *Spam* Pornográfico Infantil 2.0". El autor del delito obtuvo acceso a las computadoras de sus víctimas, instaló el *malware*, encriptó sus contenidos, bloqueó el acceso para los dueños y exigió USD 3,000 para recuperar los archivos. Sin embargo, las autoridades dicen que desde este caso se han visto limitadas a seguir sólo algunas líneas de investigación dada su falta de información sobre las últimas técnicas de intrusión y codificación maliciosa.

Dado que cada estado de la República Mexicana enjuicia a las personas en forma independiente por los delitos cometidos, no existen cifras disponibles respecto del total de enjuiciamientos por delitos cibernéticos a nivel nacional.

Nicaragua

★ Managua

Población: **6,216,000**

Cobertura de Internet: **13.5%**

Suscriptores de banda ancha fija: **1.7%**

Dentro del Gobierno de Nicaragua, la responsabilidad en materia de seguridad cibernética y delito cibernético está compartida entre varios organismos e instituciones. Las dos entidades principales son el Consejo Nicaragüense de Ciencia y Tecnología (CONICYT - www.conicyt.gob.ni) y la Comisión de Gobierno Electrónico de Nicaragua (GOBENIC - http://www.gobenic.gob.ni), adscritos a la Vicepresidencia de la República.

El Gobierno de Nicaragua no tiene ninguna estrategia ni política oficial en materia de seguridad cibernética. En la actualidad, tanto el CONICYT como la GOBENIC se ocupan del uso y la explotación de las TIC que afectan a los sistemas de información, los datos públicos y el comercio electrónico, con relativamente poco énfasis en la seguridad de los sistemas de información en sí. Está previsto que esas dos autoridades propongan en un breve plazo nuevas leyes sobre delito cibernético y nuevas políticas gubernamentales sobre seguridad de la información, para prevenir incidentes que afectan a los sistemas de información y responder ante ellos.

Hasta la fecha, el Gobierno de Nicaragua no estableció un CSIRT ni ningún mecanismo, procedimiento ni política formal para responder ante los incidentes cibernéticos. Así, no hay ninguna autoridad a nivel nacional capaz de brindar una respuesta inmediata ante un incidente de seguridad crítico.

Tampoco existe ninguna oficina, división ni unidad designada oficialmente para prevenir o investigar los cibercrímenes. Sin embargo, la Policía Nacional llevó a cabo investigaciones que involucraron computadoras y/o evidencia digital, relacionadas principalmente con la clonación de tarjetas de crédito, y realizó análisis forenses y tareas de recuperación de información digital para presentarla como evidencia en juicios penales relacionados con el crimen organizado y el lavado de dinero, entre otros delitos graves. Estos esfuerzos han involucrado el trabajo de diversas ramas de la Policía

Nacional, que incluyen a la División de Delitos Especiales, la Dirección de Investigación Económica, la Dirección de Inteligencia Policial, la Dirección de Auxilio Judicial y el Laboratorio de Criminalística. Y cada vez más el Laboratorio de Criminalística brinda apoyo a otras instituciones del Estado cuando un incidente requiere un análisis forense digital.

Cabe señalar que la Dirección de Investigación Económica propuso la creación de un Departamento de Análisis Forenses Cibernéticos (DAFI), para actuar como organismo técnico especializado y coordinar el trabajo de las diversas entidades policiales y judiciales que combaten el crimen organizado y otros delitos complejos que suelen involucrar el uso de TIC. Además, el Laboratorio de Criminalística creó un departamento especializado en el análisis y la verificación de evidencia audiovisual en formatos digitales para brindar apoyo a las investigaciones penales relevantes. Los funcionarios que trabajan en estas tareas en la Policía Nacional reciben capacitación de expertos de muchos otros países que incluyen México, Guatemala, El Salvador, Estados Unidos y España.

Si bien no ha habido nuevas leyes aprobadas recientemente, Nicaragua tiene en vigencia un marco legislativo que permite a las autoridades gubernamentales investigar y enjuiciar determinadas actividades relativas a las TIC, y tomar otras medidas necesarias para fortalecer la postura del país en materia de seguridad cibernética. Las leyes pertinentes actualmente en vigencia incluyen: Artículo 197 sobre registros prohibidos (Título III, Capítulo I), Artículo 198 sobre acceso y uso no autorizado de información (Título III, Capítulo I), Artículo 229 sobre estafas cibernéticas (Título VI, Capítulo V), Artículo 245 sobre la destrucción de registros cibernéticos (Título VI, Capítulo VIII), Artículo 246 sobre el uso de programas destructivos (Título VI, Capítulo VIII), Artículo 250 sobre protección de software (Título VI, Capítulo IX), y Artículo 275 sobre la incautación de secretos de empresas (Título VI, Capítulo VIII).

Según se informó, en la actualidad la mayoría de los legisladores de Nicaragua creen que el uso de TIC y de Internet son ante todo un medio para cometer otros delitos frecuentes –como fraude, lavado de dinero, pornografía infantil, falsificación, robo de propiedad intelectual, corrupción de menores, extorsión, amenazas, terrorismo, etcétera– y no un espacio de actividades que son potencialmente delitos en sí mismos. Así, el consenso actual en la legislatura es que no hay una necesidad apremiante de contar con una nueva ley que trate específicamente del delito cibernético.

Si bien el Código Penal de Nicaragua requiere que toda persona con información sobre un delito que es objeto de investigación la comparta con las autoridades investigadoras, no existe ninguna otra obligación legal de que las empresas privadas denuncien ante el gobierno los ataques cibernéticos ni otros incidentes que provoquen daños o pérdida de datos. En general para obtener información relacionada con un incidente específico, las autoridades investigadoras deben presentar una solicitud formal ante el proveedor de servicios de Internet (ISP) correspondiente u otro operador. Las autoridades informaron que entidades del sector privado de Nicaragua, incluido el organismo regulador de las telecomunicaciones, suelen utilizar poco sus sistemas de respaldo de datos, y no existen procedimientos de supervisión o control del uso de servidores proxy ni retención de datos, que se necesitarían para investigar incidentes de seguridad cibernética.

La cooperación internacional entre autoridades nicaragüenses y las de otros países hasta ahora es limitada. Las autoridades mencionaron una instancia de colaboración en la que INTERPOL de Nicaragua cooperó con autoridades españolas en una investigación internacional de una red de pedofilia involucrada en la producción y publicación de pornografía infantil en la *web* desde España.

Muchas instituciones académicas que incluyen a la Universidad Nacional de Ingeniería, la Universidad Central y la Universidad Nacional de Managua ofrecen cursos y capacitaciones especializadas en temas relativos a la seguridad de la información y ciencia forense cibernética.

Hasta el momento el gobierno no desarrolló ninguna campaña nacional de concientización sobre seguridad cibernética. Según las autoridades, sólo las instituciones financieras privadas se ocupan activamente de fomentar la concientización sobre seguridad cibernética. Sin embargo, se lanzó una campaña por televisión y radio a nivel nacional para informar a los padres sobre cómo proteger a sus hijos contra la explotación y el tráfico de personas, incluidas las amenazas online o las que involucran el uso de TIC.

Las autoridades nacionales dijeron no tener datos fehacientes ni estadísticas cuantitativas sobre los cambios en la incidencia de los cibercrímenes en 2013. Sin embargo, según la información disponible, el sector comercial fue el más gravemente afectado el año pasado. En un incidente considerado particularmente significativo, un grupo de personas obtuvieron acceso no autorizado a un servidor *web* y concretaron un ataque masivo de denegación de servicio en varios sitios de servicios asignados a diversas empresas, lo que provocó daños a los sitios de los suscriptores. Los autores del delito trabajaban para una de las empresas en cuestión y fueron identificados mediante un análisis de las direcciones IP y de los logs obtenidos de los servidores afectados, y se restableció el servicio. Muchas otras historias de éxito tuvieron que ver con investigaciones que recibieron apoyo de los ISP, que aceptaron identificar el origen de las comunicaciones electrónicas maliciosas, los fraudes, las estafas, las extorsiones, las amenazas o actos similares. Más tarde esa información se utilizó como evidencia en procesos judiciales que tuvieron como resultado condenas exitosas.

Con miras al futuro, las autoridades nacionales mencionaron varios desafíos o impedimentos clave que deberán resolverse para afianzar el régimen de seguridad cibernética de Nicaragua. Primero, habrá que ganarse la voluntad política de los legisladores mediante esfuerzos por concientizarlos acerca de la necesidad de contar con nuevas leyes contra el delito cibernético, y con una nueva unidad especializada encargada de identificar, investigar y enjuiciar a los autores de este tipo de delitos.

En forma similar, se debe hacer lo posible por aumentar la voluntad política en las esferas más altas del gobierno para participar en foros auspiciados por foros e iniciativas regionales e internacionales. También es preciso revisar, fortalecer y armonizar las leyes existentes y las nuevas, y aclarar las normas que rigen los procedimientos penales para garantizar que las autoridades nacionales competentes puedan investigar y enjuiciar los cibercrímenes. Debe establecerse formalmente una Unidad de Delitos Tecnológicos dentro de la estructura de la Policía Nacional, para actuar como organismo técnico especializado encargado de investigar, analizar y coordinar acciones en respuesta a las necesidades de las autoridades policiales y judiciales.

También se recomendó la creación de un CSIRT nacional oficial que se encargue de prevenir, responder a incidentes cibernéticos y mitigar sus efectos, y de coordinar entre el gobierno y otras posibles partes interesadas ante un caso de ataque cibernético o un delito cibernético grave. Se debe establecer un régimen de cooperación internacional más dinámico y eficaz, para mejorar el intercambio de información y aumentar las oportunidades de capacitación para el personal correspondiente con respecto a las amenazas, tecnologías y técnicas más nuevas.

Por último, las autoridades hicieron hincapié en la necesidad de desarrollar un enfoque de seguridad cibernética nacional e integrado bajo el liderazgo del CONICYT y la GOBENIC, con el objetivo de reducir las vulnerabilidades cibernéticas de Nicaragua.

Panamá

★ Ciudad de Panamá

Población: **3,605,000**
Cobertura de Internet: **45.2%**
Suscriptores de banda ancha fija: **7.8%**

Dentro de la esfera del Gobierno de Panamá, la institución responsable de la supervisión y la dirección de asuntos relativos a la seguridad cibernética es la Autoridad Nacional para la Innovación Gubernamental (AIG), que funciona a través del Centro de Respuesta a Incidentes de Seguridad Cibernética (CSIRC) de Panamá. El Fiscal Especial para delitos contra la propiedad intelectual y seguridad cibernética, que integra el Ministerio Público, y la Dirección de Investigación Judicial, son los organismos que guían la investigación y la acción judicial en caso de delitos cibernéticos.

A principios de 2013, el Gobierno de Panamá aprobó la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica (ENSC+IC), que orienta y coordina todas las medidas adoptadas en el ámbito nacional para progresar en la postura asumida por el país respecto de la seguridad cibernética. La ENSC+IC persigue una serie de objetivos principales, entre ellos: combatir el uso de TIC (Tecnologías de la Información y la Comunicación) con fines terroristas o criminales; proteger a los menores de edad; incrementar la capacidad de resiliencia de la infraestructura crítica frente a incidentes cibernéticos o ataques; la concientización y educación en materia de seguridad cibernética, incluso en lo relativo a prevención y buenas prácticas; reforzar las alianzas con el sector privado, la sociedad civil, el mundo académico y otras partes interesadas; aumentar la colaboración nacional e internacional; y promover una cultura de seguridad cibernética. Actualmente, la ENSC+IC está siendo implementada por diversas instituciones del país y, según estimaciones oficiales, su implementación total llevará por lo menos tres años.

CSIRT PANAMÁ es el Centro Nacional de Respuesta a Incidentes de Seguridad Cibernética de Panamá, que administra la Autoridad Nacional para la Innovación Gubernamental, en virtud del Decreto Ejecutivo Nº 709 (2011). El CSIRT PANAMÁ coordina todas las actividades orientadas a prevenir y responder a ataques dirigidos contra los sistemas cibernéticos gubernamentales e infraestructuras que se consideren críticas para el Estado, y funciona como eje central en las relaciones con los CSIRT de otros países. Asimismo, promueve la colaboración permanente y brinda asesoramiento a las partes interesadas respecto de posibles medidas para aumentar la seguridad; funciona como depósito de información sobre incidentes, herramientas y tecnologías para ciberdefensa y protección; e investiga y difunde información sobre nuevas tecnologías y herramientas en el área de la seguridad cibernética.

