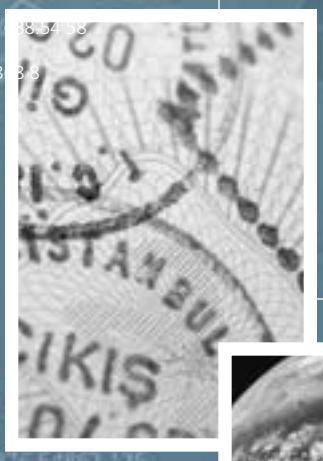
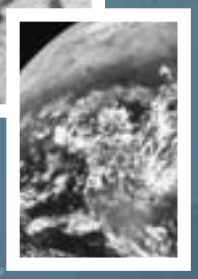
McAfee

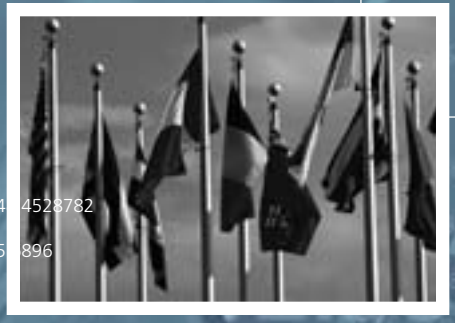
Informe sobre Criminología Virtual de McAfee

Ciberdelincuencia y ciberley

Estudio global anual de McAfee sobre la delincuencia organizada e Internet en colaboración con destacados expertos internacionales en materia de seguridad







454868.45 5 48

89 8 488.5545 6896

45645 866 665

4568 [illegible]

486 8[illegible]

454868.45 5 4[illegible]4528782

89 8 488.5545 [illegible]896

44 822.656

4568 45 4582 688.54 58

486 86484 8 8

Colaboradores

Dr. Ian Brown
Lilian Edwards
Matthew Bevan
Sharon Lemon
Bob Burls
Peter Sommer
Richard Clayton
Philip Virgo
Matthew Pemble
James Blessing
Peter Milford
Dr. Marco Gercke
Marc Vilanova
Haim Vismonski
Ferenc Suba
Erka Koivunen
Eugene H Spafford
Andrea Matwyshyn
Mary Kirwan
Leo Adler
Dr. Paulo Marco Ferreira Lima
Adriana Scordamaglia Fernandes Marins
Renato Opice Blum
Alana Maurushat
Peter Guttman
Andrew Adams

ÍNDICE

1 Prólogo

2 Introducción

4 **Capítulo uno:** Crisis general – La magnitud del problema

10 **Capítulo dos:** El frente de la batalla contra la ciberdelincuencia

18 **Capítulo tres:** Cooperación internacional. ¿Un mito o una posibilidad?

24 **Capítulo cuatro:** Pasos a seguir

26 Colaboradores

Prólogo

La ciberdelincuencia es un problema en auge que nos afecta negativamente a todos. Aunque en la última década se ha trabajado mucho para combatirla, los delincuentes siguen teniendo la sartén por el mango. Según algunos expertos, un ataque informático podría llegar a ser económicamente más devastador que los ataques físicos perpetrados el 11 de septiembre de 2001, lo que constituye una prueba clara y evidente de que algo debe cambiar. Este año, el *Informe sobre criminología virtual de McAfee®* aborda los factores que pueden impulsar este cambio.

La ciberdelincuencia tiene un impacto económico significativo en las empresas y en los consumidores en todo el mundo, y el uso cada vez más extendido de la tecnología en los países en vías de desarrollo está generando nuevas oportunidades para los delincuentes.

Como parte del esfuerzo de McAfee en la lucha contra la ciberdelincuencia global, hemos lanzado recientemente "McAfee Initiative to Fight Cybercrime", una iniciativa de gran alcance que tiene como objetivo cerrar brechas esenciales en la batalla contra la ciberdelincuencia. Aunque ahora disponemos de nuevas leyes en materia de ciberdelincuencia, y se han producido acusaciones formales recientes, creemos que todavía queda un largo camino por recorrer.

Está a punto de leer nuestro cuarto *Informe anual sobre criminología virtual.* Este año, el informe analiza en qué medida la ciberguerra está ganando la batalla a la ciberley y explica exactamente por qué es necesaria esta iniciativa de McAfee.

Para este informe, hemos consultado a más de una docena de especialistas en seguridad de importantes instituciones de todo el mundo. Hemos pedido a estos expertos, que también combaten en primera línea en la batalla diaria contra la ciberdelincuencia, su opinión sobre hasta qué punto la ciberley está evolucionando a la par que los delitos que se cometen, y les hemos solicitado un análisis sobre cómo podemos librar –y ganar– la batalla contra los autores de los ciberdelitos.

¿Qué conclusiones se han extraído? Siga leyendo para conocer los detalles, pero los expertos del más alto nivel coinciden en que es necesario adoptar medidas internacionales contra la ciberdelincuencia en cuanto a legislación, aplicación de la ley, acciones judiciales y sentencias.

La lucha contra la ciberdelincuencia es una batalla global sin tregua y no ha hecho más que empezar.

Dave DeWalt

Presidente y Director Ejecutivo

McAfee Inc.

Introducción

El objetivo del *Informe anual sobre criminología virtual de McAfee* ha sido siempre detectar las tendencias nuevas e inminentes en el comportamiento de la ciberdelincuencia, así como poner de manifiesto hasta qué punto este fenómeno es cada vez más organizado, sofisticado y global en lo que respecta a su enfoque y sus consecuencias.

Este año, en colaboración con expertos en ciberdelincuencia de todo el mundo, el cuarto *Informe anual sobre criminología virtual de McAfee* revela en qué medida la ciberdelincuencia está ganando la batalla a la ciberley, y deja patente la necesidad de un esfuerzo global coordinado para restablecer el equilibrio.

Por encargo de McAfee, el Dr. Ian Brown del Oxford Internet Institute y Lilian Edwards, profesora de Derecho de Internet en la Universidad de Sheffield en el Reino Unido, han llevado a cabo una extensa investigación entre fuerzas de seguridad, autoridades judiciales y expertos en seguridad de todo el mundo para evaluar el estado actual de la lucha contra la ciberdelincuencia y analizar las amenazas y retos con el objeto de preparar una ofensiva global para el futuro.

Tres conclusiones clave

En primer lugar, los gobiernos aún no consideran la ciberdelincuencia como una auténtica prioridad, lo que dificulta el desarrollo de la lucha para combatirla en todo el mundo. Además, la amenaza física de terrorismo y desplome económico está desviando la atención política a otras cuestiones y, mientras tanto, los ciberdelincuentes no pierden el paso. La recesión ha resultado ser terreno fértil para las actividades delictivas, ya que los estafadores se afanan por sacar partido del uso cada vez más extendido de Internet y del clima de miedo y preocupación. ¿Corremos el riesgo de minar irrevocablemente la confianza de los consumidores y, como consecuencia, limitar las posibilidades de recuperación económica?

En segundo lugar, la acción transfronteriza de las fuerzas de seguridad sigue siendo un requisito insalvable para combatir la ciberdelincuencia. La coyuntura local dificulta la aplicación transnacional de las leyes. Por lo tanto, a menos que se asignen los suficientes recursos a los esfuerzos internaciones, los ciberdelincuentes seguirán siempre jugando con ventaja.

En tercer lugar, las fuerzas de seguridad siguen respondiendo de forma improvisada según el momento y no están convenientemente preparadas para hacer frente a la situación. Si bien se ha observado un cierto progreso, todavía existe una importante carencia en cuanto a formación y conocimientos en análisis forense digital y recopilación de elementos probatorios, así como en los tribunales de justicia de todo el mundo. Los cerebros de la ciberdelincuencia siguen sueltos mientras que los conocidos como "mulas" (o personas utilizadas con fines delictivos, a menudo sin ser conscientes de ello) responden ante la justicia. Algunos gobiernos son culpables de proteger a los delincuentes de su propio país. Las conclusiones sugieren que existe una necesidad cada vez mayor de armonizar las prioridades y coordinar las fuerzas policiales entre los distintos países.

El informe termina con un análisis de las medidas propuestas, tanto a escala local como internacional, para que la lucha contra la ciberdelincuencia sea más eficaz.

CAPÍTULO UNO
Crisis general – La magnitud del problema

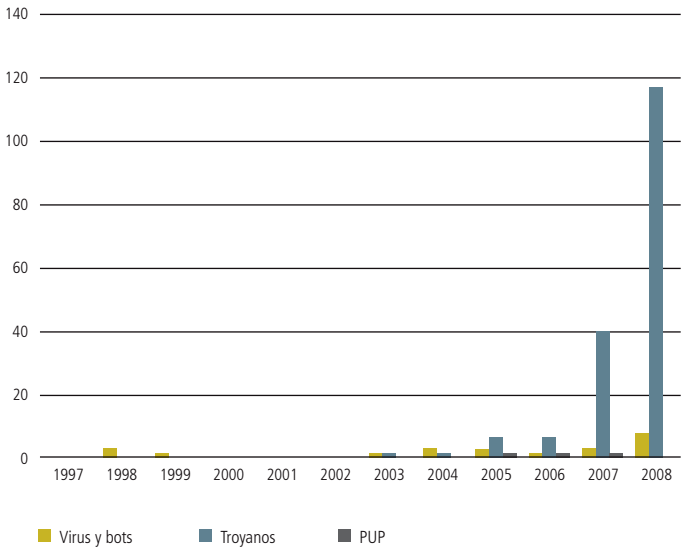
La magnitud de los problemas de seguridad en Internet aumenta a paso acelerado. Los delincuentes han aprovechado las vulnerabilidades tanto del software como de la psicología humana para concebir un amplio espectro de amenazas, como son los ataques de spyware, phishing, adware, rootkits, spam o redes de bots.

Pese al notable aumento del volumen de malware observado en los últimos 12 meses, los ciberdelincuentes cada vez recurren más a técnicas comprobadas y de eficacia demostrada para causar estragos y conseguir dinero.

La desaceleración económica puede exacerbar los problemas de seguridad

Crecimiento del malware y los programas potencialmente no deseados[1] (principales variantes)

En miles



1 Un PUP (programa potencialmente no deseado) es un programa no deseado a pesar de que el usuario puede haber dado su consentimiento para descargarlo: los PUP incluyen spyware, adware y marcadores.

Los estafadores on line disponen de una amplia variedad de medios, que no dejan rastro, para blanquear los ingresos procedentes de sus actividades delictivas

La fiebre del oro

E-gold es una moneda de oro digital que permite la transferencia instantánea de la propiedad del oro. A diferencia de las tarjetas de crédito, todos los pagos son definitivos e irreversibles. En la actualidad existen más de cinco millones de cuentas e-gold en todo el mundo. Debido al anonimato conferido a los titulares de las cuentas, se convirtió en un método popular entre los ciberdelincuentes para convertir en dinero limpio los ingresos obtenidos de forma ilícita.

En julio de 2008, trascendió el secuestro del hermano de Joseph Yobo, el segundo capitán de la selección de fútbol nigeriana y uno de los mejores futbolistas del Everton en la Premier League, por el que se pidió un rescate de 10.000 dólares en e-gold. Este suceso dejó patente una nueva modalidad digital de un antiguo delito.

Asimismo, en julio de 2008, e-gold Ltd. y sus tres directores, se declararon culpables de las acusaciones de blanqueo de dinero y de la "gestión de una empresa de transmisión de dinero sin licencia". Aunque los ejecutivos de e-gold están pendientes de sentencia, la empresa confía en que el negocio pueda revitalizarse.

En octubre de 2008, e-gold avanzó hacia su total legalización registrándose en la Financial Crimes Enforcement Network (FinCEN), una de las principales agencias del Departamento del Tesoro estadounidense en la lucha contra el blanqueo de dinero.

Los ciberdelincuentes cada vez son más activos y dejan menos rastro

Un gran número de equipos conectados a Internet sin protección se han convertido en la actualidad en un refugio seguro para los ciberdelincuentes. Según revelan cifras recientes, sólo en el último trimestre, el número de equipos zombis afectados en redes de bots se ha cuadruplicado y ahora podrían saturar Internet con más de 100.000 millones de mensajes de spam diarios. Las redes de bots se centran cada vez más en ataques de phishing, de denegación de servicio distribuido (DDoS) y a sitios Web, con capacidad para infligir grandes daños y que suponen una amenaza creciente para la seguridad de las naciones, la infraestructura de información nacional y la economía.

También están surgiendo nuevos métodos para blanquear el dinero conseguido de forma ilícita. Los estafadores on line disponen de una amplia variedad de medios, que no dejan rastro, para blanquear los ingresos procedentes de sus actividades delictivas. Anteriormente, era posible detectar y recuperar los pagos fraudulentos en los sistemas bancarios; sin embargo, en la actualidad los expertos coinciden en que la ley no ha evolucionado al mismo ritmo que los sistemas de pago.

Los estafadores on line recurren con mayor frecuencia a servicios de pago no bancarios, como "e-gold". Como consecuencia, en la era de la ciberdelincuencia cada vez resulta más complicado aplicar la antigua consigna de "Sigue al dinero".

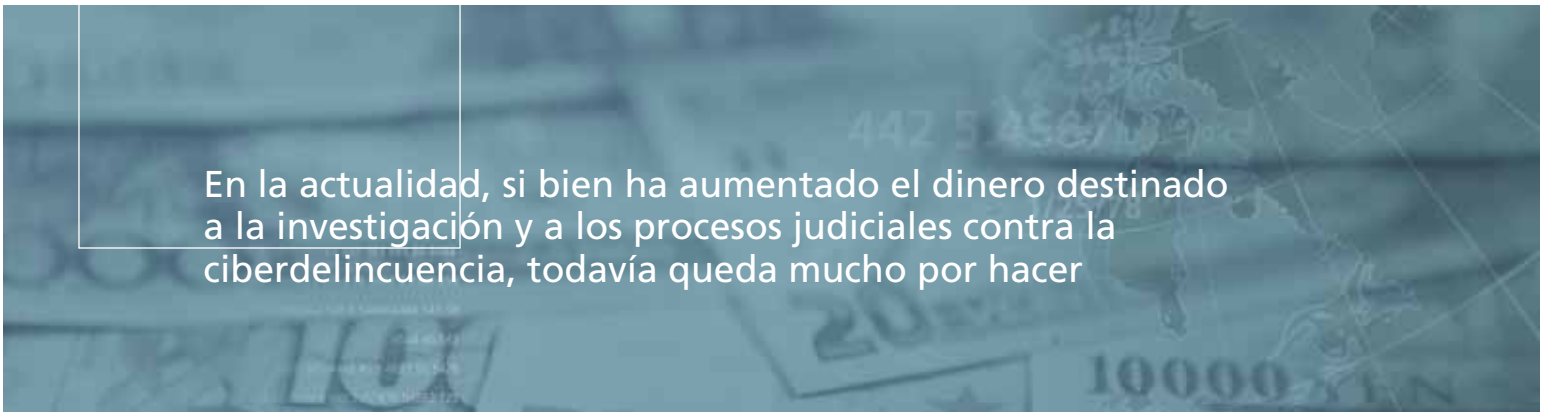
Los ciberdelincuentes también están recurriendo a las monedas de mundos virtuales como medio para legitimar dinero. Por ejemplo, pueden abrir una cuenta, ingresar fondos procedentes de fraudes, el uso de malware y otras actividades delictivas, y tener un socio en el otro lado del mundo que retire fondos como beneficios o incluso como capital activo para otra empresa con fines delictivos. Por otra parte, el envío de mensajes es gratuito en el mundo on line, por lo que el dinero también puede reinvertirse en campañas de spam y blanquearse como ingresos provenientes de dichas operaciones.

Asimismo, es probable que la amplia difusión del método de pago a través del teléfono móvil ("m-payment") en países menos desarrollados –que a menudo carecen de un marco regulador y donde la corrupción es moneda corriente– facilite aún más el blanqueo de dinero en la ciberdelincuencia, así como la financiación de actividades terroristas.

La recesión mundial puede beneficiar a los ciberdelincuentes

La situación puede empeorar si los problemas más alarmantes, la crisis económica global y la incesante guerra contra el terrorismo, acaparan toda la atención. Curiosamente, nunca ha sido tan necesario como ahora centrarse en la seguridad de Internet, ya que las oportunidades para que los ciberdelincuentes saquen tajada nunca han sido mayores y el coste para los consumidores, la industria y la seguridad nacional sigue aumentando.

Como explica Matthew Bevan, un pirata informático reformado: "No creo que los ciberdelincuentes estén utilizando nuevas técnicas, simplemente están adoptando enfoques ligeramente distintos para engañarnos. Las amenazas más modernas y eficaces tienden a ser ataques automatizados, ya que para los delincuentes son mucho más fáciles de perpetrar y les permiten ganar más con menos esfuerzo, por así decirlo. Cuanto menos tengan que invertir, ya sea en tiempo o dinero, para obtener un mayor beneficio, mejor".



En la actualidad, si bien ha aumentado el dinero destinado a la investigación y a los procesos judiciales contra la ciberdelincuencia, todavía queda mucho por hacer

Los ciberdelincuentes se aprovechan del miedo de los consumidores

Los ciberdelincuentes se aprovechan de que la desaceleración económica haya motivado en todo el mundo un uso cada vez más frecuente de Internet para buscar las mejores ofertas y trabajos, y para gestionar sus finanzas. Se aprovechan del miedo y de la incertidumbre, y sacan partido porque los consumidores suelen ser más vulnerables y más negligentes en los momentos difíciles. De hecho, las oportunidades de ataque van en aumento.

Como advierte Philip Virgo, Secretario General del EURIM (European Information Group Society), la alianza para la seguridad de la información (Information Security Alliance) del Reino Unido: "Estamos asistiendo a una oleada de mensajes de phishing que supuestamente proceden de bancos que ofrecen una respuesta a la crisis. También observamos la aparición de una serie de sitios para buscar empleo y tramitación de currículum vítae que son falsos y cuyo principal objetivo es recabar datos personales".

Asimismo, con el aumento de la volatilidad de la seguridad laboral y las tasas de desempleo, existe el riesgo de que los consumidores se sientan atraídos por los sistemas de hacer dinero fácil a través de Internet y acaben convirtiéndose en "mulas" al servicio de las bandas de ciberdelincuentes. Los estafadores contratan a las mulas en calidad de "representantes de ventas internacionales", "responsables de transporte" u otros empleos falsos y les piden que reciban "pagos" que luego ellos se encargan de transferir al extranjero tras deducir una pequeña "comisión".

Del mismo modo, existen sitios que ofrecen dinero a los internautas simplemente por añadir unas pocas líneas de código en sus páginas Web. En este sentido, se convierten en el tipo de mula más básico: el punto de ataque.

Matthew Bevan está de acuerdo en que los consumidores están cada vez más expuestos a la ciberdelincuencia: "En el clima económico actual, cuando el dinero es una de nuestras principales inquietudes, bajamos la guardia y es más fácil que caigamos en la trampa de los timos de dinero fácil. Estoy seguro de que este tipo de ataques irá en aumento y seguirá creciendo durante el próximo año. La crisis crediticia también está afectando a los ciberdelincuentes, por lo que incrementarán sus esfuerzos para hacer 'dinero'".

Y sigue así: "También creo que habrá más víctimas de la ciberdelincuencia, ya que las ventajas de contar con seguridad no son evidentes de forma inmediata, y es posible que algunas personas empiecen a escatimar; por ejemplo, prescindiendo de las últimas actualizaciones o versiones del software de seguridad, lo que las hace todavía más vulnerables".

Sin embargo, el e-commerce y el e-goverment dependen de la tranquilidad y la confianza del consumidor en las operaciones on line y, consecuentemente, son esenciales para la recuperación económica y el desarrollo continuado.

Como resume Alana Maurushat, Directora en funciones del Centro de Políticas y Derecho del Ciberespacio de la Universidad de Nueva Gales del Sur en Australia, los consumidores acabarán impulsando la demanda de ciberseguridad en todos los niveles: "Los consumidores van avanzando lentamente en la familiarización con los temas de seguridad. Esto tendrá una reacción en cadena similar a la observada en los movimientos de consumo ecológico; al igual que los consumidores han demandado productos respetuosos con el medio ambiente, acabarán por demandar productos y servicios seguros, incluidas transacciones de Internet seguras".

"Hace unos años, la balanza estaba equilibrada: el nivel de inversión en seguridad era insuficiente tanto por parte del sector privado y corporativo, como por parte de las fuerzas de seguridad en materia de ciberdelincuencia... En la actualidad, si bien ha aumentado el dinero destinado a la investigación y a los procesos judiciales contra la ciberdelincuencia, todavía queda mucho por hacer".

"Hemos pasado de un enfoque pasivo a un enfoque reactivo. La prevención activa es el componente clave que falta".

La industria está en la cuerda floja entre el gasto a corto plazo y las pérdidas a largo plazo

Una cuestión clave que cabría plantearse como consecuencia de la falta de liquidez es si las leyes que garantizan una mayor seguridad pueden considerarse factibles o aceptables para la industria, dada la delicada situación financiera de muchos sectores, especialmente el bancario.

El argumento contrario sería que las leyes son esenciales en épocas de vacas flacas, ya que los requisitos de conformidad con las normativas se anteponen al gasto por encima de lo recomendable.

Peter Sommer, profesor visitante del Grupo de Integridad de Sistemas de Información de la London School of Economics y profesor adjunto en la Open University del Reino Unido, se muestra optimista y piensa que se reconocerá la necesidad de inversión para reducir pérdidas potenciales, si bien es consciente del coste de consolidación de la industria. Es probable que la fusión precipitada de infraestructuras de TI heterogéneas y fragmentadas revele problemas de conformidad, al tiempo que comprometa la seguridad de datos valiosos.