Dentro de la Dirección de Investigaciones Judiciales se creó una unidad investigadora sobre delitos cibernéticos, que está siendo objeto de desarrollo y capacitación para llevar a cabo investigaciones y tareas digitales forenses. La capacitación inicial del personal incluye clases dadas por el plantel técnico de la Oficina de Seguridad de la Información, que se complementaría con una pasantía en la Oficina y el Instituto Nacional de Medicina Legal, Subdirección de Cibernética Forense. Las autoridades informaron que el alcance de la capacitación será ampliado en el futuro para reforzar las capacidades investigadoras de los alumnos para la realización de tareas de confiscación, recolección y gestión de pruebas digitales.

A la fecha, Panamá ha contrarrestado actividades cibernéticas ilícitas con diversos instrumentos, muchos de los cuales han sido adoptados hace relativamente poco tiempo. Estas herramientas incluyen la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica (2013); el

Documento de Posición sobre Resiliencia de las Infraestructuras Críticas, Protección de Menores de Edad en Internet y Seguridad Cibernética (2013); Ley Nº 79 – Adopción del Convenio de Budapest (2013); y adhesión oficial al Convenio de Budapest (2014). En la actualidad existe también una iniciativa ante la Asamblea Nacional para reformar el Código Penal en materia de delitos cibernéticos.

La adhesión por parte de Panamá al Convenio de Budapest es un importante paso adelante en la agenda oficial del gobierno para combatir la ciberdelincuencia. Para cumplir con los requisitos de dicho instrumento, el Código Penal de Panamá será reformado e incorporará nuevas conductas como actos que constituyen ciberdelitos y se elaborarán leyes relativas a la recolección de pruebas digitales y la protección de datos personales.

En Panamá, las entidades del sector privado no tienen la obligación de brindar información acerca de ataques cibernéticos, independientemente de que puedan o no haberse visto comprometidos ciertos datos. No obstante, las autoridades gubernamentales han dedicado su tiempo a reforzar sus relaciones con el sector privado en distintos aspectos de la seguridad cibernética, especialmente cuando estas entidades privadas son titulares u operadoras de infraestructura, o brindan servicios que se consideran críticos para el Estado. Por ejemplo, a pesar de la ausencia de reglamentaciones que exijan informar o compartir información, las autoridades locales mantienen abiertas y activas las líneas de colaboración con las principales empresas privadas del sector bancario e hidroeléctrico. Sin embargo, existe un principio jurídico arraigado que establece que las empresas privadas tienen el deber de cooperar con la policía y el Procurador General cuando se encuentre en curso una investigación; ello incluye brindar la asistencia o información que se les solicite.

CSIRT Panamá ha colaborado con diversos CSIRT nacionales de la región y del resto del mundo, incluidos los de Brasil, Alemania, México y Venezuela, entre otros. La reciente adhesión por parte del Estado al Convenio de Budapest brinda un marco para una posible colaboración permanente a través de investigaciones, asistencia jurídica recíproca, y extradiciones con algunos países dentro y fuera de América.

Las autoridades nacionales informaron que tanto las universidades del sector privado como el público ofrecen programas de maestría en seguridad cibernética, ingeniería cibernética, controles y auditoría. Asimismo, la Autoridad Nacional para la Innovación Gubernamental, a través de su Instituto de Tecnología e Innovación, y el Instituto Nacional de Formación Profesional y Capacitación para el Desarrollo Humano (INADEH) brindan cursos especializados sobre temas relativos al ciberdelito y la seguridad cibernética.

En 2013, Panamá se unió formalmente al movimiento de mensajería PARA.PIENSA.CONÉCTATE. para potenciar e implementar en todo el país una campaña de concientización que permita afianzar una cultura de seguridad cibernética y combatir la ciberdelincuencia. Más aun, CSIRT Panamá brinda talleres y seminarios abiertos dedicados a los aspectos técnicos y administrativos de la seguridad de la información para el personal TIC de instituciones públicas, así como a los miembros de la sociedad civil que estén interesados.

Las autoridades de Panamá informaron que la cantidad de incidentes cibernéticos denunciados aumentó 30% de 2012 a 2013. Se observó un marcado aumento en el porcentaje de incidentes relacionados con *phishing* (suplantación de identidad), que ascendió de 7%, en 2012, a 47% en 2013. De manera similar, se observó un importante incremento en incidentes del tipo relacionado con programas maliciosos, que pasó de 3% a 21% sobre el total de incidentes en los que intervino CSIRT Panamá, con lo que se convirtió en el tipo más frecuentemente denunciado entre los que se resolvieron el año pasado. Otros incidentes cada vez más frecuentes incluyen: deformación de página *web*, acceso no autorizado a sistemas y cuentas, y ataques de denegación de servicio (DoS). Las actividades relacionadas con ciberdelitos denunciadas con mayor frecuencia incluyen: pornografía infantil, *cyber-bullying*, robo de propiedad intelectual, suplantación de identidad, fraude y otros delitos financieros, y ataques a las redes sociales.

En cuanto a los procesos o bienes que se encuentran más expuestos y vulnerables frente accesos sin autorización y violaciones de datos, las autoridades han mencionado a las páginas de Internet de bancos, portales de Internet gubernamentales, cuentas de correo personales, cuentas comerciales, cuentas postales institucionales y procesos de comercialización. Esta determinación no parece estar

en línea con los datos disponibles en materia de casos de ciberdelincuencia iniciados en 2013. Las autoridades informaron que se inició un total de 262 casos el año pasado, que incluyen: 118 casos de delitos financieros, 85 casos de violaciones a la seguridad cibernética, 30 casos de pornografía infantil y 1 caso de terrorismo, entre otros.

Para ejemplificar un incidente importante denunciado, las autoridades hicieron referencia a un caso en el que una persona obtuvo acceso sin autorización a la red social Twitter. El ataque fue llevado a cabo desde un servidor en Panamá y, luego de la investigación, el autor del delito pudo ser identificado y detenido. En ocasiones, los investigadores han experimentado ciertas dificultades para reunir las pruebas necesarias del servidor ya que éste se encuentra programado en LINUX, y los investigadores no estaban familiarizados con este sistema.

Dado el gran progreso realizado por las autoridades gubernamentales en 2013, no resulta difícil identificar ejemplos de medidas adoptadas que hayan sido exitosas. Las autoridades mencionan la adhesión por parte del país al Convenio de Budapest sobre la Ciberdelincuencia como quizás el logro más importante a la fecha.

Las autoridades gubernamentales remarcan que la postura actual del estado panameño es un claro reflejo del compromiso del país hacia un libre acceso a la información, la resiliencia de infraestructura crítica, y la protección de los sistemas gubernamentales y los datos personales de los ciudadanos. No obstante, las autoridades admiten que aún queda mucho por hacer. Se informó que el principal obstáculo para un mayor desarrollo de la seguridad cibernética en Panamá probablemente se deba a la falta de conocimiento de la dependencia que las infraestructuras críticas tienen respecto de los sistemas cibernéticos. Debido a esta falta de conocimiento se torna difícil fomentar la conciencia sobre la cuestión, así como lograr aprobaciones presupuestarias para proyectos técnicos. Otros impedimentos mencionados incluyen la necesidad de una mayor capacitación, la naturaleza evolutiva y fluida de la tecnología, la necesidad de montar el equipamiento de un laboratorio informático forense, la falta de una unidad de investigación sobre ciberdelincuencia, y la tendencia de las víctimas a no denunciar los ciberdelitos. La reciente Estrategia Nacional y el Plan de Acción, y otras iniciativas permanentes deben procurar resolver cada uno de estos impedimentos en el corto a mediano plazo.

Paraguay

★ Asunción

Población: **6,849,000**

Cobertura de Internet: **27%**

Suscriptores de banda ancha fija: **1.2%**

El Equipo de Respuesta a Emergencias Cibernéticas (CERT-py), dependiente de la Secretaría Nacional de Información y Tecnologías de la Comunicación (SENATIC), es la principal autoridad designada en materia de seguridad cibernética en Paraguay, y la Unidad Especializada en Delitos Cibernéticos, en el ámbito de la Fiscalía Nacional, es la principal autoridad a cargo de la investigación y la acción judicial en caso de delitos cibernéticos.

El CERT-py se conformó a fines de 2012 con el objetivo de facilitar y coordinar la protección de los sistemas cibernéticos y de la información que respaldan la infraestructura nacional y gubernamental, y garantizar una respuesta eficaz y oportuna a los incidentes cibernéticos. En la actualidad, su

capacidad operativa se limita a un ofrecimiento de orientación y soporte en tiempo real para el desdoble de incidentes, aunque ello le permite comprender y revisar las políticas internas de las organizaciones a las que asiste. En función de la experiencia acumulada, CERT-py está diseñando políticas, procedimientos y mecanismos para responder a incidentes cibernéticos y tiene como objetivo continuar posicionándose como recurso y referencia nacional para orientación proactiva y reactiva.

En la actualidad las autoridades gubernamentales trabajan en el desarrollo de un Plan de Seguridad Cibernética Nacional que se abocará a una amplia gama de prioridades relativas a la seguridad cibernética y la lucha contra la ciberdelincuencia.

La capacitación y la construcción de capacidades del personal de CERT-py y la Unidad Especializada en Delitos Cibernéticos ha sido una de las principales prioridades, y se ha contado con la ayuda de numerosos socios, incluida la OEA, el Departamento de Estado de los Estados Unidos (DS/ATA), y otras autoridades nacionales competentes de la región. La capacitación adicional brindada al personal gubernamental y representantes de otros sectores de la sociedad se dirige a impedir los ciberdelitos e incidentes cibernéticos mediante la concientización de los riesgos y las buenas prácticas. En esta misma línea, el gobierno ha lanzado una campaña denominada "Conéctate Seguro PY [Paraguay]", cuyo principal objetivo es concientizar al público acerca de los peligros de publicar información personal sensible en los sitios de redes sociales. En 2013, SENATIC adoptó una iniciativa complementaria, PARA.PIENSA.CONÉCTATE, que se encuentra en su fase de implementación.

En la actualidad el gobierno trabaja con las principales instituciones del sector privado para desarrollar pautas comunes en materia de seguridad de la información, incluidos esfuerzos conjuntos de información y cooperación. A la fecha, la Fiscalía General es la única autoridad gubernamental capaz de solicitar información a los prestadores de servicio internacionales (Facebook, Google, Twitter, etc.) cuando dicha información sea necesaria para una investigación. Sin embargo, el Código Penal de Paraguay (Ley Nº 1286/98) establece que cualquier persona que tenga conocimiento relativo a un acto punible por parte del Estado deberá compartir dicha información con el Ministerio Público o con la Policía Nacional.

Como se mencionó anteriormente, las autoridades responsables del Gobierno de Paraguay recibieron capacitación de diversos socios de la región. La cooperación fue tomando la forma de trabajo con las autoridades equivalentes de otros países para responder a incidentes cibernéticos y, cuando sea necesario, desactivar sitios que hayan participado en la exposición de los datos vulnerables. Al respecto, El CERT-py ha tomado medidas para desarrollar sus lazos cooperativos con otros CSIRT nacionales de la región, por lo que, según aseguró, pudo mantenerse más informado acerca de la evolución de las técnicas y amenazas cibernéticas.

Las autoridades gubernamentales comunicaron que ciertas universidades de Paraguay están comenzando a ofrecer módulos y cursos especializados en seguridad cibernética; sin embargo, no existe información adicional disponible.

En cuanto a las últimas tendencias, las autoridades nacionales han observado una reducción de los ataques por parte de grupos activistas, y un incremento en ataques de denegación de servicios (DoS y DDoS), incluidos incidentes dirigidos a los portales de Internet del Ministerio de Finanzas, la Presidencia y Vicepresidencia de la República. El *hackeo* comprende la mayor cantidad de incidentes cibernéticos, incluida la denuncia de un acto que aún se encuentra bajo investigación, y en el que el autor modificó datos en un dominio mediante la violación del usuario y contraseña del registro de dominio del sistema de administración. La mayor cantidad de ciberdelitos estuvieron relacionados con prácticas fraudulentas mediante el empleo de tarjetas de crédito falsas y la explotación de otros mecanismos de pago electrónico, así como pornografía infantil. Sin embargo, todas estas observaciones son anecdóticas y no concluyentes, dado que las autoridades solo cuentan con acceso limitado a los datos de proveedores de servicios de internet (ISP), bancos y otras instituciones financieras.