"Aunque se pueda pensar que la falta de liquidez afectará a las inversiones en seguridad, varias conversaciones recientes me han persuadido de que la mayoría de las empresas son conscientes de que los presupuestos para seguridad deben ir en función de los esfuerzos para reducir pérdidas, no un porcentaje arbitrario de costes de infraestructura de TCI (tecnología de información y comunicaciones). Varios responsables de seguridad de instituciones financieras piensan que realmente tendrán que aumentar sus presupuestos para satisfacer las necesidades de los nuevos marcos reguladores y de conformidad con las normativas. Otro problema añadido será gestionar los costes de transición derivados de fusiones rápidas y forzadas entre instituciones donde dos infraestructuras de TCI y dos culturas corporativas distintas deberán reducirse a una".

Las empresas deben ser precavidas a la hora de realizar la evaluación global de sus riesgos y activos, e invertir en seguridad en consecuencia. La seguridad en época de recesión es fundamental para preservar las buenas prácticas corporativas, la reputación y la confianza del público.

Mary Kirwan, abogada internacional y antigua fiscal de ciberdelincuencia en Canadá, considera que la desaceleración está llevando a las empresas de vuelta a lo básico. Esto puede tener un efecto positivo si se realiza de forma apropiada, pero puede tener consecuencias nefastas si no se frena el desarrollo de las brechas vitales en seguridad:

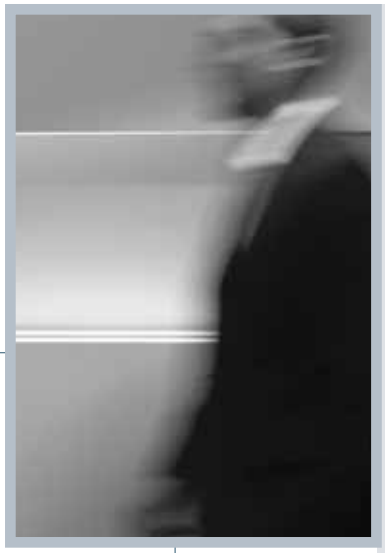
"Hay un salto hacia la calidad, hacia la seguridad, hacia el estudio de los principios básicos. Se huye de la complejidad y se busca la simplicidad. Las empresas están volviendo a lo básico. La gestión de riesgos vuelve a estar en boga. La seguridad debe recuperar su lugar, en lo alto de la cadena de valor, como un componente crítico de una estrategia de gestión de riesgos racional. Una vez en su sitio, su futuro será prometedor".

"Sin embargo, resulta evidente la necesidad de recuperar la confianza para restablecer el orden en el caos de los mercados globales. No habrá solución si las empresas, para colmo de males, tratan de forma negligente la información confidencial de los consumidores y los dejan a merced de los piratas informáticos".

Amenaza constante de ataque nacional

El informe del año pasado se centró en el uso cada vez más extendido de Internet como arma para el espionaje político, militar y económico. Se trata de una tendencia que no se ha disipado en los últimos 12 meses, como evidencia el número creciente de ataques registrados.

Con frecuencia se ha considerado la amenaza del ciberterrorismo sobredimensionada, sin embargo, cada vez son más quienes opinan que los piratas informáticos acabarán siendo lo suficientemente audaces y poderosos para lanzar ataques que puedan dañar y destruir elementos de la infraestructura nacional de importancia crítica.



Caso real **Mayores indicios de ciberespionaje y ataques nacionales**

En mayo de 2008, Bélgica y la India se sumaron a la creciente lista de países que alegan ser víctimas de ataques supuestamente procedentes de China. Bélgica, en el punto de mira por albergar algunas de las principales sedes de la UE y la OTAN en Bruselas, ha sido víctima del envío de mensajes con spyware a las secretarías de estado. Del mismo modo, la India sostiene que su gobierno y las redes del sector privado son el blanco de constantes ataques informáticos.

En agosto de 2008, se coordinó un ataque informático contra la infraestructura de Georgia que afectó a los sitios Web del gobierno georgiano, incluido el Ministerio de Asuntos Exteriores. El gobierno de Georgia declaró que los daños habían sido causados por ataques perpetrados por Rusia en relación con el conflicto entre los dos estados por la provincia de Osetia del Sur.

En octubre de 2008, en la Conferencia Internacional sobre Terrorismo y Medios Electrónicos, se destacó el uso actual de Internet como la principal fuente para la creación de amenazas terroristas, y que en la actualidad existen más de 7.500 sitios vinculados a amenazas terroristas en la Web.

El potencial es significativo y los gobiernos deben continuar reuniendo recursos para la lucha contra la ciberdelincuencia pese a la recesión económica global.

Los gobiernos relegan la seguridad a un segundo plano

A pesar de un aumento evidente del riesgo para la seguridad nacional, los gobiernos siguen sintiéndose intimidados ante el primer obstáculo en lo que a ciberdelincuencia se refiere. No conciben la ciberseguridad como una prioridad debido a la ignorancia técnica y la falta de previsión de riesgos generalizados y a largo plazo, y no le dedican tiempo ni recursos legislativos.

Peter Sommer, profesor visitante del Grupo de Integridad de Sistemas de Información de la London School of Economics y profesor asociado en la Open University, declara: "La ciberdelincuencia era un tema muy preocupante para el gobierno a finales de los 90, cuando la Administración Blair estaba convencida de que Gran Bretaña tenía que convertirse en una economía altamente competitiva y en la meca del comercio electrónico; incluso entonces, costó muchos esfuerzos que se fundara la Unidad de Delitos Tecnológicos Nacional (National High-Tech Crime Unit, NHTCU). La NHTCU dejó de existir en 2006 cuando desapareció la Brigada Nacional contra el Crimen (National Crime Squad), y la Agencia contra el Crimen Organizado (SOCA, Serious Organised Crime Agency) no forma parte de la estructura de las fuerzas policiales del Reino Unido, y su modo "furtivo" de funcionamiento original perdió la confianza del público a causa de su invisibilidad".

"A partir de la primavera de 2009, dispondremos de una unidad policial central especializada en delitos electrónicos (PceU), pero ha llevado mucho tiempo y todavía está en ciernes. Es probable que los ciudadanos sigan teniendo dudas sobre dónde acudir para denunciar un delito. También habrá tres organismos semiautónomos consagrados a servicios de información y denuncia de fraudes, con la Policía de la Ciudad de Londres a la cabeza de la lucha contra el fraude. En otros lugares, también habrá una oficina para la lucha contra el fraude (Serious Fraud Office). Todo esto es un caldo de cultivo para disputas entre agencias. En general, la lucha contra la ciberdelincuencia no ha sido una prioridad para los círculos del Gobierno laborista, donde ha tenido las de perder frente al terrorismo y el comportamiento antisocial".

Caso real **El gobierno considera innecesarias las medidas para reforzar la seguridad**

En agosto de 2007, el Comité de Ciencia y Tecnología de la Cámara de los Lores del Reino Unido advirtió al gobierno de que Internet apuntaba maneras para convertirse en un "Lejano Oeste" fuera de la ley y precisaron que era necesario actuar de inmediato para que la Web no se convirtiera en un "patio de recreo de delincuentes". Pusieron de relieve que el miedo a los delitos electrónicos estaba sobrepasando al del atraco y que sin la implementación de medidas e incentivos esenciales para tomar control de la seguridad, se perdería la confianza del público en Internet.

En noviembre de 2007, el gobierno del Reino Unido decidió rechazar prácticamente todas las recomendaciones del informe por considerarlas innecesarias.

Peer Lord Broers, que presidió las sesiones de seguridad de Internet del Comité, afirmó: "En nuestro informe inicial, planteamos nuestra preocupación por que la confianza pública en Internet se viera deteriorada si no se hacía más para prevenir y perseguir los delitos electrónicos. Teníamos la impresión de que el Gobierno, la policía y los desarrolladores de software estaban eludiendo sus responsabilidades e, injustificadamente, estaban dejando a los usuarios en la estacada".

Sin embargo, después de las masivas fugas de datos que han azotado a las agencias gubernamentales del Reino Unido, como la agencia tributaria HMRC (Her Majesty's Revenue and Customs) el año pasado, la Cámara de los Lores ha reiterado sus recomendaciones básicas y es posible que esta vez se les preste más atención.

Entonces, ¿qué ocurrirá si continuamos relegando y desdeñando la ciberdelincuencia?

Mary Kirwan lo resume del siguiente modo: "Los maleantes heredarán la tierra, y nosotros quedaremos abandonados a nuestra suerte".

"El talón de Aquiles del sector tecnológico es la misma vulnerabilidad que tiene al sector de los servicios financieros: arrogancia a raudales. Se venera la complejidad como un fin en sí mismo y se menosprecia la simplicidad. Hay un desconocimiento de las interdependencias críticas por falta de comunicación. Prácticamente ignoramos qué es lo que mantiene unidas las piezas del monstruo de Frankenstein que hemos creado y qué puede hacerlo pedazos de igual modo".

"Pero los maleantes están bien informados y están preparados para aprovechar la manifiesta falta de pensamiento holístico en el sector".

CAPÍTULO DOS
El frente de la batalla contra la ciberdelincuencia

Es sabido que en todo el mundo se están adoptando nuevas medidas de ciberseguridad, pero, vistos los miles de millones que se pierden al año por culpa de la ciberdelincuencia, ¿no será demasiado poco y demasiado tarde?

EUROPA La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) es un centro de asesoramiento para los Estados miembros y las instituciones de la UE en materia de seguridad de las redes y de la información. Ayuda a modernizar Europa y a asegurar el correcto funcionamiento de la economía digital y la sociedad de la información. El presupuesto de 2008 ascendía a 8 millones de euros.