Un caso exitoso al que hacen referencia las autoridades implicó la rápida respuesta ante un ataque DoS contra un sitio de Internet gubernamental, en el que el CERT-py detectó el incidente, adoptó inmediatamente medidas correctivas, y alertó a otros CSIRT nacionales de la región para que pudieran implementar las medidas necesarias para impedir que dicho ataque se produjera también contra sus

propios bienes. En otro caso, se encontró a cuatro ciudadanos búlgaros utilizando tarjetas de crédito clonadas en negocios y cajeros automáticos. Se identificó a estas personas como miembros de una organización criminal internacional más amplia, y se los juzgó y condenó por sus delitos. Uno de ellos fue extraditado a Estados Unidos por delitos similares cometidos allí.

De acuerdo con las autoridades denunciantes, los sectores más afectados fueron organismos gubernamentales (especialmente aquellos con funciones relacionadas con la seguridad), instituciones financieras y bancarias. La Unidad Especializada en Delitos Cibernéticos informó que se procesaron 12 casos el año pasado, y se detuvo a 25 personas por actividades ilícitas.

Las autoridades citan una serie de impedimentos para la mejora de la seguridad cibernética y la reducción de la delincuencia cibernética en Paraguay. Estas limitantes incluyen la falta de conciencia entre los usuarios individuales y públicos acerca de las amenazas cibernéticas y las buenas prácticas para su mitigación, así como una falta de interés y conciencia general por parte de las empresas e instituciones del sector público. Este último punto se corresponde con una deficiencia en las inversiones para la mejora de la seguridad cibernética, especialmente en inversiones para infraestructura, equipos y herramientas. Las autoridades a cargo de la investigación y acciones judiciales por ciberdelitos mencionan la necesidad de una capacitación más especializada respecto de las amenazas, técnicas para combatirlas y el uso adecuado de las herramientas disponibles.

Perú

★ Lima

Población: **30,476,000**
Cobertura de Internet: **38.2%**
Suscriptores de banda ancha fija: **4.7%**

En Perú, dos organismos asumen la responsabilidad principal en las iniciativas vinculadas con la seguridad y delitos cibernéticos. El PeCERT, el equipo de respuesta a incidentes de seguridad cibernéticos (CSIRT) peruano, se fundó en 2009 y es la principal entidad responsable de los asuntos relacionados con la seguridad cibernética en Perú, incluidas la prevención y gestión de incidentes. La investigación de los delitos cibernéticos y las responsabilidades correspondientes le competen fundamentalmente a la División de Investigación de Alta Tecnología (DIVINDAT), comprendida en la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú (PNP).

Si bien el PeCERT es un CSIRT operativo con responsabilidades a nivel nacional, en la actualidad se encuentra abocado a la tarea de revisar y actualizar sus mecanismos, procedimientos y políticas en materia de respuesta ante incidentes.

Perú no posee una estrategia o política nacional oficial de seguridad cibernética, pero actualmente trabaja en su elaboración.

Tanto la DIVINDAT como el PeCERT capacitan intensamente a su personal con el fin de que desarrolle y mantenga la capacidad requerida para desempeñar sus funciones básicas. La DIVINDAT, por ejemplo, informa que lleva a cabo regularmente talleres orientados a actualizar los conocimientos y las habilidades de su personal en lo que respecta al uso eficiente de herramientas de análisis forense digital. Si bien se informó que en Perú existen instituciones académicas que ofrecen programas de

grado con especializaciones en seguridad cibernética y delito cibernético, no se brindó información acerca de si los funcionarios gubernamentales accedían a esas oportunidades de formación.

En lo que atañe al aspecto legislativo, la reciente aprobación de tres leyes –la Ley que Incorpora los Delitos Cibernéticos al Código Penal (Ley 27309), la Ley de Protección de Datos Personales (Ley 29733) y la Ley de Delitos Cibernéticos (Ley 30096)– ha fortalecido el marco jurídico con que cuenta el país para promover la seguridad cibernética y combatir el delito cibernético. Se encuentran en estudio otras modificaciones de leyes en vigor.

Las entidades del sector privado no tienen obligación de denunciar incidentes cibernéticos ante las autoridades nacionales competentes. No obstante, el PeCERT ha iniciado conversaciones orientadas a aumentar la colaboración con el sector privado, en particular con ISP (proveedores de servicios de Internet) y bancos. Esta iniciativa obedece, en parte, al reconocimiento de que las empresas privadas suelen contar con mayor capacidad para detectar tráfico inusual y ataques, así como con sistemas de gestión de la seguridad más consolidados, y serían, por ese motivo, socios de inmenso valor en la labor de asegurar la infraestructura nacional.

La colaboración y el intercambio de información con autoridades nacionales competentes de otros países ha sido algo limitada; este es un aspecto que se mencionó como una de las áreas en las que deberán implementarse nuevas medidas en el futuro.

Tanto el PeCERT como la DIVINDAT indicaron que se encuentran activamente abocados a mejorar la seguridad de la población a la que atienden, así como a incrementar su capacidad de recuperación y resiliencia. Esas iniciativas consisten en una combinación de medidas preventivas y reactivas.

En lo correspondiente a la prevención, se asignó prioridad fundamental a las campañas educativas y de concientización internas y externas. Las campañas de concientización internas conducidas dentro de las propias instituciones incluyeron una variedad de actividades orientadas a lograr que los usuarios comprendan conceptos que no siempre se asocian con la seguridad cibernética pero que son clave para que exista, como por ejemplo la seguridad física, seguridad lógica y la seguridad humana. Respecto de las actividades de concientización externas, se llevaron a cabo campañas en los medios de comunicación, y se efectuaron actividades de difusión de información y educación en entidades del sector privado como bancos, servicios de procesamiento de pagos y otras entidades empresariales y comerciales. También se dirigieron campañas de concientización a la ciudadanía en general en las que se enfatizaba la adopción de buenas prácticas básicas para reducir la vulnerabilidad y proteger la propia identidad y los datos personales al usar Internet y las TIC (tecnologías de la Información y la Comunicación).

La DIVINDAT solicita la ayuda de entidades extranjeras toda vez que es apropiado. Asimismo, mantiene relaciones activas de cooperación con ONG nacionales e internacionales dedicadas a la lucha contra los delitos cibernéticos y otros actos ilícitos que involucren el uso de TIC (trata de personas, prostitución, pornografía, tráfico de órganos, etc.) y apoya sus iniciativas.

El PeCERT y la DIVINDAT señalaron la existencia de diversos impedimentos que deberán superarse con el fin de mejorar la posición del país en materia de seguridad cibernética y mejorar su capacidad para combatir el delito cibernético. Los obstáculos relativos al acceso a la información recibieron particular atención, entre ellos la dificultad de obtener datos de los ISP u otros proveedores de servicios de manera oportuna. También se indicaron como impedimentos clave la insuficiencia de recursos y la falta de voluntad de compartir información y cooperar por parte de otras instituciones gubernamentales y privadas.

Los datos oficiales muestran que en 2013 se registró un incremento de alrededor de 30% en la cantidad de incidentes cibernéticos denunciados ante autoridades nacionales e identifican al sector empresarial, el académico, el de las telecomunicaciones y el policial como los sectores más afectados de la población, entre otras instituciones del sector público.

En 2013, se denunció una amplia variedad de delitos ante las autoridades; los más comunes fueron: clonación de tarjetas de crédito, suplantación de identidad, amenazas por correo electrónico, intrusión mediante *hackeo* o *crackeo*, acceso no autorizado a bases de datos, extorsión por Internet, chantaje sexual, operaciones financieras fraudulentas, pornografía infantil y piratería de *software*. Las técnicas empleadas para perpetrar esas actividades fueron tan variadas como los actos delictivos e incluyeron:

intrusiones en puntos de venta (PoS), ingeniería social, *pharming* (estafa a través de ingeniería social y sitios fraudulentos), *phishing* (suplantación de identidad) y *malware* (programas maliciosos).

La DIVINDAT informó que en 2013 se registraron varios incidentes de impacto relativamente alto, a los cuales lograron responder con eficacia: la división identificó, localizó y aprehendió a los culpables y los entregó a las autoridades judiciales competentes. En un caso, el presidente de una institución estatal recibía mensajes de correo electrónico amenazantes y difamatorios. Mediante la aplicación de técnicas forenses, el personal de la DIVINDAT logró determinar el origen de los mensajes de correo electrónico e identificar el remitente; a continuación, notificó a sus colegas de la Policía Nacional con el fin de iniciar el procesamiento penal del infractor. El PeCERT, en otro caso, respondió con éxito a un ataque (vandalismo) contra el portal *web* de la Presidencia de la Nación: obtuvo acceso a la información pertinente, la analizó y adoptó las medidas necesarias para restaurar su integridad.

San Cristóbal y Nieves

★ Basseterre

Población: **55,000**

Cobertura de Internet: **79.4%**

Suscriptores de banda ancha fija: **27.3%**

La Unidad de Delitos Cibernéticos de la Fuerza Policial Real de San Cristóbal y Nieves es el principal organismo con competencia en asuntos relacionados con la seguridad cibernética en San Cristóbal y Nieves, si bien cuando es necesario recibe apoyo del personal técnico del Ministerio de Tecnología y otros ministerios, según se requiera. No existe un CIRT nacional ni otro equipo similar; tampoco se ha elaborado una política o estrategia oficial en materia de seguridad cibernética a nivel nacional. No obstante, se han emprendido iniciativas de concientización, en particular una reunión nacional convocada por el Ministerio de Tecnología, en la que se encontraron representantes del sector público y privado para intercambiar opiniones sobre cuál es la mejor manera de que el país pueda avanzar en lo relativo a seguridad cibernética. Además, numerosos funcionarios gubernamentales pertenecientes a diversos organismos con funciones legales, policiales y vinculadas con la tecnología participaron en talleres de capacitación técnica y formulación de políticas organizados por la OEA.

No se encuentra en vigor ninguna ley, acuerdo o protocolo que rija la denuncia de ataques cibernéticos por parte del sector privado; las autoridades gubernamentales refieren que es difícil evaluar la respuesta del sector privado ante incidentes de esa índole porque no han recibido denuncias de ataques perpetrados contra instituciones privadas. De hecho, las autoridades nacionales informan que no se han observado incrementos del número de incidentes cibernéticos de ningún tipo en 2013, tampoco ningún incidente particular notable por su naturaleza o sus consecuencias.

En lo referente a cooperación internacional, el Gobierno de San Cristóbal y Nieves no ha firmado ningún memorando oficial de entendimiento sobre seguridad cibernética con otros gobiernos. No obstante, cuando recibe solicitudes de intervención en relación con amenazas a la seguridad cibernética conocidas o sospechadas, cuenta con los mecanismos y la capacidad requerida para responder a tales amenazas y proporcionar apoyo. Además, en los organismos gubernamentales trabajan profesionales de la seguridad cibernética competentes que mantienen comunicación informal, aunque diaria, con sus pares de otros países de la región.

Para el futuro, el Gobierno de San Cristóbal y Nieves identifica varios desafíos que deberán superarse para mejorar la posición nacional en materia de seguridad cibernética. Entre ellos, se destacan la necesidad de crear un CIRT nacional, así como el marco jurídico necesario para investigar y enjuiciar delitos cibernéticos. Las autoridades afirman que el país se ha visto beneficiado con la participación de algunos funcionarios en diversos cursos y talleres de capacitación realizados en los últimos años, y que ha adoptado algunas medidas para reducir el riesgo que conllevan los incidentes cibernéticos para la infraestructura crítica nacional. No obstante, el hecho de que no exista un CIRT nacional ni un marco legal, así como la falta de conciencia acerca del problema y de cooperación entre entidades clave del sector público y privado implican que el riesgo se mantiene elevado. Si bien en la actualidad el gobierno cuenta con capacidad para responder con eficacia a incidentes de escala pequeña a media, las autoridades no consideran que el gobierno esté preparado para hacer frente a un ataque de gran escala.