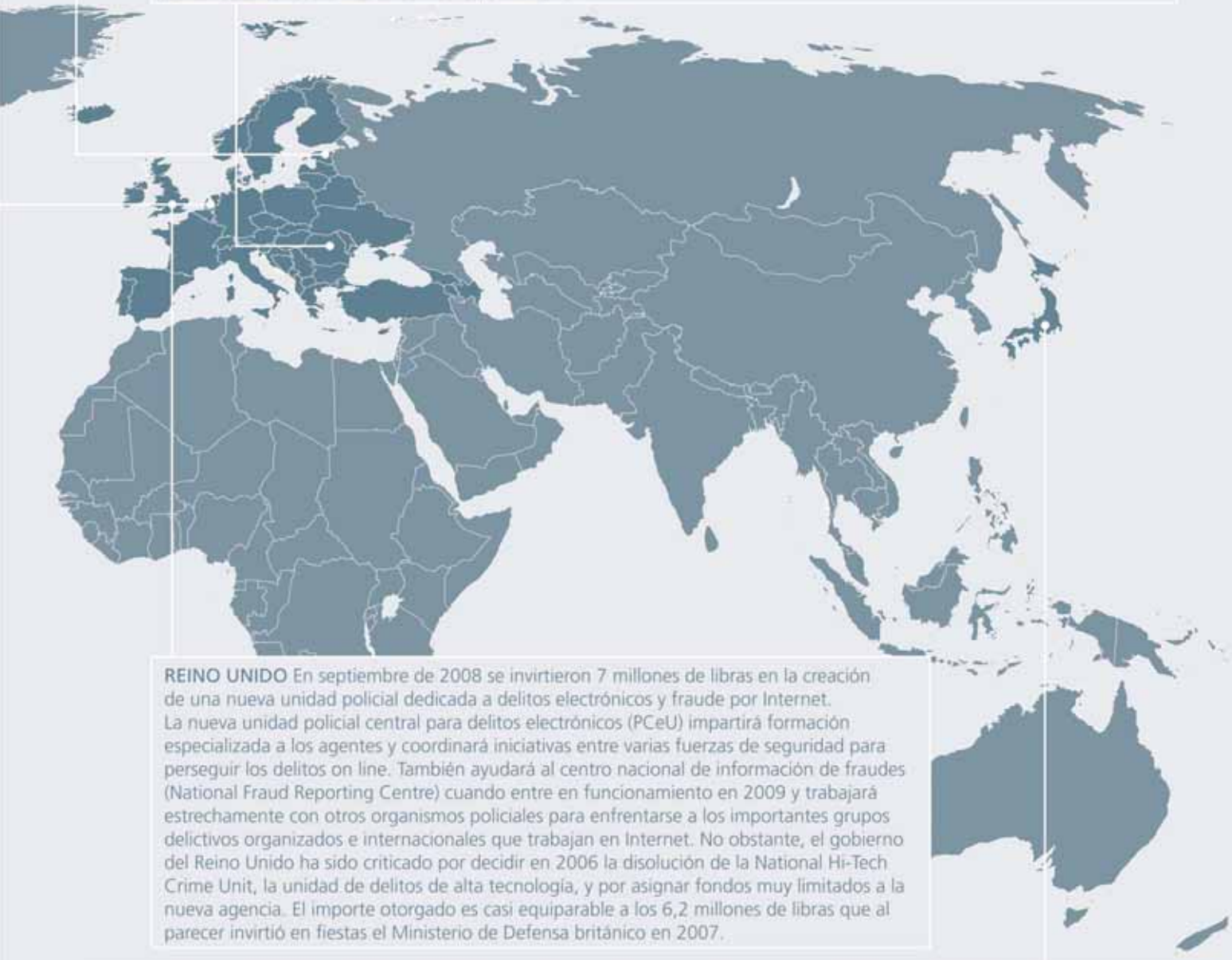
EE. UU. Es el país del mundo que más invierte en ciberseguridad y que tiene a los técnicos e investigadores más especializados trabajando en este problema, ya sea en universidades, en el ámbito empresarial o en el gobierno. El Departamento de Seguridad Nacional presupuestó 155 millones de dólares en ciberseguridad para 2008 y pretende elevar la partida a 200 millones para el año fiscal 2009. El presidente Bush también solicitó 17.000 millones de dólares al Congreso para una iniciativa de ciberseguridad. Sin embargo, esta iniciativa ha sido criticada por destinar miles de millones a "proyectos desacertados y probablemente ilegales y a tecnología embrionaria cuya eficacia está por demostrar", y por centrarse demasiado en la vigilancia interna en vez de en la defensa activa contra los ataques.

Obama ha prometido nombrar un ciberasesor nacional directamente a sus órdenes (en lugar de tres puestos más abajo en el escalafón, como en la Administración Bush) para sincronizar la actividad. Para él, la ciberseguridad es una "prioridad máxima" del siglo XXI. Aun así, los detalles de sus planes siguen siendo imprecisos.

BRASIL Considerado uno de los tres países del mundo más infectados con equipos zombis y redes de bots, Brasil ha sido además víctima de 166.987 tentativas de ciberataque en 2008, cifra con la que ocupa el tercer puesto mundial. Pero Brasil se defiende y está reconsiderando adherirse al Convenio sobre la Ciberdelincuencia del Consejo de Europa mediante varios proyectos de ley que se ciñen al contenido del Convenio. Sin embargo, las discrepancias entre los distintos proyectos de ley que se están debatiendo en las cámaras legislativas brasileñas son considerables. En la práctica, uno de ellos representa incluso un paso atrás en los avances de investigación logrados hasta la fecha.

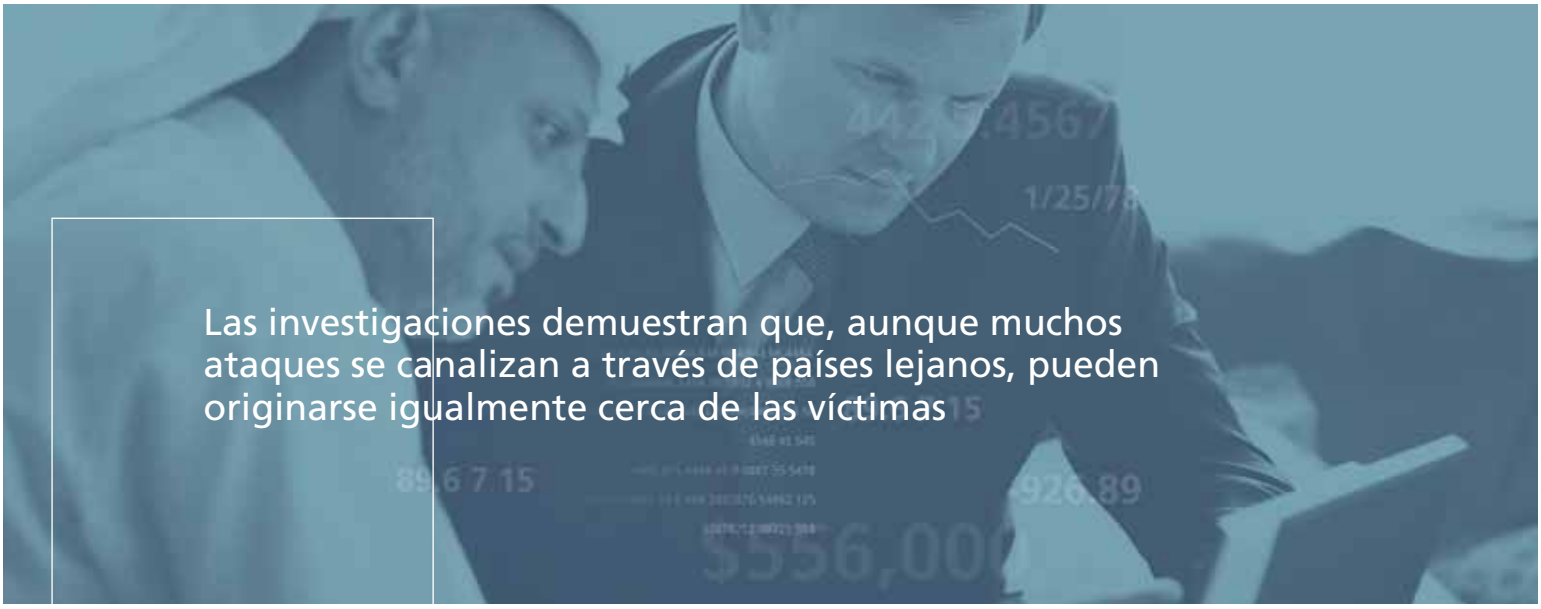
ESTONIA Aun siendo pequeño, Estonia está considerado como uno de los países con mayor capacidad tecnológica de Europa en cuanto a ciberseguridad y medidas contra el terrorismo electrónico. Este dinamismo se debe a los prominentes y repetidos ataques DDoS que sufrieron los servidores del gobierno, los medios de comunicación y los bancos en abril de 2007. En mayo de 2008, Estonia instaló un concentrador secreto de ciberseguridad, operativo desde agosto de 2008, con el respaldo de la OTAN y de siete países de la UE (Estonia, Alemania, Italia, Letonia, Lituania, Eslovaquia y España). Estonia también ha donado 50.000 € para apoyar el Convenio sobre la Ciberdelincuencia del Consejo de Europa.

RUMANÍA ha dado grandes pasos para perseguir la ciberdelincuencia aprobando nueva legislación contra la piratería y reforzando su capacidad para luchar contra la ciberdelincuencia. Estas medidas han surgido como consecuencia de los ataques de phishing coordinados de bandas delictivas rumanas contra bancos estadounidenses, perjudicados hasta tal punto que algunas empresas bloquearon todo el tráfico de Internet procedente de Rumania. Estos hechos coincidieron con los esfuerzos oficiales para fortalecer los lazos con Occidente y entrar en la OTAN, por lo que frenar la ciberdelincuencia cobró gran importancia. Rumania volvió a colaborar con el FBI en 2008 para arrestar de nuevo a docenas de rumanos pertenecientes a una banda de fraude por Internet.



REINO UNIDO En septiembre de 2008 se invirtieron 7 millones de libras en la creación de una nueva unidad policial dedicada a delitos electrónicos y fraude por Internet. La nueva unidad policial central para delitos electrónicos (PCeU) impartirá formación especializada a los agentes y coordinará iniciativas entre varias fuerzas de seguridad para perseguir los delitos on line. También ayudará al centro nacional de información de fraudes (National Fraud Reporting Centre) cuando entre en funcionamiento en 2009 y trabajará estrechamente con otros organismos policiales para enfrentarse a los importantes grupos delictivos organizados e internacionales que trabajan en Internet. No obstante, el gobierno del Reino Unido ha sido criticado por decidir en 2006 la disolución de la National Hi-Tech Crime Unit, la unidad de delitos de alta tecnología, y por asignar fondos muy limitados a la nueva agencia. El importe otorgado es casi equiparable a los 6,2 millones de libras que al parecer invirtió en fiestas el Ministerio de Defensa británico en 2007.

JAPÓN ha implantado las redes de comunicaciones de próxima generación más rápidas y avanzadas del mundo. En los últimos años también ha estado expuesto a varios ataques de malware y fugas de datos muy perjudiciales, especialmente con gusanos que se propagan a través de la red peer to peer (P2P) Winny. Japón ha contraatacado de forma inusual procesando al creador del sistema P2P Winny por ayudar a infringir derechos de autor. Recurrió a este planteamiento poco convencional porque carece de leyes adecuadas para criminalizar la creación de virus. Los proveedores de servicios de Internet (ISP) japoneses también están desempeñando un papel activo para poner freno al malware: cuatro de los ISP más importantes del país han emprendido un plan colectivo para anular el acceso a Internet de los usuarios sorprendidos utilizando tecnología de intercambio de ficheros tipo Winny. Sin embargo, la lentitud con que el Gobierno ha implantado las medidas de la Ley para la Protección de Información Personal de 2003 no estimula a los sectores público ni privado a tratar los problemas de seguridad con la seriedad que debieran.



Las investigaciones demuestran que, aunque muchos ataques se canalizan a través de países lejanos, pueden originarse igualmente cerca de las víctimas

Chivos expiatorios de los delitos de alta tecnología

Siempre se ha dicho que los ciberdelitos se organizan principalmente desde paraísos legales como Moldavia y países en desarrollo como Brasil y China. No obstante, las investigaciones demuestran que, aunque muchos ataques se canalizan a través de países lejanos, pueden originarse igualmente cerca de las víctimas, donde resulta mucho más fácil transferir dinero electrónicamente de su cuenta bancaria.

"Es un mito que los piratas sean chavales de 15 años encerrados en cuartos oscuros y que todos los ciberdelincuentes estén en el extranjero", afirma Bob Burls, Agente de la Unidad de Delitos Informáticos de la Policía Metropolitana de Londres. "Al igual que con las drogas, hay grandes traficantes, pero también camellos callejeros. Donde hay delincuencia, hay jerarquías de delincuentes y también focos locales de delincuencia".

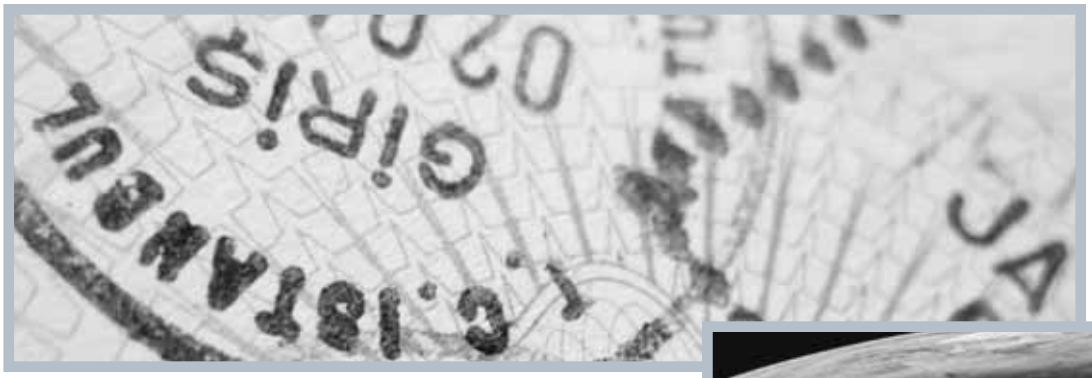
Eugene Spafford, profesor de Informática en la Universidad de Purdue y Director Ejecutivo del Centro de Educación e Investigación en Seguridad y Garantía de la Información (CERIAS) en Estados Unidos, también destaca que los delincuentes son cada vez más ingeniosos a la hora de ocultar su "posición" y con frecuencia están mucho más cerca de lo que se creía al principio:

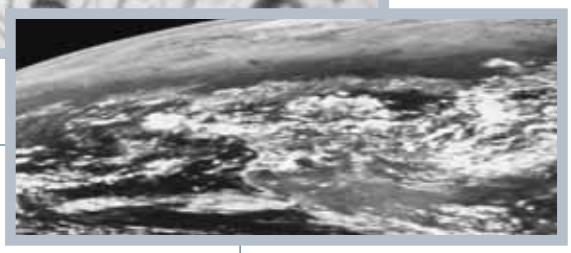
"He trabajado con varias fuerzas de seguridad intentando rastrear fraudes que parecen provenir de otros países. Es posible que algunos se originen en ellos, pero puede que otros procedan de la calle de al lado, donde alguien accede a un ordenador de otro país y lo utiliza para encubrir su participación".

Alana Maurushat, de la Universidad de Nueva Gales del Sur en Australia, cree que se trata de una tendencia creciente y que algunos países se utilizan habitualmente como chivo expiatorio de la actividad delictiva:

"Ahora mismo el chivo expiatorio es Brasil, punto desde el que chinos y vietnamitas redirigen el tráfico. Pero lo verdaderamente interesante es que los ataques propiamente dichos se llevan a cabo de forma local con total impunidad".

"De hecho, el quid de la cuestión parece ser la ocultación. No es difícil hacer creer que el malware y las actividades de espionaje proceden de un país que no es el de origen. En este sentido hay bastante desorientación, porque mucho tráfico se desvía como señuelo. El ataque en sí puede originarse en la misma ciudad que el objetivo. Esto suele ocurrir en casos de espionaje entre países y empresas".





¿Estamos capturando a los cibercapos? Los expertos creen que no

Aunque los esfuerzos en la lucha contra la ciberdelincuencia y los arrestos de ciberdelincuentes reciben amplia cobertura, los expertos coinciden en que suele apresarse y encarcelarse a las denominadas "mulas", es decir, los intermediarios que realizan las transferencias, y no a los barones del delito.

"Normalmente, cuando se trata de phishing se arresta a los blanqueadores de dinero en lugar de a los que diseñan los mensajes engañosos de correo electrónico. En uno de los casos de mayor envergadura hasta ahora en el Reino Unido, el principal responsable huyó a Rusia mientras se detenía a las "mulas" de menor importancia. Fue una investigación muy costosa que tuvo poca difusión", recuerda Peter Sommer.

"En general, es fácil seguir la pista a las transacciones internacionales. Los recopiladores de datos de cuentas venden bloques de información con cierto nivel de garantía a través de sitios Web encubiertos, por lo que son difíciles de rastrear. En consecuencia, sus compradores tienen que asumir riesgos para convertir la información en dinero contante, por ejemplo, a través de retiradas de efectivo, cargos en tarjetas de crédito o fraudes crediticios; para ello, contratan a su vez a mulas prescindibles que de hecho son los que corren el mayor riesgo de ser arrestados. El dinero se blanquea en subastas falsas y casinos".

4205 5622350479 658. 7895200.02. 33695 454868.45 5
48 4528782

45 4582 688.54 58 89 8 488.5545 6896

44 822 656

4568 45 4582 688.54 58

486 86484 8 8

6541215.23. 5656

565.369 21 4477787 4651

546 78952

5

65271

7894152 02 30

"Los ataques DDoS casi siempre terminan en extorsión y deben tratarse de ese modo, atrapando a los responsables justo cuando se paga el rescate. Identificar a los autores de los ataques resulta demasiado difícil, así que la carrera armamentista entre agresores y defensores proseguirá".

Paulo Lima, abogado criminalista de Sao Paulo, está de acuerdo en que los cibermafiosos siguen sueltos debido a la lentitud de las fuerzas de seguridad para adaptarse y seguir los pasos de esta amenaza creciente y cada vez más eficaz:

"Son pocos los casos en los que se ha arrestado a los ciberdelincuentes con prontitud pero, en general, eran autores de pequeños ataques. Los responsables de las grandes operaciones nunca han sido apresados. Normalmente el sector público se ha limitado a aplicar paños calientes, atacando el síntoma y no la enfermedad: el sistema legal está anticuado y las fuerzas de seguridad carecen por completo de preparación".

Los ciberdelincuentes, protegidos frente a la ley

Atrapar a los cibermafiosos es todavía más difícil cuando están blindados frente a la ley por simpatías políticas.

Como explica Eugene Spafford: "La conducta delictiva todavía recibe amparo político. Por ejemplo, los ataques de denegación de servicio de Myanmar contaron con el apoyo de Europa Oriental y Rusia. Rusia y China son especialmente contrarios a cooperar con las fuerzas de seguridad extranjeras por motivos de reputación e inteligencia".

Alana Maurushat cree que es un caso de apoyo mutuo: "La conducta delictiva siempre ha recibido el amparo político de los gobiernos. Es un arma de doble filo. Con bastante frecuencia, los que poseen la experiencia y los conocimientos técnicos que los gobiernos necesitan para manejar las tareas con éxito son piratas informáticos. Por lo que yo he visto, los piratas informáticos llevan varios sombreros: algunos blancos, otros negros, muchos grises".

La escasez de ciberpolicías: la falta de conocimientos y formación de policías y tribunales impide progresar

Los expertos coinciden en que los ciberdelincuentes también son inmunes al arresto por la incapacidad de la policía de seguir el ritmo de la era digital.

A menudo Internet contiene las pruebas que podrían servir para detener a los ciberdelincuentes. Sin embargo, es frecuente que se minimice o se descarte el uso de tecnología de rastreo digital y análisis forense porque los implicados en el proceso, desde las investigaciones hasta el juicio, carecen de formación sobre cómo desenterrarla y aprovecharla exhaustivamente.

"Ahí fuera hay montañas de pruebas digitales; el problema es que no hay suficientes investigadores, fiscales y jueces bien formados que las utilicen con eficacia. Con el uso cada vez más extendido de los ordenadores personales y la banda ancha, desde cualquier equipo pueden encontrarse fácilmente pruebas directas e indirectas.

2 En el momento de la entrevista, McAfee estaba en el proceso de adquisición de Secure Computing

Caso real **Los ataques de Myanmar y la protección política**

En julio de 2008, los sitios Web de la Voz Democrática de Birmania (Democratic Voice of Burma, DVB) en Oslo y de Mizzima News en Nueva Delhi recibieron ataques DDoS que los mantuvieron cerrados durante varios días. En agosto se desactivaron y cerraron dos foros comunitarios, Mystery Zillion y Planet Myanmar, y el 17 de septiembre sufrieron ataques similares The Irrawaddy, DVB y New Era Journal en Bangkok.

Se cree que estos ataques concertados fueron coordinados por el gobierno birmano en previsión del primer aniversario de la Revolución del Azafrán, la protesta pacífica de monjes budistas, monjas y estudiantes contra la opresión del régimen militar. Todos los sitios Web eran simpatizantes de los monjes. Parece que todos los ataques se originaron básicamente en China y Rusia, principales partidarios diplomáticos de la Junta (gobierno militar) y lugares donde se insinúa que la Junta ha recibido formación técnica.

Pocos delincuentes tienen la capacidad técnica para no dejar huellas digitales o borrarlas", asegura Peter Sommer.

"En el Reino Unido, los casos complejos suelen investigarse a fondo, ya que hay un pequeño núcleo de policías enormemente competentes en investigaciones electrónicas. El problema es que la mayoría de sus compañeros todavía tienen que aprender dónde están las pruebas, cómo acceder a ellas y utilizarlas, y cómo interaccionar con los investigadores forenses".

Paulo Lima también secunda la idea de que la ciberpolicía tiene que conocer mejor los tecnicismos concretos de la ciberdelincuencia. En Brasil, aunque se han realizado intentos específicos para abordar el problema, en su mayoría, las investigaciones corren a cargo de funcionarios con medios insuficientes para comprender las complejidades de los delitos basados en Internet:

"En algunos estados, como Río de Janeiro y Minas Gerais, el fiscal del distrito tiene oficinas especializadas. En el resto, la investigación la realizan indistintamente todas las fuerzas de seguridad, en general policías sin la formación adecuada para luchar con eficacia contra este tipo de delito".

Matthew Bevan, ex-hacker, opina que el reto está en reclutar a gente con el perfil técnico correcto: "No creo que las fuerzas de seguridad estén preparadas para enfrentarse a los ciberdelincuentes; siempre ha sido así, ya que las personas a las que les gusta la informática y que reúnen los conocimientos adecuados buscan trabajo en ese campo, no en las fuerzas de seguridad. Es rarísimo que un especialista en TI quiera entrar en la policía. Por lo tanto, las fuerzas de seguridad carecen de las aptitudes necesarias para entender la ciberdelincuencia y saber qué buscar. Un ejemplo sencillo sería una nueva tarjeta USB que parece un cable partido pero que en realidad tiene capacidad para 4 GB de datos: la policía no la reconocería".