San Vicente y las Granadinas

★ Kingstown

Población: **97,000**

Cobertura de Internet: **47.5%**

Suscriptores de banda ancha fija: **12.5%**

El organismo principal en materia de seguridad cibernética de San Vicente y las Granadinas es la Fuerza Policial de San Vicente y las Granadinas, que ha creado la Unidad de Tecnología de la Información para supervisar y apoyar la investigación de todos los delitos cibernéticos y asuntos vinculados con la seguridad de la información. Si bien la oficina del Primer Ministro también ha desempeñado un papel de guía y facilitación en el análisis de la política de seguridad cibernética, no se encuentra en vigor una estrategia o plan nacional establecido en materia de seguridad cibernética; San Vicente y las Granadinas tampoco ha creado un CSIRT nacional. No obstante, las autoridades nacionales informaron que se encuentra en desarrollo un organismo nacional que se encargará de la gestión de incidentes. No se ha implementado una campaña nacional de concientización sobre seguridad cibernética, y las autoridades refirieron que en la actualidad no se están realizando acciones tendientes a desarrollar ese tipo de iniciativa.

Las autoridades de la Fuerza Policial de San Vicente y las Granadinas informaron que el aumento observado más notable en incidentes cibernéticos se relacionó con el uso de redes sociales en instituciones educativas, pues como resultado de la iniciativa "Una *notebook* por niño" implementada por el gobierno, se incrementó la posibilidad de acceso de los alumnos a computadoras e Internet. No obstante, el incremento de la incidencia de esa clase de incidentes, que involucran en su mayoría difamación y amenazas a través de redes sociales como Facebook, no dio origen a medidas específicas por parte del Estado hasta el momento.

En los casos en que se denunciaron actos que involucraban difamación o amenazas, las autoridades identificaron las direcciones IP de origen, que luego se informaron a los ISP. No queda claro si se implementó alguna acción, y en ese caso cuál, en respuesta a esas situaciones.

Las autoridades señalaron que, en efecto, la Fuerza Policial de San Vicente y las Granadinas coopera y comparte información con empresas del sector privado, aunque no se brindó información específica acerca de la forma o frecuencia de esas interacciones ni si existe alguna base legal para ellas.

La cooperación internacional consistió, en gran medida, en la solicitud de apoyo a los especialistas del Laboratorio de Cibernética Forense de Antigua y Barbuda cuando fue necesario. Asimismo, integrantes del personal de la Unidad de Tecnología del gobierno han participado en sesiones de capacitación sobre seguridad cibernética y delito cibernético ofrecidas por socios regionales e internacionales, entre ellos la OEA, el Departamento de Estado de Estados Unidos (DS/ATA), la UAT e INTERPOL, entre otros. En San Vicente y las Granadinas no existen carreras de grado ni programas que ofrezcan certificaciones sobre seguridad cibernética a nivel universitario aunque, al igual que en el caso de otros países del Caribe, es frecuente que los estudiantes interesados en ese campo cursen estudios en otras universidades de la región, o en Estados Unidos o Europa.

Las autoridades mencionaron los vínculos que se establecieron recientemente entre diversos países del Caribe para el Sistema Automático de Identificación de Huellas Dactilares (AFIS) como un ejemplo de los avances logrados en el país en materia de seguridad cibernética durante 2013.

Surinam

★ Paramaribo

Población: **539,000**

Cobertura de Internet: **34.7%**

Suscriptores de banda ancha fija: **5.5%**

El Gobierno de Surinam se encuentra en la actualidad abocado a revigorizar y ampliar su sistema nacional de seguridad cibernética, para lo cual está adoptando medidas en varios frentes. El Organismo Central de Inteligencia y Seguridad (CIVD) es responsable en forma interina de los asuntos vinculados con la seguridad cibernética, pero está en marcha la creación de una Unidad de Delitos Cibernéticos en el ámbito de la Policía Nacional. Además, el equipo de respuesta a incidentes de seguridad cibernéticos (CSIRT) de Surinam, que había dejado de existir, está en proceso de reactivación, y pronto contará con un nuevo sitio *web*. Se están llevando a cabo negociaciones entre las partes interesadas con el fin de elaborar una política y una estrategia nacional de seguridad cibernética; asimismo, personal de la fuerza de defensa nacional está asistiendo a un curso sobre seguridad cibernética.

No se exige a las entidades del sector privado que denuncien los incidentes cibernéticos que las afectan ante las autoridades gubernamentales; no obstante, el CIVD está en proceso de negociación con instituciones financieras de primera línea y otros actores clave respecto del mejor modo de compartir información y mantener relaciones de cooperación. La cooperación entre el CIVD u otras autoridades nacionales y sus pares en otros países no ha sido significativa.

Sin embargo, las autoridades nacionales señalaron que la participación de funcionarios gubernamentales surinameses en actividades de desarrollo de capacidades relativas a la seguridad cibernética organizadas por la OEA, entre ellas el Ejercicio de Gestión de Crisis llevado a cabo en Washington, DC en junio de 2013, y el Simposio de Seguridad Cibernética realizado en Uruguay en noviembre de 2013, resultaron decisivos para la reactivación del SurCSIRT. En lo que respecta a recursos para el desarrollo de la capacidad disponibles en el país, desde mayo de 2014 la Universidad de Surinam ofrecerá un curso sobre seguridad cibernética, aunque no se sabe con certeza si habrá funcionarios gubernamentales que aprovechen esta oportunidad de formación.

El Gobierno de Surinam no cuenta con un sistema o mecanismo centralizado para la denuncia de delitos cibernéticos o incidentes vinculados con la seguridad, de modo que no existe un registro oficial de incidentes ni se dispone de los datos correspondientes. Las autoridades afirman que, en general, los delitos cibernéticos no son particularmente frecuentes en Surinam, si bien señalan que han observado en el último año un incremento de los incidentes que involucran *skimming* (clonación de tarjetas) y fraudes bancarios. Puesto que no existen registros oficiales y las denuncias provenientes del sector privado son mínimas, no es posible saber si hay casos en los que el incidente se haya resuelto con éxito.

Con miras al futuro, las autoridades identificaron varios obstáculos clave que deberán resolverse con el fin de promover la seguridad cibernética en Surinam. Entre ellos se cuenta la actual falta de confianza entre los actores, que inhibe el intercambio de datos sensibles, la falta relacionada de colaboración entre ellos, el financiamiento insuficiente para la implementación de iniciativas vinculadas con la seguridad y el delito cibernético, la falta de personal capacitado en forma adecuada y la ausencia de un marco legislativo nacional para dar sustento al desarrollo y operación eficaz del CIRT del país, el SurCSIRT.

Trinidad y Tobago

★ Puerto España

Población: **1,344,000**
Cobertura de Internet: **59.5%**
Suscriptores de banda ancha fija: **13.8%**

Actualmente, en Trinidad y Tobago los organismos nacionales que encabezan las acciones relativas a la seguridad cibernética y los delitos cibernéticos son dos: el Ministerio de Seguridad Nacional y la Unidad contra Delitos Cibernéticos de la Policía de Trinidad y Tobago. En general, las organizaciones han manejado su seguridad cibernética de manera independiente, de modo que en cada organización hay un encargado de seguridad en la red, que es responsable por el sistema y la seguridad de la información de la organización. Para crear conciencia sobre la seguridad cibernética se adoptaron algunas medidas, la mayoría en la forma de talleres de sensibilización que organizó el Ministerio de Seguridad Nacional, la Policía y el Ministerio de Ciencia y Tecnología.

Para Trinidad y Tobago, el 2013 fue un año activo en la lucha por la seguridad cibernética y marcó un punto de inflexión en la regulación nacional de seguridad cibernética en el país. En 2011, se creó una Comisión Interministerial (IMC) de seguridad cibernética, bajo la dirección del Ministerio de Seguridad Nacional, que está integrada por representantes de algunos ministerios y reparticiones clave, y también por el sector privado. La IMC se constituyó con mandato por dos años para alcanzar los siguientes objetivos: desarrollo de una estrategia y un plan de acción para la seguridad cibernética, actualización del marco normativo del país, creación de un CSIRT nacional, desarrollo e implementación de un régimen regulatorio y creación de un esquema y un mecanismo de evaluación de los riesgos cibernéticos que pueden afectar la infraestructura de la nación. Mediante un trabajo interno consistente en un proceso de interacción de distintos organismos a través de sub-comités que contaron con el apoyo de organismos internacionales para los aspectos técnicos y de desarrollo de capacidades, al cabo de dos años de trabajo la IMC hizo avances significativos en la consecución de sus objetivos.

En diciembre de 2012, el Gobierno aprobó una Estrategia Nacional de Seguridad cibernética, destinada a servir de guía para todas las acciones e iniciativas referentes a la seguridad cibernética en Trinidad y Tobago. La estrategia se basa sobre el Marco de Políticas a Mediano Plazo del Gobierno

2011-2014, en el que se destaca el rol de las tecnologías de la información y la comunicación (TIC) para impulsar el desarrollo nacional. La estrategia se apoya en los cinco pilares de gobernabilidad, gestión de incidentes, colaboración, cultura y legislación y, hasta el momento, resultó útil para orientar las acciones que se están llevando a cabo en relación con la seguridad cibernética.

Actualmente, existe un proyecto de ley de delitos cibernéticos sometido a tratamiento por el Congreso. En términos generales, el proyecto busca: penalizar como conductas ilícitas los delitos informáticos y los delitos cibernéticos, institucionalizar mecanismos de investigación, permitir el uso de evidencia electrónica en los procesos penales y definir las obligaciones y limitaciones de la responsabilidad de los ISP. Asimismo, se espera que en los próximos meses se lleve adelante una capacitación de las fuerzas de seguridad, los fiscales y los funcionarios judiciales, con el propósito de desarrollar las capacidades necesarias para aplicar la nueva legislación.

En breve está prevista la creación de una Agencia de Seguridad cibernética de Trinidad y Tobago (TTCSA), bajo la órbita del Ministerio de Seguridad Nacional, que actuará como responsable principal por la coordinación y gestión de las acciones sobre seguridad cibernética. Sus obligaciones específicas incluyen: implementar y brindar asesoramiento sobre la estrategia nacional de seguridad cibernética; proporcionar información sobre la conciencia que existe respecto del entorno, y recabar y analizar datos relacionados con la seguridad cibernética; promover una gestión eficaz de la seguridad cibernética y en la red; concientizar y promover la cooperación en el plano local e internacional.

En este momento, el Gobierno también está trabajando en la creación de un CSIRT (TT-CSIRT), bajo la órbita del Ministerio de Seguridad Nacional, que estará encargado de: alertar sobre potenciales amenazas, incidentes o ataques; facilitar el intercambio de información y la coordinación dentro del área de influencia del TT-CSIRT; analizar metodologías relacionadas con vulnerabilidad cibernética, incidentes cibernéticos y ataques cibernéticos; prestar asistencia técnica al gobierno u otras partes interesadas; llevar adelante investigaciones y análisis forenses; asumir la defensa frente a ataques a la infraestructura de la información; y liderar acciones de recuperación en el plano nacional en caso de un ciberincidente.

El cuarto pilar ("cultura") de la estrategia nacional aborda la necesidad de concientizar al público mediante un enfoque multidisciplinario, con la participación de todas las partes interesadas. Esto incluye incorporar la seguridad cibernética a aspectos más amplios de la formulación de políticas y educar a todos los usuarios de las TIC y de Internet acerca de sus respectivos roles en el ciberespacio. El Ministerio de Seguridad Nacional está próximo a lanzar una campaña de concientización destinada a la población en general, en la que utilizarán cortometrajes sobre los distintos tipos de delitos cibernéticos y artículos periodísticos y anuncios de servicios públicos que ofrecen información básica sobre seguridad cibernética. El Ministerio también está trabajando con ONG locales para crear un sitio *web* con información sobre seguridad cibernética.