No son sólo las fuerzas de seguridad de primera línea los que se las ven y se las desean para localizar a los infractores, sino que, en los casos en que se dicta una sanción, la falta de conocimiento de los tribunales también amenaza la imposición de multas y condenas justas.

Por otro lado, tradicionalmente las penas se han basado en la cuantía de los daños materiales, que permiten ver el impacto real del delito. Sin embargo, con la ciberdelincuencia puede ser mucho más difícil averiguar el alcance del perjuicio ocasionado. Una de las dificultades de las fuerzas de seguridad es conseguir que las víctimas se involucren, ya sea porque no se dan cuenta de que han sido víctimas de un ataque, o bien porque, especialmente en el caso de las empresas, no quieren admitirlo.

Vijay Mukhi, Presidente de la Fundación para la Tecnología y la Seguridad de la Información (FIST) en India declara: "Este año la ciberdelincuencia se ha convertido en un gran problema en India. Aun así, ni políticos ni magistrados saben cómo enfrentarse a él y, de hecho, pocos de ellos utilizan alguna vez Internet. La policía es reacia a aceptar casos porque son muy difíciles de llevar a los tribunales. La ley india de TI del año 2000 contiene algunas disposiciones importantes, pero sólo se han traducido en un procesamiento satisfactorio, el de unos estafadores de tarjetas de crédito. En general, el fraude y el suministro de secretos comerciales son delitos civiles y, por lo tanto, no los investiga la policía. Kingfisher Airlines perdió recientemente

205 5622350479 658. 7895200.02. 33695 454868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656 546 78952 565.369 21 4477787 4651

cuatro o cinco millones de dólares por robo de tarjetas de crédito. Después de Kingfisher, ninguna otra compañía aérea ha denunciado a la policía fraudes similares porque no ocurrió nada".

Mary Kirwan también comenta: "A jueces y miembros del jurado les abruma la jerga tecnológica. Hay programas formativos en Canadá e Irlanda, pero una vez más el problema es la diferencia entre los que saben de tecnología y los que no. Además, los jueces deberían recibir formación para ser mucho más especializados en cuestiones de tecnología y seguridad tecnológica".

El profesor Peter Sommer añade: "En los últimos tiempos, los tribunales del Reino Unido utilizan mejor a los expertos; por ejemplo, las normas para procedimientos penales permiten que los expertos de la acusación y la defensa lleguen a un acuerdo sobre asuntos consensuados, como el modo en que funciona la tecnología y, en ocasiones, sobre la cronología de los acontecimientos. No obstante, todavía no ha entrado en funcionamiento el plan del Consejo de Profesionales Forenses para acreditar a expertos. Los criterios de evaluación deben ser flexibles en un terreno que evoluciona con tal rapidez, pero esto no hace sino aumentar los gastos de la acreditación, en especial si ésta ha de tener algún valor. Quizá sea necesario hacerla obligatoria".

Además, igual que en el mundo real, las víctimas tienen que hacer más para protegerse, especialmente cuando se trata de preservar pruebas. Las empresas necesitan programas de preparación forense; las personas necesitan formación básica y asesoramiento.

La empresa privada capta a los ciberespías

En los casos excepcionales en los que la policía está debidamente adiestrada para hacer frente a los desafíos técnicos propios del negocio de la ciberdelincuencia, las gratificaciones e incentivos se reparten mal y minan la moral.

"Las recompensas a la labor policial se otorgan a los altos rangos, no a los especialistas de primera línea; por ejemplo, algunos de los mejores investigadores digitales siguen siendo detectives o sargentos", comenta Peter Sommer.

Normalmente, ésta es la razón de que la empresa privada logre atraer a los ciberpolicías con la promesa de un salario más alto, lo que significa perder la inversión y dejar un vacío de experiencia imprescindible.

Caso real **Caso omiso de los expertos electrónicos**

En enero de 2007, Julie Amero, profesora suplente en Connecticut, fue condenada por cuatro cargos de atentado contra la integridad moral de menores porque sus alumnos del colegio estuvieron expuestos a imágenes pornográficas que aparecieron en la pantalla durante una clase de informática en 2004.

Los expertos en Internet concluyeron que Amero fue víctima de las circunstancias y que todo se debió a un malware malicioso que se activó espontáneamente; pudo hacerlo porque los filtros de Internet del colegio no funcionaban bien ese día.

Según el testigo experto de la defensa, en el primer juicio a los abogados no se les permitió presentar pruebas para corroborar esta teoría.

La sentencia se retrasó cuatro veces por falta de pruebas y por la incapacidad de evaluar el caso debidamente. Al final, la condena fue rechazada en junio de 2007 y se concedió un nuevo juicio. Aún no se ha fijado la fecha.

Caso real **La delgada línea entre ciberpolicía y delincuente**

En 2003, el pirata informático Brian Soledo fue sentenciado a nueve años en prisión por intentar robar datos de tarjetas de crédito en la cadena de hardware Lowe en EE. UU. La verdad es que había intentado abandonar el plan, pero se vio obligado a llevar a cabo el atraco on line por las amenazas que recibió del comprador de las tarjetas de crédito, ya apalabradas.

En agosto de 2008 se descubrió que el comprador, que trabajaba con el nombre de SoupNazi, era Alberto González, de 27 años y en aquel momento a sueldo de la policía federal. Fue arrestado en Miami en posesión de más de 20.000 dólares en efectivo.

Las autoridades admitieron que González trabajaba como informador en una investigación independiente sobre piratería informática para el servicio secreto estadounidense. Utilizaba la información de su investigación para ayudar a sus cómplices a eludir el arresto.

Alana Maurushat, comenta: "La policía local y estatal canadiense, estadounidense y australiana encuentra extremadamente difícil fichar a ciberpolicías, a menudo a causa de pequeños escollos, como el requisito de patrullar la calle durante siete años o la necesidad de estar en forma. Una vez instruidos, a menudo los capta la industria por salarios muy superiores".

También ha habido algún caso de ciberpolicías ya formados atraídos por grupos delictivos clandestinos. Por lo tanto, las fuerzas policiales deben garantizar una trayectoria profesional clara a los agentes especializados en la lucha contra la ciberdelincuencia.

No obstante, aunque no hay duda de que es fundamental impartir formación especializada para ciberespías, también es necesario equilibrar su técnica exclusiva con la instrucción policial básica para que dispongan de aptitudes e instintos completos en lugar de centrarse únicamente en la tecnología.

Tal y como advierte Mary Kirwan: "No deberíamos encerrar en un gueto a las fuerzas de seguridad y dejarnos llevar por la mística de la tecnología en perjuicio de las técnicas policiales tradicionales. Aunque el medio sea otro, hablamos de un delito y sigue tratándose de dinero. Por lo tanto, las técnicas tradicionales –utilizar informadores, reunir pruebas, pensar de forma creativa para entender la mentalidad de los delincuentes– son todavía necesidades prioritarias y sigue haciendo falta pericia para comprender y practicar la ingeniería social".

¿Ciberpolicías de facto? El papel crucial de los ISP en las investigaciones sobre ciberdelincuentes

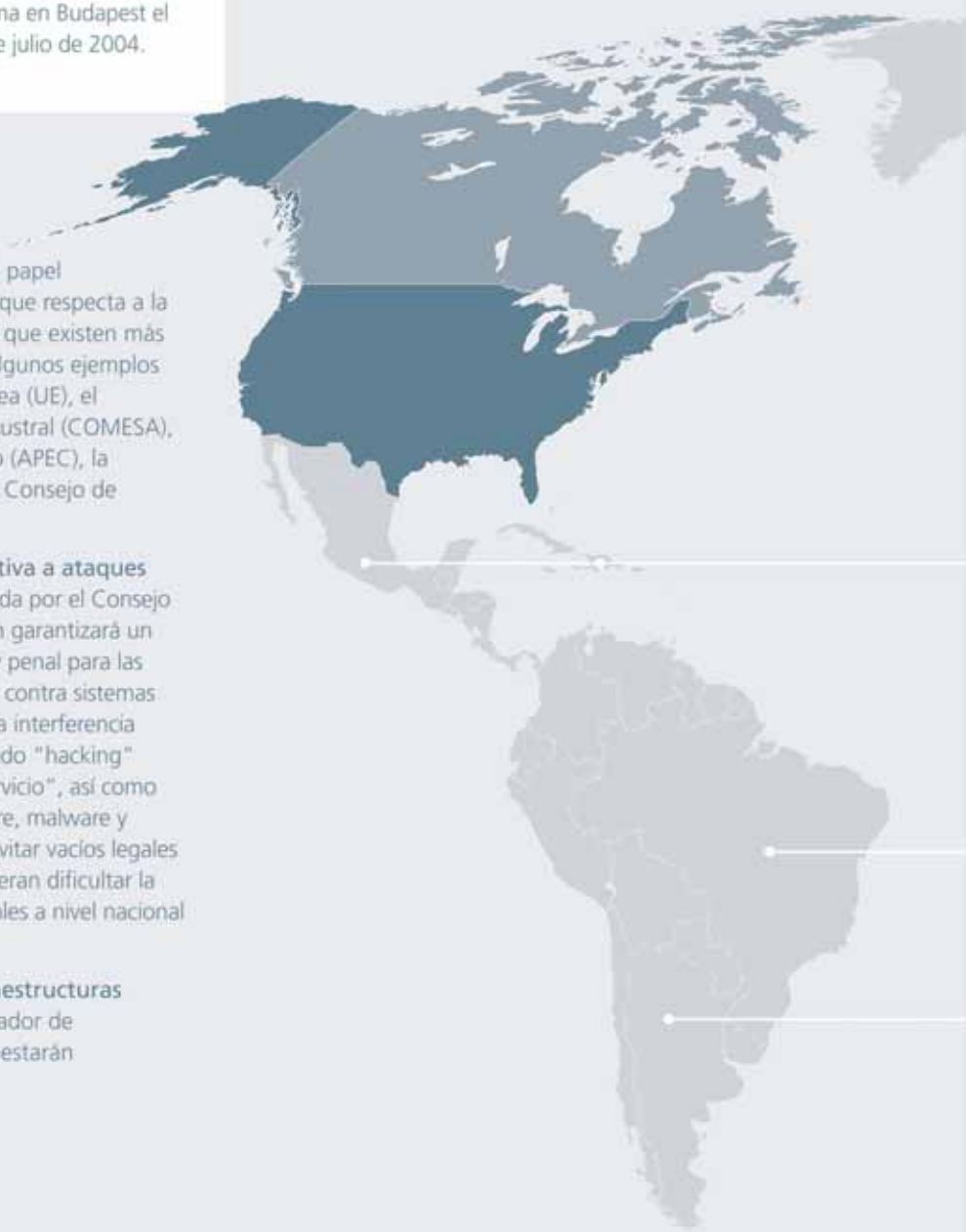
Internet no se ha regulado nunca del mismo modo que, por un lado, los medios de comunicación tradicionales y, por otro, los bancos, servicios financieros, fábricas de municiones y otros sectores– todas ellas actividades que pueden causar potencialmente graves perjuicios a los intereses básicos de la sociedad. Sin embargo, Internet es tan crucial como el primero, como medio de comunicación, y tan capaz de causar daños como el último.