Si bien en la actualidad el sector privado no tiene obligación de reportar incidentes ante ninguna autoridad gubernamental, las autoridades continúan trabajando, en estrecha vinculación con empresas privadas, en especial del sector bancario, en diversos temas de seguridad cibernética. Esto incluye la redacción de un borrador de la Política Nacional sobre Delitos Cibernéticos aprobada en febrero de 2013, e iniciativas conjuntas que se están llevando a cabo a fin de definir aspectos que, en el futuro, podrían entrañar alianzas y colaboración.

Hoy en día la cooperación con otros países se funda en relaciones de trabajo informales, con la única excepción de la Unidad de la Autoridad Central del Ministerio de Justicia, que tiene a su cargo la asistencia legal mutua. No obstante, la creación del TTCSA permitirá establecer con otras naciones relaciones bilaterales formales para temas de seguridad cibernética. Por otra parte, existen ya relaciones de trabajo excelentes con organizaciones internacionales, tales como la Organización de Estados Americanos, la Unión Internacional de Telecomunicaciones y la Secretaría del Commonwealth.

Actualmente, si bien existen algunas instituciones académicas en donde se ofrecen cursos de *hackeo* legítimo, no hay en el país estudios de grado ni programas de acreditación sobre seguridad cibernética. No obstante, el gobierno tiene intención de asociarse con terceros a fin de desarrollar estos programas.

Aunque la sanción de la ley de delitos cibernéticos, actualmente en tratamiento en el Congreso, entrañará una solución, las autoridades nacionales señalaron que la ausencia de legislación sobre delitos cibernéticos, así como la lenta concientización sobre delito cibernético y seguridad cibernética, hasta ahora fueron los mayores obstáculos para la seguridad cibernética del país. También fue un impedimento importante para el desarrollo de la seguridad cibernética nacional la carencia de recursos financieros y humanos para implementar la estrategia nacional con eficacia.

En cuanto a las tendencias observadas para 2013, como los incidentes cibernéticos rara vez son denunciados ante las autoridades nacionales se torna difícil para el Gobierno aseverar con certeza un aumento o disminución de la actividad ilícita. En 2013, la policía investigó 85 casos vinculados al delito cibernético, aunque ninguno terminó en condena. Otras informaciones, fundadas en relatos no comprobados, indican que la mayoría de los incidentes reportados se relacionan con la suplantación de identidad en Facebook u otras redes sociales, o la explotación de cuentas de correo electrónico con fines de suplantación de identidad o fraude. Un caso que fue objeto de especial atención y que todavía está siendo investigado, se originó en el uso indebido de las cuentas de correo electrónico de varios oficiales de alto rango. Algunos reportes incompletos parecen indicar que, de todos los sectores clave de la sociedad, el sector bancario del país fue el más afectado.

Uruguay

★ Montevideo

Población: **3,297,000**
Cobertura de Internet: **55.1%**
Suscriptores de banda ancha fija: **16.6%**

La autoridad principal en materia de seguridad cibernética del Gobierno de Uruguay, es la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), bajo cuyo eje opera también el Centro de Respuesta a Incidentes de Seguridad Cibernética del Uruguay, CERTuy. La Unidad de Delitos Cibernéticos de la Policía Nacional tiene responsabilidad primaria por la investigación de delitos cibernéticos y acciones similares, y recibe asistencia técnica del CERTuy cada vez que la necesita.

Aunque Uruguay no cuenta con un documento específico sobre políticas o estrategias de seguridad cibernética, en iniciativas sobre temas afines, como la Agenda Digital del Gobierno, se definen e incorporan lineamientos sobre la materia. Además, mediante la emisión de una serie de decretos oficiales se creó un marco regulatorio claro, aplicable a las iniciativas sobre seguridad cibernética en el plano nacional. El Decreto 452 (2014), por ejemplo, establece que las reparticiones del gobierno central deben tener una política de seguridad cibernética, en tanto en el Decreto 92 (2014) se subraya la necesidad de que los organismos nacionales de servicios públicos se homologuen bajo un criterio común para la clasificación de sitios web (v. gr. ".gun.uy" y ".mil.uy), así como de poseer estándares de seguridad altos para el centro de datos, correos electrónicos y nombres de dominio pertenecientes a la administración central.

Personal de la Unidad de Delitos Cibernéticos de la Policía Nacional recibió capacitación técnica de socios externos, incluso de la OEA, fundamentalmente centrada en el perfeccionamiento de sus capacidades de investigación y análisis forense. El personal del CERTuy asistió a múltiples talleres y seminarios técnicos y de diseño de políticas, tanto como participantes como en calidad de capacitadores expertos.

Las entidades del sector privado no están legalmente obligadas a reportar información sobre ataques cibernéticos, o información comprometida ante las autoridades nacionales. Las instituciones y los organismos públicos, en cambio, sí tienen la obligación de reportar ante el CERTuy. Cuando un incidente de potencial alto impacto afecte, o pueda afectar, la comunidad objetivo o el Estado, el CERTuy, sin importar qué sector se encuentra afectado (público o privado), ejerce un rol activo en la respuesta y mitigación del ataque.

Las autoridades uruguayas, y en particular el personal de la AGESIC y el CERTuy, cooperan estrecha y regularmente con sus pares de otros países, inclusive en la respuesta a incidentes ocurridos tanto en Uruguay como en otros países. Las autoridades informaron que, hasta ahora, estas actividades de cooperación dieron resultados positivos. Asimismo, el CERTuy trabaja asociado a varias organizaciones internacionales para fomentar una mayor colaboración y comunicación entre distintos centros de respuesta, inclusive la OEA, el Comité Interamericano contra el Terrorismo (CICTE), el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), el Foro de los CIRT (FIRST) y la Unión Internacional de Telecomunicaciones (ITU), entre otras.

Las autoridades informaron que tanto universidades públicas, como privadas en Uruguay ofrecen carreras de grado y programas de acreditación de saberes en temas de seguridad cibernética y lucha contra el delito cibernético.

En noviembre de 2013, el CERTuy lanzó la campaña "Seguro te conectas", dirigida al público en general, que busca crear conciencia sobre los problemas que puede generar el uso de las TIC. El CERTuy está intentando asegurar la cooperación de otras organizaciones o socios, a fin de dar una difusión más amplia en el futuro. Además, el centro también adhirió oficialmente la campaña de concientización PARA.PIENSA.CONÉCTATE.

Datos recabados por el CERTuy durante el seguimiento y reporte de incidentes indican que el número de incidentes cibernéticos aumentó considerablemente (aunque el personal del CERTuy apunta que, durante ese período, sus técnicas de seguimiento y recolección de datos siguieron actualizándose). El incidente cuya frecuencia mostró el mayor aumento es el *phishing*.

Las autoridades uruguayas indicaron que la gestión de amenazas y riesgos a la seguridad cibernética es, por su propia naturaleza, un desafío global que está en permanente evolución, puesto que no hay límites geográficos definidos. Tal como sucede desde que el país empezó a hacer frente a los problemas de seguridad cibernética y delito cibernético en 2007, las autoridades uruguayas continuarán haciendo esfuerzos para lograr que la seguridad cibernética sea considerada e integrada en todos los proyectos y las iniciativas en las que haya necesidad y ocasión de hacerlo.

Esto requerirá abordar tres impedimentos básicos que siguen dificultando las acciones relacionadas con la seguridad cibernética y el delito cibernético en el país, esto es, la escasa conciencia sobre la importancia de la seguridad cibernética en otras instituciones públicas, recursos materiales y financieros insuficientes para llevar adelante acciones necesarias, y falta de personal capacitado.

Venezuela

★ Caracas

Población: **29,760,000**
Cobertura de Internet: **44.1%**
Suscriptores de banda ancha fija: **6.7%**

En Venezuela, el principal responsable por la seguridad cibernética, incluida la prevención y respuesta a ataques, es un organismo denominado Sistema Nacional de Gestión de Incidentes Telemáticos (popularmente conocido como VenCERT). La responsabilidad por investigar y enjuiciar el delito cibernético le corresponde al Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), y su División de Delito cibernético, así como al Centro Nacional de Cibernética Forense (CENIF), dependiente de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

Si bien no hay una estrategia o política nacional de seguridad cibernética, sí existe desde hace tiempo un marco legislativo que regula las acciones del Gobierno en el ámbito informático. Éste se compone de tres leyes específicas, que son: la Ley N° 1,204 sobre Mensajes de Datos y Firmas Electrónicas (2001), la Ley Especial contra los Delitos Cibernéticos (2001) y la Ley de Interoperabilidad (2012). La última ley sancionada, la Ley de Infogobierno (2013), amplía el marco normativo para abarcar también acciones de gobierno correspondientes a seguridad cibernética. Su objetivo central es establecer principios, normas y lineamientos que regulen el uso de las TIC en el ámbito público, y consagrar el valor legal de la firma electrónica, los mensajes de datos y cualquier información en formato electrónico. Asimismo, sienta las bases y los principios que rigen el acceso e intercambio electrónico de datos, información y documentos entre organismos estatales, con el propósito de asegurar la adhesión a un estándar de interoperabilidad común. Ante todo, las autoridades esperan que la ley favorezca y aumente la transparencia de la gestión pública, facilite el acceso a la información por parte de los ciudadanos, y fomente el desarrollo nacional de modo tal de asegurar la soberanía tecnológica.

Las autoridades nacionales se abocan regularmente al desarrollo de las capacidades del personal encargado de la seguridad cibernética y el delito cibernético mediante, por ejemplo, la participación de personal técnico de diversas instituciones públicas en cursos sobre seguridad de la información, gestión de incidentes, trabajo con redes sociales, análisis forense informático, y *hackeo* legítimo.

Según la legislación vigente, el sector privado no está obligado a reportar incidentes ante las autoridades nacionales; sin embargo, en este momento se está redactando un proyecto de ley de protección de datos que, en un sentido o en otro, legislará sobre la cuestión. Asimismo, se inició un debate con el sector privado y, en especial, con las empresas vinculadas al rubro de ciencia y tecnología, con el objetivo de identificar y desarrollar oportunidades para el fortalecimiento de la seguridad de la información en la sociedad venezolana.

Si bien oficialmente el Gobierno de Venezuela no mantiene relaciones de cooperación con otros países, las autoridades lograron coordinar de manera exitosa y eficaz acciones de respuesta a incidentes específicos con otros CSIRT alrededor del mundo. De modo similar, se creó en el seno del Mercosur un grupo de trabajo con expertos en seguridad cibernética, a fin de aumentar el intercambio de información dentro de la región.

Las acciones de concientización impulsadas por el Gobierno de Venezuela, en general giraron en torno de una campaña llamada “La Seguridad de la Información Comienza por Tí”, que empezó en noviembre de 2009 y que hoy enfatiza en la educación de los empleados de organismos de gobierno y de las comunidades organizadas.

A pesar de que la información sobre oportunidades de educación y capacitación en Venezuela es escasa, se señaló que existen ofertas de cursos y estudios de grado en seguridad cibernética y delito cibernético, que llegan hasta el cuarto nivel de estudios (título de grado, especialización y título de posgrado).

Según información disponible de 2013, se produjo un claro aumento en la frecuencia de una gran variedad de incidentes cibernéticos. Los actos de vandalismo contra sitios *web* aumentaron alrededor de 50%, por ejemplo, mientras que los ataques por Denegación Distribuida de Servicios (DDoS) se incrementaron en 40%. Uno de los incidentes más importantes se originó en el vandalismo de los portales *web* de varias instituciones estatales por parte de grupos de *hacktivistas* nacionales e internacionales. Las autoridades lograron identificar con éxito a los autores mediante el análisis de los registros del historial de los servidores involucrados.

Según las autoridades nacionales, el principal obstáculo para el desarrollo de la seguridad cibernética en Venezuela es el aumento en la frecuencia de ataques cibernéticos en relación con la limitada capacidad operativa de VenCERT. Un incremento insuficiente en la cantidad de empleados dedicados a gestionar un gran número de incidentes cibernéticos redujo la ya limitada cantidad de tiempo que los empleados pueden dedicar a la investigación, el análisis y la prueba de nuevas herramientas y técnicas en el campo de la seguridad de la información. Esto último es importante porque la diversificación de las herramientas utilizadas para los ataques y su disponibilidad en la red exige que las autoridades mantengan actualizadas sus propias capacidades.

APORTACIONES

Como parte de las acciones implementadas para fomentar la participación y colaboración de socios afines de diversas entidades comerciales, gubernamentales, académicas y otras organizaciones no gubernamentales, la **OEA** y **Symantec** solicitamos a las instituciones con las que trabajamos en forma regular su colaboración para este informe. Cada una de esas entidades —Microsoft, LACNIC, ICANN y el APWG—nos proporcionó información sobre su misión o especialidad.

Anti-Phishing Working Group

Dos veces al año, el Anti-Phishing Working Group (APWG) publica su Encuesta Global Sobre *Phishing*, elaborada por Greg Aaron y Rod Rasmussen. Se trata de un informe cuyo objetivo es cuantificar y comprender el problema global del *phishing*. En él se examina la cantidad de ataques de *phishing* observados y en qué dominios de nivel superior (TLD) ocurrieron esos casos de *phishing*, se proporcionan otros parámetros y se explican las últimas técnicas delictivas. El último informe, "Global Phishing Survey: Trends and Domain Name Use in 2H2013" (Encuesta Global Sobre Phishing: Tendencias y Uso de Nombres de Dominio en el Segundo Semestre de 2013), está disponible en: http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf

Ese informe analizó los dominios y los ataques de *phishing* para ver cómo estaban distribuidos entre los dominios de nivel superior (TLD). La mayoría de los ataques de *phishing* en todo el mundo siguen concentrándose en unos pocos espacios de nombres. La mayoría ocurren en nombres de dominio comprometidos, donde el delincuente logró entrar al servidor *web* donde se aloja el dominio.

En 2013 hubo al menos 115,565 ataques exclusivos de *phishing* en todo el mundo. De ese total, 8,865 ocurrieron en nombres de dominio correspondientes a dominios con código de país de América. Estos ataques ocurrieron mayormente en servidores *web* "*hackeados*", lo que indica que son comunes las infracciones de seguridad en los proveedores de hospedaje de la región y de todo el mundo.

Las estadísticas completas se pueden encontrar en el informe, y a continuación se incluyen las estadísticas de los dominios de nivel superior con códigos de país (ccTLD) de las Américas.

- En todo el mundo, la proporción de dominios de *phishing* de cada 10.000 dominios registrados en un TLD (denominado el "valor de dominios cada 10,000") fue, en promedio, de 4.9
- .COM, el TLD más grande y omnipresente del mundo, registró un valor de dominios cada 10,000 de 3.7. .COM contenía el 46 por ciento de los dominios de *phishing* del conjunto de datos, y el 42 por ciento de los dominios a nivel mundial
- Los autores sugieren que los valores de dominios cada 10,000 entre 3.7 y 4.9 ocupan la franja intermedia, y los valores superiores a 4.9 indican los TLD con *phishing* cada vez más predominante

Dominios de nivel superior correspondientes a códigos de países (ccTLD) en América

Fuente: APWG

TLD (dominio de nivel superior)	Ubicación del TLD	Número de ataques tipo *phishing* únicos —2da. mitad de 2013	Nombres de dominio únicos usados para *phishing* —2da. mitad de 2013	Dominios registrados, noviembre de 2013	Puntuación: dominios de *phishing* cada 10,000 dominios —2da. mitad de 2013	Puntuación: ataques cada 10,000 dominios —2da. mitad de 2013	Tiempo de actividad promedio en hh:mm —2da. mitad de 2013	Tiempo de actividad promedio en hh:mm —2da. mitad de 2013	Número total de dominios maliciosos registrados —2da. mitad de 2013	Puntuación de los registros maliciosos/ 10,000 dominios registrados
ag	Antigua y Barbuda	3	3	19,766	1.5	1.5	22:56	25:15	2	
ai	Anguila	7	4	3,800	10.5	18.4	13:05	11:54		
an	Países Bajos	16	2	800	25.0	200.0	36:05	42:03		
ar	Argentina	829	658	2,800,000	2.4	3.0	36:29	8:51	7	0.0
aw	Aruba	0		625						
bm	Bermuda	1	1	8,100	1.2	1.2	25:46	25:46		
bo	Bolivia	12	11	8,500	12.9	14.1	9:42	4:40		
br	Brasil	3,674	3,023	3,322,000	9.1	11.1	33:16	9:43	29	0.1
bs	Bahamas	0		2,400						
bz	Belice	28	20	44,845	4.5	6.2	60:15	9:37	1	
ca	Canadá	671	527	2,195,000	2.4	3.1	54:17	9:51	3	0.0
cl	Chile	1,010	807	443,251	18.2	22.8	38:52	10:40	3	0.1
co	Colombia	406	274	1,576,833	1.7	2.6	15:12	5:35	23	0.1
com	TLD genérico	53,592	42,086	114,076,050	3.7	4.7	35:18	9:19	12,347	1.1
cr	Costa Rica	10	8	15,161	5.3	6.6	41:54	9:03		
cu	Cuba	0		2,351						
dm	Dominica	0		14,000						
do	República Dominicana	18	18				19:30	0:26		
ec	Ecuador	35	31	30,500	10.2	11.5	37:58	9:13		
gd	Granada	11	3	4,400	6.8	25.0	9:20	10:37		
gp	Guadalupe	29	17	1,500	113.3	193.3	34:50	11:30		
gt	Guatemala	11	10	13,256	7.5	8.3	15:11	14:15		
gy	Guyana	13	3				7:14	8:49		
hn	Honduras	2	2				102:34	149:35		
ht	Haití	428	5	2,200	22.7	1.945.5	16:19	11:17		
jm	Jamaica	2	2	6,300	3.2	3.2	0:17	0:17		
kn	San Cristóbal y Nieves	0								
ky	Islas Caimán	3	3				1:00	1:07		
lc	Santa Lucía	15	12	3,950	30.4	38.0	12:19	10:36	1	
ms	Montserrat	23	8	9,500	8.4	24.2	90:16	54:24	1	1.1
mx	México	486	335	687,155	4.9	7.1	24:38	7:02		
ni	Nicaragua	4	4	6,650	6.0	6.0	13:08	6:14		
pa	Panamá	4	4				11:32	13:36		
pe	Perú	112	100	75,116	13.3	14.9	44:52	8:17		
py	Paraguay	37	33	15,000	22.0	24.7	79:46	8:02	1	0.7
tc	Islas Turcas y Caicos	8	7				5:36	4:08	1	
tt	Trinidad y Tobago	0		2,500						
us	Estados Unidos	420	338	1,795,000	1.9	2.3	33:27	8:25	46	0.3
uy	Uruguay	50	42	68,381	6.1	7.3	51:11	11:50		
vc	San Vicente y las Granadinas	281	8	9,051	8.8	310.5	19:57	10:59	1	1.1
ve	Venezuela (estimado)	196	150	215,000	7.0	9.1	37:58	11:54		
vg	Islas Vírgenes Británicas	1	1	8,600	1.2	1.2				
vi	Islas Vírgenes	0		17,500						

Los 10 principales TLD utilizados para *phishing* por puntuación de dominio —2da. mitad de 2013*

Fuente: APWG

	TLD	Ubicación del TLD	Número de ataques de *phishing* únicos —2da. mitad de 2013	Nombres de dominio únicos usados para *phishing* —2da. mitad de 2013	Dominios registrados, noviembre de 2013	Puntuación: Dominios de *phishing* cada 10,000
1	.np	Nepal	105	88	32,500	27.1
2	.pw	Palau	1,007	924	350,000	26.4
3	.th	Tailandia	215	155	64,990	23.8
4	.cl	Chile	1,010	807	443,251	18.2
5	.pe	Perú	112	100	75,116	13.3
6	.gr	Grecia	463	407	377,000 (est.)	10.8
7	.id	Indonesia	126	104	101,892	10.2
8	.ec	Ecuador	35	31	30,500	10.2
9	.br	Brasil	3,674	3,023	3,322,000	9.1
10	.ma	Marruecos	44	33	43,325	7.6

* Al menos 25 dominios de *phishing* y 30,000 nombres de dominio registrados

Infección de *malware*

En el cuarto trimestre de 2013, PandaLabs, miembro de APWG, realizó un análisis de diversas computadoras en todo el mundo como parte de un proyecto de medición de infecciones de *malware* en curso. PandaLabs descubrió que, en apariencia, 28,39% de las computadoras en todo el mundo estaban infectadas por alguna clase de *malware*. Esta tasa de infección global es una de las más bajas registradas alguna vez por PandaLabs. China presentaba la tasa de infección más elevada —53.85% de todas las computadoras analizadas estaban infectadas. Las regiones de América Latina y Asia presentaron la mayor cantidad de infecciones. Ocho de los 10 países con menor tasa de infección estaban en Europa.

Rango superior	País	Tasa de infección
1	China	53.85%
2	Taiwán	39.57%
3	Turquía	37.50%
4	Polonia	36.65%
5	Perú	35.63%
6	Rusia	34.55%
7	Argentina	34.42%
8	Canadá	34.31%
9	Colombia	33.33%
10	Brasil	32.25%

Rango superior	País	Tasa de infección
45	Suecia	16.18%
44	Reino Unido	18.18%
43	Portugal	18.55%
42	Suiza	19.23%
41	Alemania	20.69%
40	Francia	21.02%
39	Países Bajos	21.07%
38	Venezuela	23.13%
37	Estados Unidos	23.85%
36	España	26.82%

La Corporación de Internet para la
Asignación de Nombres y Números

Seguridad, Estabilidad y Resiliencia de los Sistemas de Identificación de Internet: ICANN, en América

El Equipo de Seguridad, Estabilidad y Resiliencia de ICANN (Equipo SSR), que trabaja en todo el mundo con la comunidad de Internet para buscar cumplir con el objetivo corporativo de preservar y mejorar la estabilidad, confiabilidad y seguridad de los sistemas de identificación de Internet, tal como lo establecen los estatutos de ICANN. El equipo SSR busca cumplir este objetivo al relacionarse y colaborar con los responsables de la seguridad u operación de la infraestructura de Internet, que van desde los registros de nombres de dominios y los de los encargados de los Registros Regionales de Internet (RIR), puntos de intercambio de tráfico de Internet y proveedores de servicios de Internet (ISP), compañías de investigación y seguridad, universidades, voluntarios y organismos policiales.

A fin de cumplir con dichos objetivos, el Equipo SSR participa de actividades que incluyen la concientización respecto a las amenazas y la preparación, medición y análisis de los comportamientos o desempeño del sistema de identificación, así como participación colaborativa que enfatice la coordinación, la generación de capacidades y la transferencia de conocimientos.

Pero ¿qué significa todo esto? A continuación, repasaremos brevemente un caso de éxito que ejemplifica qué representa abordar una amenaza contra un sistema de identificación de Internet, discutiremos sobre la generación de capacidades y nos enfocaremos en lo que todo esto significa para América.

Caso de éxito: el Grupo de Trabajo de Conficker

Un ejemplo excelente de la coordinación y la participación colaborativa exitosa llevada a cabo por el Equipo SSR de ICANN es el rol que desempeñó en la respuesta coordinada que llevó a detener inicialmente el gusano Conficker en 2009, y las tareas continuas de contención realizadas desde entonces. Tal como lo establece el informe "Resumen y repaso de Conficker", tanto el Conficker como la respuesta operativa para contenerlo fueron casos históricos: Los investigadores de la seguridad de Internet y los proveedores de sistemas operativos y *software* de antivirus que descubrieron el gusano a fines de 2008, junto con los organismos policiales y el personal de ICANN, "formaron un grupo de tareas ad hoc con ICANN, registros de dominios de primer nivel y registradores de nombres de dominios de todo el mundo para contener la amenaza; esto lo lograron al evitar que los autores de *malware* utilizaran decenas de miles de nombres de dominio generados en forma algorítmica por la infección Conficker".

El *malware* utilizaba nombres de dominio registrados en más de 100 dominios de primer nivel, incluidos los genéricos y los específicos por país, en lugar de direcciones IP para hacer que su *botnet* sea resistente a la detección y eliminación. La respuesta operativa detuvo el comando de *botnet* y las comunicaciones de control y logró que los autores de *malware* cambiaran su comportamiento, lo que mitigó una amenaza grave contra el Sistema de Nombres de Dominio (DNS).

De más está decir que posteriormente al Grupo de Trabajo de Conficker, el Equipo SSR de ICANN continuó abordando satisfactoriamente distintas amenazas en colaboración con las partes interesadas pertinentes de la comunidad.