Los expertos coinciden en que hoy en día los principales ciberpolicías son en realidad los ISP. Muchos timadores son atrapados por discutir sus planes en mensajes de correo electrónico no cifrados, lo cual, cuando hay una autoridad legal capacitada, ha demostrado tener un valor incalculable en los interrogatorios.

Los ISP y los demás intermediarios, como las agencias de transferencia de dinero, pueden tener un enorme impacto en el éxito de las investigaciones y, por lo tanto, deben participar en la lucha contra la ciberdelincuencia.

CAPÍTULO TRES
Cooperación internacional. ¿Un mito o una posibilidad?

Actualmente, el Convenio sobre la Ciberdelincuencia del Consejo de Europa es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional). Adoptado por el Comité de Ministros del Consejo de Europa en su sesión nº 109 del 8 de noviembre de 2001, se presentó para su firma en Budapest el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.



Convenio sobre la Ciberdelincuencia. Estado actual de ratificaciones

Las acciones a nivel regional también juegan un papel importante. Esto tiene especial relevancia en lo que respecta a la criminalización de contenidos ilícitos, área en la que existen más similitudes a nivel regional que a nivel global. Algunos ejemplos de intentos a nivel regional son: la Unión Europea (UE), el Mercado Común para África Oriental y África Austral (COMESA), el Foro de Cooperación Económica Asia-Pacífico (APEC), la Organización de Estados Americanos (OAS) y el Consejo de Cooperación del Golfo (GCC).

1. **CE, Decisión 2005/222/JAI del Consejo relativa a ataques contra los sistemas de información,** adoptada por el Consejo de Europa el 17 de enero de 2005. La Decisión garantizará un nivel mínimo común de aproximación de la ley penal para las formas más significativas de actividad delictiva contra sistemas de información, tales como el acceso ilícito o la interferencia ilícita en datos y sistemas. Esto incluye el llamado "hacking" (piratería) y los ataques de "denegación de servicio", así como la difusión de código malintencionado, spyware, malware y virus. Esta aproximación es deseable a fin de evitar vacíos legales en las leyes de los Estados miembros que pudieran dificultar la respuesta de las autoridades judiciales y policiales a nivel nacional ante estas crecientes amenazas.

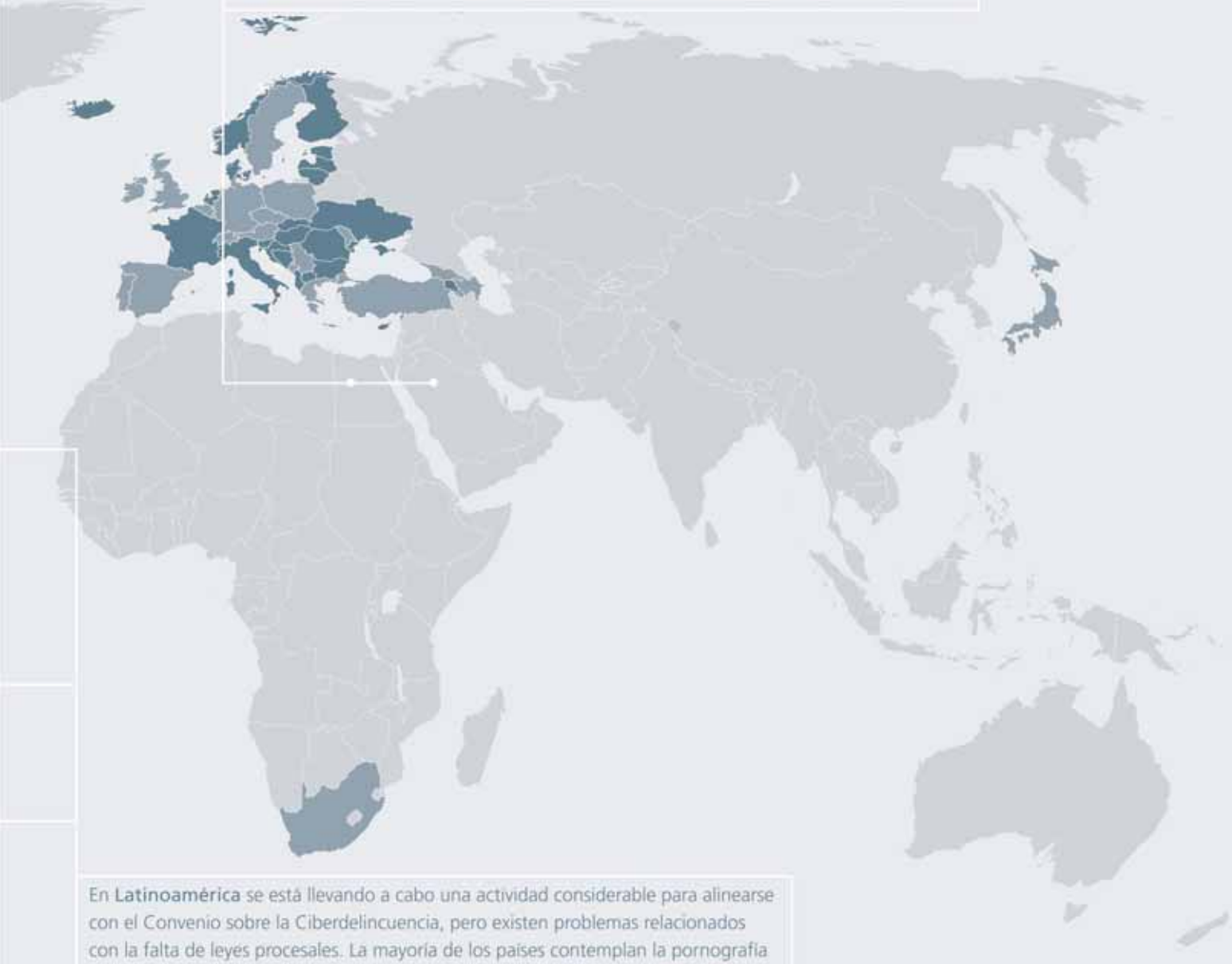
   Programa Europeo de Protección de Infraestructuras Críticas (DG JLS): se ha redactado ya un borrador de la Directiva, pero los criterios y normativas se estarán desarrollando hasta final de 2008.

2. **Otras iniciativas del grupo europeo**
   Subgrupo de Delitos Tecnológicos del G8
   Grupo EuroSCADA
   Grupo Gubernamental Europeo CERT
   Foro del Equipo de Respuesta a Emergencias y Seguridad

3. **http://www.virtualglobaltaskforce.com/. La Virtual Global Taskforce (VGT)** está constituida por fuerzas policiales de todo el mundo que, trabajan conjuntamente contra el abuso infantil a través de Internet.

Algunas regiones, especialmente las **árabes**, consideran que no se ha contado con ellos para el desarrollo del Convenio sobre la Ciberdelincuencia y prefieren establecer sus propios instrumentos regionales en lugar de adherirse a éste. Aun así, en la mayoría de los casos, dichos instrumentos se mantienen en la línea del Convenio.

Los **estados del Golfo Pérsico**, por su lado, han optado por preparar sus propias leyes, tomando como modelo el Convenio sobre la Ciberdelincuencia. Emiratos Árabes Unidos fue el primer país que decretó una ley global sobre ciberdelincuencia entre los estados del Golfo Pérsico. Esta ley ha funcionado bien contra la ciberdelincuencia en el país y ahora se planea extender la ley a otros estados del Consejo de Cooperación del Golfo (GCC).

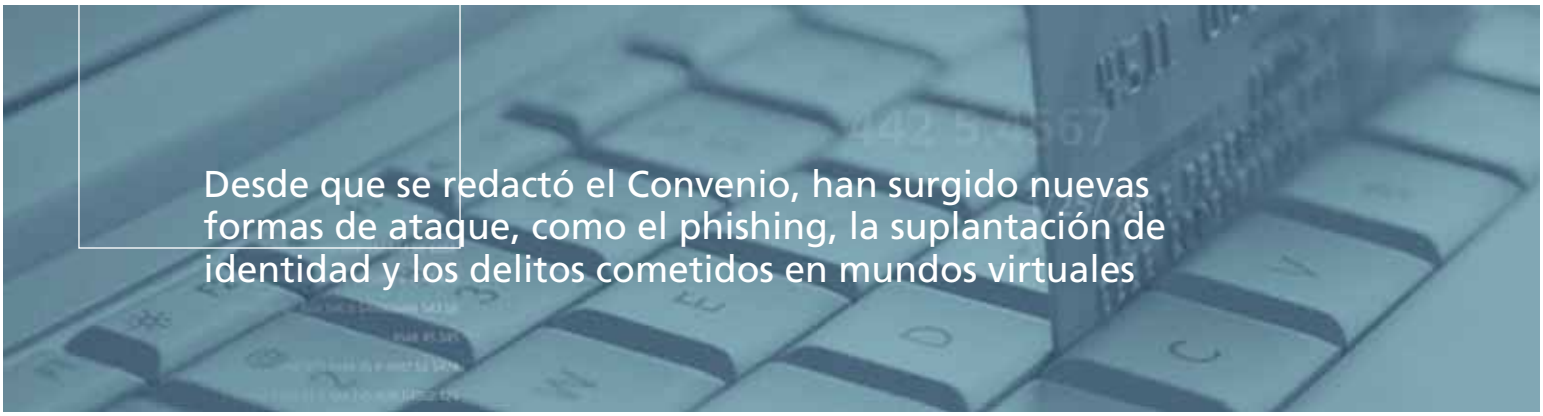


En **Latinoamérica** se está llevando a cabo una actividad considerable para alinearse con el Convenio sobre la Ciberdelincuencia, pero existen problemas relacionados con la falta de leyes procesales. La mayoría de los países contemplan la pornografía infantil y los ataques a sistemas, pero la eventual ilegalidad de la redes de bots no está del todo clara. A Costa Rica y México se les ha solicitado la adhesión al Convenio, mientras que Argentina y la República Dominicana ya tienen legislación al respecto. Brasil está preparando una legislación sobre ciberdelincuencia que, aunque está en fase de debate, se presume que será "muy dura".

Países que han **ratificado** el Convenio sobre la Ciberdelincuencia

Países que han **firmado** el Convenio sobre la Ciberdelincuencia

Países que todavía no han participado en el Convenio sobre la Ciberdelincuencia



Desde que se redactó el Convenio, han surgido nuevas formas de ataque, como el phishing, la suplantación de identidad y los delitos cometidos en mundos virtuales

La adopción de estándares internacionales tropieza con el fracaso en la coordinación de los países

45 países en total se han adherido al Convenio sobre Ciberdelincuencia hasta la fecha, pero cuando han transcurrido siete años desde su creación, sólo la mitad lo han ratificado.