Generación de capacidades y transferencia de conocimientos

En muchas regiones del mundo, incluida América Latina y el Caribe, a los organismos policiales les falta personal con niveles altos de conocimientos, pericia y entendimiento sobre el panorama de amenazas en línea. Sí, algunos países han trabajado para crear unidades anti delitos cibernéticos; sin embargo, esas unidades muchas veces se enfocaban en investigaciones de análisis forense digital (cómo encontrar la aguja en el pajar), evidencia digital (descubrimiento, preservación, administración y presentación) y anti piratería de los derechos de autor.

Esto significa que existen regiones del mundo donde las autoridades que deberían llevar a cabo acciones, o coordinarlas, para detener, mitigar, evitar e impedir amenazas en línea, pueden no estar preparadas o no tener el equipamiento necesario. En dichas regiones, los riesgos contra los sistemas de identificación de Internet pueden convertirse en amenazas reales y los delincuentes saben que la impunidad en línea es muy alta, al igual que sus oportunidades de sacar provecho de ella. Los países en América Latina y el Caribe, así como los de la mayoría de las demás regiones, deberían continuar preparándose y equipándose para poder garantizar que no se encuentran en esa situación.

El Equipo SSR de ICANN ofrece continuamente capacitación a los miembros locales y regionales de las comunidades de todo el mundo que, de una forma u otra, tienen una infraestructura de Internet o pueden ayudar a hacerla más segura, estable y resistente. Con el transcurso de los años, los operadores de ccTLD, el personal policíaco, los ISP, y otros actores de todo el mundo han recibido capacitación, desde lo básico a lo más avanzado, sobre las cuestiones relacionadas con la operación de los DNS, el abuso y uso incorrecto de los DNS, y también de DNSSEC e IPv6. Asimismo, a través de su participación en la Iniciativa contra el Cibercrimen, el Equipo SSR de ICANN ofrece estos programas de generación de capacidades a los fiscales y juristas de los estados del Commonwealth que lo solicitan.

ICANN y el Equipo SSR en América

Como parte de nuestros esfuerzos de globalización, en 2013, ICANN abrió una oficina de participación en la Casa de Internet de América Latina y el Caribe en Montevideo. Con personal senior exclusivo de comunicaciones y participación en Montevideo, Brasil, México y Santa Lucía, ICANN ha desarrollado, junto con los miembros de la comunidad, una Estrategia para Latinoamérica y el Caribe que incluye proyectos relacionados con la generación de capacidades y fortalecimiento de la seguridad, estabilidad y resiliencia del DNS en la región.

También, el Equipo SSR de ICANN está presente en toda América y busca activamente fortalecer sus relaciones con organizaciones regionales tales como la Organización de los Estados Americanos, LACNIC, LACTLD, los administradores de ccTLD y los ISPs, los organismos policiales, las oficinas centrales regionales en Buenos Aires de Ameripol e Interpol, y también de compañías de seguridad que tienen su atención puesta sobre el panorama latinoamericano de amenazas en línea.

Según los países involucrados, abordar las amenazas a los sistemas de identificación de Internet en América puede implicar afrontar lo siguiente:

- Diferencias de idioma, lo cual puede dificultarles a los investigadores de la región el uso de muchas herramientas que se podrían utilizar para detectar, detener, mitigar y evitar amenazas
- Diferencias entre el derecho civil y la jurisprudencia de los países, que muchas veces hace que los investigadores de un país puedan hacer suposiciones erróneas sobre asuntos de otro país tan diversos como, por ejemplo, definiciones legales (“delito inducido” es un buen ejemplo), requisitos legales de la cadena de custodia, derechos de privacidad y demás
- No todos los países son miembros de tratados de asistencia judicial recíproca (MLATs) ni participan de redes que permiten que sus organismos policiales compartan información con sus pares internacionales. A pesar de saber que en cuestión de minutos, o segundos, se pueden implementar amenazas importantes, muchas veces un pedido de información enviado por un organismo policial de un país a sus pares en un país vecino puede tardar en ser respondido nueve meses, sin tener la garantía de que se suministrará la información requerida

El Equipo SSR de ICANN está familiarizado con problemas de este tipo y, por lo tanto, se encuentra en una excelente posición para aportar sus conocimientos, pericia y colaboración a las partes interesadas regionales pertinentes. Esto siempre se hace de la manera que ayude a que toda la comunidad pueda abordar las amenazas relacionadas con el DNS.

ICANN está comprometida a fortalecer su participación en América Latina y el Caribe y, por ejemplo, proveer contenido y capacitación en español y, al mismo tiempo, mantener el foco en su mandato de conservar y mejorar la seguridad, estabilidad y resiliencia de los sistemas de identificación de Internet.

Lacnic

RESUMEN EJECUTIVO

El enrutamiento es una de las funciones más importantes en lo que respecta al funcionamiento de Internet. El sistema de enrutamiento está basado en tecnologías que en esencia no se han modificado durante más de 15 años. En el presente informe, se describirán ciertas debilidades que afectan el sistema. Asimismo, se destacará el trabajo que se lleva a cabo para fortalecer la función de enrutamiento, así como la implementación de nuevas técnicas en América. En particular, se describirá el Sistema de Certificación de Recursos (RPKI) y se mostrará su potencial en lo que respecta a mitigar los riesgos asociados con las mencionadas debilidades. El alcance del sistema mundial de enrutamiento es tal que los eventos que tienen lugar en una región pueden ejercer un enorme impacto en otra, lo que pone de relieve la necesidad de cooperación interregional.

Administración de recursos de numeración de Internet

La estructura de registro de Internet se creó con el fin de preservar las direcciones IP, la rutabilidad de Internet y la captura pública de direcciones. Éste se implementa mediante una jerarquía de varios niveles compuesta por las siguientes organizaciones, en orden descendente:

01 **La Autoridad de Números Asignados en Internet (IANA)** administra todos los espacios de números utilizados en Internet, incluidos las direcciones IP y los Números del Sistema Autónomo

02 **Los Registros Regionales de Internet (RIRs)** son organizaciones que operan en grandes áreas geográficas. En la actualidad, existen cinco RIR: ARIN, para Estados Unidos, Canadá y parte del Caribe; RIPE NCC, para Europa, Medio Oriente y parte de Asia Central; APNIC, para la región de Asia-Pacífico; LACNIC, que cubre América Latina y parte del Caribe; y AfriNIC, correspondiente a África. Los RIRs administran el espacio de direcciones IP que les asigna la IANA y establecen políticas y procedimientos que permiten alcanzar un equilibrio adecuado entre las diferentes metas establecidas por la RFC 2050

03 **Los Registros Locales de Internet** atienden áreas coincidentes con territorios nacionales; se establecen bajo la autoridad y el reconocimiento de los RIRs y la IANA. Administran las direcciones IP que les asignan los RIRs, y sus obligaciones son similares a las de los RIRs

Las restricciones establecidas en los documentos que describen el procedimiento de asignación de direcciones IP pueden resultar conflictivas, en particular en lo que atañe a la conservación y la rutabilidad. Si solo la conservación tuviera prioridad sobre otras restricciones, entonces las direcciones IP se asignarían en bloques pequeños a las organizaciones y solo cubrirían necesidades a corto plazo. Sin embargo, como resultado, se produciría un importante incremento de la cantidad de entradas de la tabla de enrutamiento mundial, un efecto secundario no deseado que, a su vez, provocaría un aumento de costo para los proveedores y una disminución de la velocidad de los tiempos de respuesta para la Internet en su totalidad.

Desde que se puso en marcha el sistema de registro de Internet, se ha procurado establecer procesos de desarrollo de políticas que sean abiertos a todos los actores y procedan desde las bases hacia arriba, lo que anota la importancia asignada a la negociación orientada a lograr un equilibrio entre metas conflictivas.

Breve descripción del sistema de enrutamiento mundial

Dado su tamaño y alcance mundial, Internet se ha particionado en dominos administrativos más pequeños. Ese esquema ha sido uno de los factores fundamentales que hizo posible el crecimiento exponencial de Internet durante períodos prolongados e incluso en momentos de depresión o incertidumbre económica. Tales dominios administrativos se llaman Sistemas Autónomos (AS) y se identifican mediante números denominados Números del Sistema Autónomo (ASN). La operación de los AS corresponde a diferentes organizaciones que acuerdan intercambiar información sobre enrutamiento. Esa información es, en esencia, un índice inmenso que contiene los datos requeridos para que los paquetes de Protocolo de Internet recorran Internet y conecten cualquier par de puntos terminales. Durante cada intercambio de información (denominado una "**actualización**") los AS vecinos se informan mutuamente cómo llegar a diferentes porciones de Internet. Cada actualización contiene una lista de redes a las cuales es posible llegar (conocidos como "**prefijos**"), y cada prefijo contiene un conjunto de atributos que ayuda a controlar el modo en que esa información de enrutamiento se propaga y utiliza.

Se dice que los prefijos se **originan** en un sistema autónomo. Este AS de origen es el primer AS que anuncia cierto prefijo a sus vecinos. El AS de origen es un atributo de cada prefijo. Hasta hoy, se da implícitamente por supuesto que la organización que administra el AS de origen de un prefijo tiene **autoridad** sobre el uso del recurso numérico que se anuncia.

Debilidades del sistema de enrutamiento mundial

Se parte del supuesto implícito de que las organizaciones que originan los prefijos de su AS tienen autoridad para hacerlo. Los registros regionales y locales de Internet cuentan con bases de datos acreditadas en las que se vinculan organizaciones y recursos de números; por ende, son la autoridad definitiva en lo relativo a uso de recursos. Se insta a los proveedores de servicios de Internet (ISP) que intercambian información de enrutamiento con otros AS a que comprueben si los prefijos que reciben de sus vecinos provienen de asignatarios legítimos. Lamentablemente, los ISP no siempre implementan esos controles o lo hacen con descuido. Para agravar aún más la situación, no existe un repositorio único de información que los ISP puedan consultar para confirmar el derecho de uso de un recurso.

Si bien existen algunas bases de datos, por ejemplo los diferentes Registros de Enrutamiento de Internet (IRR), donde una organización puede registrar sus recursos y sus políticas de enrutamiento, su uso no es obligatorio, y muchas organizaciones no los utilizan. Los proveedores de servicios suelen implementar sus controles fuera de línea, lo que implica que en caso de ejecutar algún control de autoridad, no se implementa en el equipo de enrutamiento en sí sino en sistemas de información externos a los dispositivos de la red, lo cual resulta en que se produzcan extensas demoras en la aplicación de cualquier decisión de aceptación o rechazo respecto de un anuncio de prefijo.

Estas lagunas dejan el sistema de enrutamiento mundial expuesto a manipulaciones y errores operativos que podrían afectar importantes porciones de Internet. Por ejemplo, un atacante podría anunciar prefijos correspondientes a la red de una organización bancaria o financiera importante a su ISP de subida y, si lograra perpetrar el engaño, parte del tráfico destinado a la organización víctima podría redirigirse a la red del atacante, lo cual en potencia podría exponer datos relativos a transacciones, credenciales de inicio de sesión, correos electrónicos y otros datos confidenciales. Tal ataque también podría generar situaciones generalizadas de denegación de servicio, en las que los usuarios legítimos del servicio no pudieran obtener acceso a los recursos debido a que el tráfico se redirige a otra ubicación. El escenario que se ha descrito es un ejemplo de lo que en la bibliografía se denomina, comúnmente, "secuestro de ruta". Si bien no existen registros de ataques maliciosos de estas características, se han presentado algunos casos de errores operativos en los últimos dos años.

El incidente de INDOSAT, 2014

El 2 de abril de 2014, el proveedor de servicios de Internet de Indonesia INDOSAT reclamó la propiedad de más de 320,000 prefijos, que representan alrededor de 60% de todas las rutas válidas de Internet. Muchas redes de las Américas se vieron afectadas, incluidos los servicios de LACNIC, así como otros operadores de primera línea del hemisferio. Afortunadamente, la visibilidad de estos anuncios espurios fue limitada, y las situaciones de denegación de servicio se vincularon mayormente con operadores cercanos a Indonesia.

Incidentes de secuestro de rutas en América

Existen datos que señalan la existencia de eventos de secuestro de rutas locales en la región, si bien no se han dado a conocer informes oficiales. En 2012, un ISP de Chile anunció por error en Internet, prefijos pertenecientes a un operador de cable de Argentina, lo que provocó una situación moderada de denegación de servicio para el ISP argentino. El mismo año, un sistema autónomo de Argentina anunció una gran cantidad de prefijos correspondientes a un ISP venezolano, lo cual volvió a ser causa de interrupciones del servicio para los usuarios. Con regularidad, salen a luz datos relativos a eventos de esta clase en listas de correo y foros de operadores.

Fortalecimiento del sistema de enrutamiento mundial

Infraestructura de Clave Pública para Certificación de Recursos (RPKI): Reclamo de autoridad sobre el uso de un recurso de número

La Infraestructura de Clave Pública para Certificación de Recursos (RPKI) es un dispositivo de seguridad que permite verificar la asociación entre titulares legítimos de recursos y los recursos de número de Internet que se les asignaron. Cualquier RIR puede emitir un **certificado de recurso** correspondiente a un recurso de número de Internet que asigne siempre que el RIR pueda verificar la legitimidad de la asignación original y el derecho del titular. Los titulares de recursos también pueden establecer sus propias **autoridades de certificación**, lo que significa que podrán emitir certificados de recursos a sus clientes. Un certificado de recursos es un documento electrónico que declara que el RIR que otorga la certificación ha registrado un recurso específico. Contiene varios campos de datos, entre ellos:

- Clave pública (parte decisiva de la RPKI, que hace posible la verificación de la firma digital)
- Recursos alcanzados por el certificado
- Firma digital del registro emisor (en este caso, el RIR emisor)

Desde el punto de vista conceptual, los certificados de recursos equivalen a certificados conocidos que muchos sitios *web* emplean para el cifrado. Sin embargo, los certificados de recursos no contienen datos de identidad personales, pues la legitimidad del verificado se comprueba controlando las firmas digitales. Se supone que quien esté en condiciones de firmar objetos con la clave privada asociada con un certificado de recurso es el propietario legítimo de los recursos enumerados en ese certificado. Los certificados de recurso no se utilizan para comprobar la identidad de un usuario sino para mejorar la confiabilidad técnica del sistema de enrutamiento mundial.

El beneficio clave que proporciona la RPKI es la posibilidad de **validación**. Una vez que se ha emitido un certificado para un recurso específico, es posible comprobar la legitimidad de ese recurso. También es posible **automatizar** el procedimiento de validación, lo que allana el camino para implementar la validación en la infraestructura de enrutamiento misma, sin necesidad de recurrir a la intervención humana.

Implementación de la RPKI en la región cubierta por LACNIC

Los operadores de redes que trabajan en la región que atiende LACNIC están adoptando la RPKI como medida orientada a mitigar el impacto de los secuestros de rutas. En la actualidad, América Latina y el Caribe ocupan el segundo lugar en lo que respecta a implementación de RPKI y tecnologías asociadas, después de Europa. Además de su adopción por parte de los operadores, en 2013, LACNIC, la Internet Society, NAP.ec y Cisco Systems se asociaron para implementar RPKI y validación de origen en enrutadores de NAP.ec. La organización agrupa a la mayoría de los proveedores conectados a Internet del Ecuador; al implementar RPKI en la red de NAP.ec, Ecuador pasó a ser el primer país del mundo que se encuentra cubierto por RPKI en casi 100%.

Microsoft

Tendencias de Seguridad en LATAM, Segundo Semestre de 2013

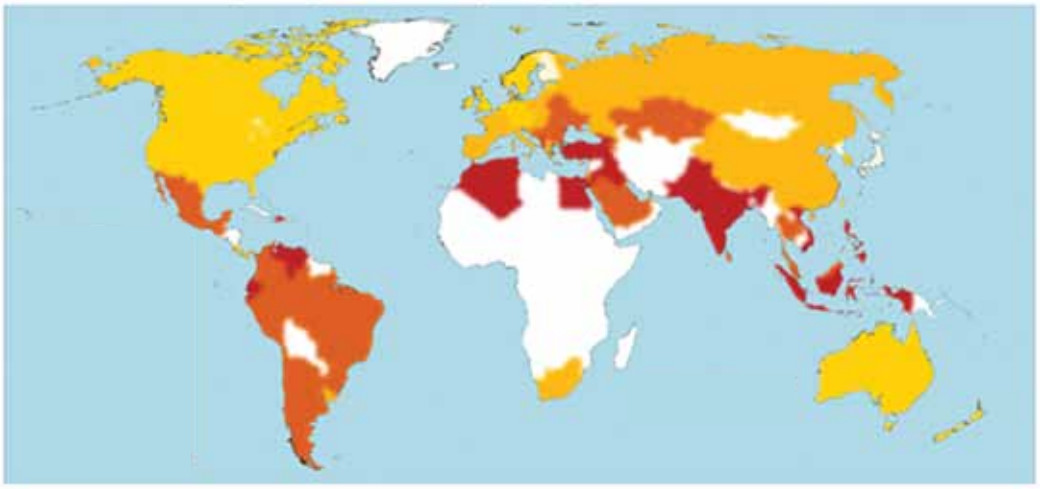
Continuando con las tendencias recientes, en 2013 los investigadores se dedicaron especialmente a buscar vulnerabilidades en las aplicaciones, en lugar de tratar de encontrarlas en sistemas operativos, aplicaciones de sistemas operativos o exploradores *web*. Es interesante observar que, a pesar de los cambios en las prioridades de las investigaciones, la cantidad de vulnerabilidades en sistemas operativos encontradas, en efecto, ha aumentado. A continuación incluimos estadísticas que dan cuenta de las tendencias globales en materia de vulnerabilidades y *malware* en 2013.

- Las vulnerabilidades en aplicaciones (sin incluir exploradores *web* ni aplicaciones de sistemas operativos) aumentaron 34.4 por ciento en el segundo semestre de 2013 y representaron 58.1 por ciento del total registrado en ese período
- Las vulnerabilidades en sistemas operativos aumentaron 48.1 por ciento en el mismo período, y pasaron de ser la vulnerabilidad menos frecuente a la más frecuente. En total, las vulnerabilidades en sistemas operativos constituyeron 17.6 por ciento del total de vulnerabilidades registradas en ese período
- Tras llegar a su punto más alto en el primer semestre de 2013, las vulnerabilidades en aplicaciones de sistemas operativos disminuyeron 46.3 por ciento en 2013, y representaron 14.7 por ciento de las vulnerabilidades denunciadas en ese período
- Las vulnerabilidades en exploradores denunciadas disminuyeron un 28.1 por ciento en la segunda mitad de 2013 y representaron el 9.6 por ciento de las vulnerabilidades denunciadas en ese período
- Los ataques por vulnerabilidad contra Java y HTML/Javascript fueron los más comunes en 2013, y los ataques contra el sistema operativo, Adobe Flash y formatos de documentos también son considerables
- Aunque van disminuyendo cada trimestre, los ataques contra Java fueron el tipo de ataque por vulnerabilidad más frecuente en la segunda mitad de 2013
- Las amenazas basadas en la *web* (HTML/JavaScript) se redujeron más de 50 por ciento en el primer semestre de 2013 y fueron el segundo tipo de ataque por vulnerabilidad más frecuente
- Las detecciones de ataques por vulnerabilidad contra sistemas operativos, Adobe Flash y documentos se mantuvieron generalmente estables durante la segunda mitad del año
- Java es víctima de una cantidad considerable de ataques de *malware*
- En promedio, cerca de 21.2 por ciento de las computadoras que informaron incidentes desde todo el mundo registraron *malware* en todos los trimestres de 2013. Al mismo tiempo, se eliminó *malware* de aproximadamente 11.7 de cada 1,000 computadoras donde se ejecutó un antivirus de Microsoft
- América Latina sigue siendo una región crítica, con altos niveles de detecciones en varios de los países más grandes —que incluyen México, Brasil, Colombia, Argentina, Perú y Chile— aunque se siguen registrando altos niveles de infecciones en la mayor parte de la región

- Las amenazas principales son los troyanos, los descargadores troyanos, los *droppers* (instaladores de *malware*) y los gusanos. Esto se relaciona con una mayor actividad en materia de robo de credenciales y *botnets* en América Latina. En Brasil, este tipo de actividad tuvo índices invariablemente más altos que la mayoría de los demás países de la región
- Las actividades de sitios maliciosos en la región suelen concentrarse principalmente en los sitios de hospedaje con distribución de *malware*, lo que probablemente se debe al aumento de las actividades de desarrollo de *malware* en algunos de los países
- Brasil registra altos niveles de actividad en materia de desarrollo y distribución de *malware*
- Las actividades de hospedaje con *drive by download* (descargas ocultas) se observan principalmente en Brasil y Colombia

Tasas de contacto (superiores) y tasas de infección (inferiores) por país/región en el T4 de 2013

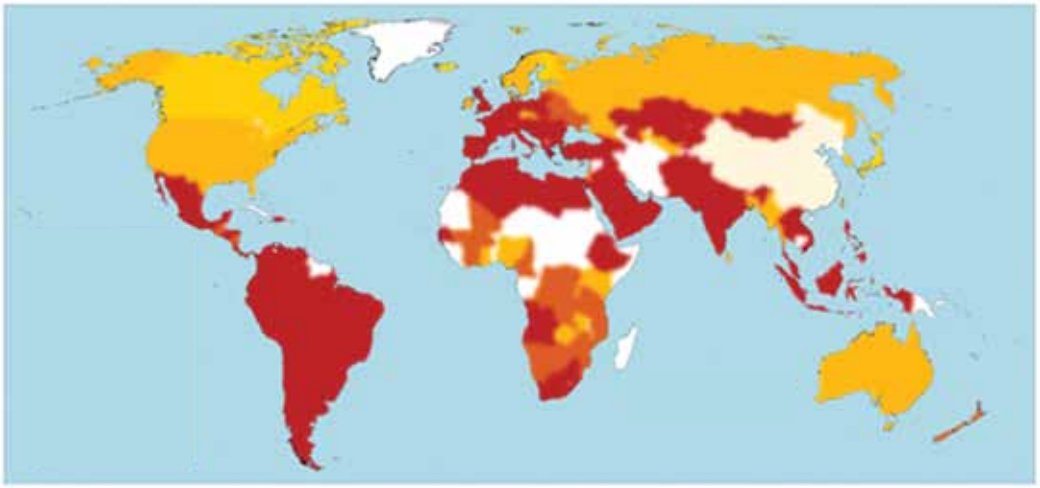
Fuente: Microsoft *Security Intelligence Report* – http://www.microsoft.com/sir



Porcentaje de computadoras que tuvieron contacto con *malware* —T4 de 2013

- 40%
- 30% a 40%
- 20% a 30%
- 10% a 20%
- >0 a 10%

A nivel mundial: 20.8



Computadoras depuradas cada 1,000 escaneadas —T4 de 2013

- 20+
- 15 a 20
- 10 a 15
- 5 a 10
- >0 a 5

A nivel mundial: 17.8

Organización de los
Estados Americanos

Organización de los
Estados Americanos

Symantec

Tendencias de Seguridad Cibernética
en América Latina y el Caribe

Latin American and Caribbean Cybersecurity Trends

Secretario General
José Miguel Insulza

Secretario General Adjunto
Albert R. Ramdin

Secretario de Seguridad Multidimensional
Adam Blackwell

Secretario Ejecutivo
del Comité Interamericano
contra el Terrorismo (CICTE)
Neil Klopfenstein

Autor Principal
Brian Sullivan

Editores
Brian Dito
Belisario Contreras

Vicepresidente
de Asuntos Gubernamentales
y Políticas Globales
de Seguridad Cibernética
Cheri McGuire

Director
William Wright

Editores colaboradores
Andrew Barris
Paul Wood

Analista de datos
Kavitha Chandrasekar

Gráficos y diseño
Scott Wallace

Edición en México
Candelaria Jaimes

Descargo de responsabilidades
Los contenidos de esta publicación no reflejan necesariamente las opiniones o políticas de la OEA o las organizaciones colaboradoras.

Junio de 2014

1889 F Street, N.W.,
Washington, D.C., 20006
United States of America

www.oas.org/cyber/

04/14