El Convenio se percibe desarrollado principalmente por Occidente y por todos los Estados no miembros que se han adherido. EE. UU. es el único país que lo ha ratificado completamente. Hay algunas excepciones notables.

A pesar de ello, Marco Gercke, profesor de la Universidad de Colonia y experto en el Convenio sobre la Ciberdelincuencia para Naciones Unidas y para el Consejo de Europa, aclara que se está demostrando que se trata de un modelo de buena coordinación: "Hay que analizar detalladamente las circunstancias de cada país o región para ver el éxito del Convenio. Por ejemplo, Alemania aún no lo ha ratificado sólo por el hecho de que le queda una disposición que corregir en su propia legislación nacional".

En líneas generales, parece que el modelo funciona, pero algunos países todavía están demasiado centrados en sus problemas y prioridades nacionales para pensar en el beneficio global a nivel internacional.

Peter Sommer indicó a este respecto: "El tratado sobre ciberdelincuencia del Consejo de Europa funciona razonablemente bien, aunque algunos países aún no lo reconocen. Proporciona definiciones estándar, asistencia legal mutua y procedimientos de intercambio de pruebas, y facilita la extradición. Las naciones de Europa Oriental son menos cooperativas, especialmente Rusia. Asisten a las reuniones (por ejemplo, la reunión del G8 hace diez años) y hacen promesas, pero luego no las cumplen. Han cooperado con más intensidad en lo que se refiere a imágenes de abusos a menores. Dejan claro que no pueden priorizar el fraude contra extranjeros. Nigeria lo hizo mal en el pasado, pero ahora está mejorando, especialmente en el refuerzo de la investigación científica policial".

Uno de los mayores problemas en la elaboración de leyes contra la ciberdelincuencia es el consenso para armonizar las definiciones. Ser capaces de llegar a un acuerdo sobre que un delito X sea lo mismo en el estado A y en el estado B es un desafío de enormes proporciones. Sin embargo, es esencial para la extradición, así como para el intercambio de pruebas y la jurisdicción.

El Convenio sobre la Ciberdelincuencia ha servido de ayuda, pero tiene numerosas cláusulas de escape, lo que significa que la sincronización real no se ha alcanzado.

Esta falta de armonización afecta también a los informes comparativos y las estadísticas, por lo que la escala y el impacto globales de la ciberdelincuencia son difíciles de medir.

Las leyes no siguen el ritmo de la ciberdelincuencia

Con siete años de antigüedad, el Convenio muestra hoy día signos de haber quedado obsoleto para enfrentarse de forma eficaz a los ataques de la era moderna que tienen lugar en el cibermundo.

Desde que se redactó el Convenio, han surgido nuevas formas de ataque, como el phishing, la suplantación de identidad y los delitos cometidos en mundos virtuales. Estos tipos de ataques no se recogen en el Convenio, que tampoco ofrece ayuda específica sobre cómo tratarlos.

Caso real **Atraco en el Habbo Hotel**

La ciberdelincuencia en los mundos virtuales es un problema cada vez mayor. El mundo de los juegos virtuales está comenzando a acusar problemas del mundo real: suplantación de identidad y activos virtuales, extorsión e incluso ataques terroristas. Esto es especialmente evidente en países como Corea del Sur, donde 30 de los 46 millones de habitantes participan en redes sociales como CyWorld, y la policía está descubriendo muchos ataques provenientes de China.

En noviembre de 2007, un adolescente holandés fue arrestado por robar presuntamente muebles virtuales por valor de 4.000 € en Habbo Hotel, una red social y sitio Web de juegos en 3D.

Otros cinco adolescentes también fueron interrogados en relación con el caso. Parece ser que el grupo creó sitios Web de Habbo falsos y convencieron a los jugadores para que los visitaran. De esta forma, consiguieron los nombres de usuario y las contraseñas que posteriormente utilizaron para acceder a las cuentas reales y robar los muebles virtuales. Los créditos para comprar muebles en la primera Web se compraron utilizando dinero real.

La policía es consciente de que necesitará mejorar su capacidad para enfrentarse a estos delitos virtuales en el futuro.

Esto dificulta el trabajo de los fiscales y vuelve a poner de manifiesto el problema de la extradición cuando los distintos países no se ponen de acuerdo en la definición de un delito y en la respuesta que se debe tener ante él.

Aunque estos delitos pueden quedar recogidos en disposiciones más generales, se facilitaría la labor de los fiscales si estuviesen tipificados. Entonces ¿necesitamos otro Convenio sobre la Ciberdelincuencia?

Marco Gercke no ve la necesidad de una estructura completamente nueva, aunque reconoce que la ley lleva un claro retraso. Es necesario que se lleven a cabo revisiones y actualizaciones periódicas con el fin de garantizar que tanto las leyes como las investigaciones avanzan al mismo ritmo que la ciberdelincuencia:

"Aunque no necesitamos un nuevo modelo de ley, podríamos haber añadido protocolos para los nuevos problemas. Creo que si la legislación actual no contempla los nuevos timos, deberían tomarse las medidas necesarias. En un estudio de 2007 del Consejo de Europa sobre suplantación de identidad, insistí en que el Convenio no contempla la transferencia de identidades obtenidas (suplantación de identidad). Este problema debería abordarse en el futuro".

"El Convenio fue desarrollado antes de final de 2001 y desde entonces han cambiado muchas cosas. Esto no sólo tiene relevancia sobre el derecho penal sustantivo, sino también sobre los instrumentos procesales necesarios. En algunos países como EE. UU. ya se están utilizando nuevos instrumentos de investigación, como los registradores de pulsaciones; por ejemplo, el software "Magic Lantern", y de identificación, como la herramienta "CIPAV" (Computer and Internet Protocol Address Verifier, verificador de protocolos informáticos y de Internet), ambos del FBI, pero éstos no se mencionan en el Convenio".

La cooperación internacional proporciona éxitos a los ciberdelincuentes ¿Por qué falla la comunicación entre las fuerzas de seguridad?

Como comenta Ferenc Suba, del equipo de respuesta de emergencias informáticas (CERT), en Hungría: "El Convenio sobre la Ciberdelincuencia del Consejo de Europa es una buena guía para legislar. Pero ahora, las necesidades operativas claman la necesidad de nuevas leyes".

"De hecho, la acción de las fuerzas de seguridad tradicional está fuertemente sujeta a las fronteras físicas nacionales. Estas distinciones normalmente no existen en Internet, por lo que para los organismos locales se hace muy difícil la aplicación de la ley".

Mary Kirwan señala que mientras los ciberdelincuentes están organizados y trabajan rápido en colaboración para asegurarse el éxito, la acción de las fuerzas de seguridad internacionales se queda corta incluso a simples efectos de comunicación:

"La ley es irrelevante para la mayoría de los ciberpiratas; ellos pueden actuar desde cualquier sitio. La realidad en lo que se refiere a la acción

205 5622350479 658. 7895200.02. 33695 454868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656 546 78952 565.369 21 4477787 4651

policial es que si queremos que actúen tan rápida y eficazmente como la comunidad internacional de ciberdelincuentes, tenemos que proporcionarles las herramientas necesarias. Si los piratas comparten toda la información que poseen, mientras que las empresas y los gobiernos no comparten nada, no es difícil dilucidar quién lo está haciendo mejor. Cuando una banda de delincuentes necesita, por ejemplo, descifrar un documento, se ponen en contacto con la comunidad y reciben una respuesta rápidamente".

En casos contados, la cooperación internacional ha capturado con éxito a los ciberdelincuentes, pero los expertos son escépticos sobre el impacto que está teniendo entre éstos, que se movilizan rápidamente y siguen avanzando.

"Mi experiencia, no sólo con tarjetas de crédito y otros instrumentos similares, sino en sitios Web 'underground' que trafican con software crackeado, herramientas para piratear e imágenes indecentes de menores, me lleva a afirmar que siempre hay varios sitios Web que compiten sobre cada 'tema' y aunque en un momento dado, uno de ellos puede dominar, si éste desaparece o se ve comprometido por alguna razón, los otros se impondrán", afirmó Peter Sommer.

La reciente operación secreta del FBI, en colaboración con otros cuerpos policiales, contra un foro de delincuentes denominado "Dark Market" (literalmente, "Mercado oscuro") se considera solamente una gota en el océano, y aunque es alentador pensar que es posible coordinar los esfuerzos, no es, ni con mucho, lo habitual.

Alana Maurushat comenta: "Cada cinco años se realiza una gran redada como ésta y la victoria de los buenos se celebra ampliamente. Aunque la operación ha sido importante, el foro Dark Market no es más que uno de los muchos de estas características. No tengo constancia de que se haya arrestado a ningún extranjero en esta operación, especialmente de países de los que procede una gran parte de este tipo de crimen organizado, particularmente de los países de Europa del Este. Creo que esto no ha tenido la más mínima incidencia en lo que se refiere al fraude on line. Dicho esto, debemos felicitar al FBI y a la Comisión Federal de Comercio (FTC) por esta operación, así como por los otros muchos arrestos realizados recientemente en relación a círculos de spam y dueños de redes de bots. Sería bueno que los organismos equivalentes de otros países también intensificaran sus investigaciones".

Caso real **Dark Market: ¿un éxito internacional o la punta del iceberg?**

En octubre de 2008, una operación policial coordinada internacionalmente acabó con el arresto de 56 miembros de una red criminal transnacional que se utilizaba para comprar y vender información financiera robada. El foro de intercambio de datos de tarjetas de crédito ("carding") alojado en el sitio Web Dark Market había atraído a más de 2.500 miembros registrados hasta su cierre.

Además de los arrestos, la policía bloqueó las cuentas de las víctimas afectadas con el fin de evitar pérdidas económicas por valor de 70 millones de dólares debido a la suplantación de identidad.

El FBI dirigió una operación de dos años con la ayuda de la Unidad de Investigación de Delitos contra la Propiedad Intelectual y Delitos Informáticos del Departamento de Justicia de EE. UU., y la Agencia contra el Crimen Organizado (SOCA, Serious Organised Crime Agency) del Reino Unido, la policía nacional turca (KOM Department), la policía criminal federal de Alemania (Bundeskriminalamt) y la policía estatal de Baden-Württemberg (Landeskriminalamt Baden).

El Director Adjunto de la División de Delitos Informáticos del FBI, Shawn Henry observó: "En el mundo actual, en el que la tecnología se extiende rápidamente y donde los ciberdelitos se cometen instantáneamente desde cualquier parte del mundo, las fuerzas policiales tienen que ser flexibles y creativas en sus esfuerzos para la persecución de estos delincuentes. Gracias a la unión de fuerzas con otros organismos policiales internacionales, hemos conseguido y conseguiremos arrestar a estos individuos y desmantelar sus foros".

Sin comunicación global, la información está aislada y los problemas se multiplican exponencialmente

La ciberpiratería, la guerra y la delincuencia son problemas transnacionales, lo que conlleva enormes dificultades para las fuerzas de seguridad a la hora de investigar a los autores, obtener pruebas, negociar la jurisdicción entre las agencias de investigación y en los juzgados, y acordar las extradiciones.

En este momento, para que la acción policial de una autoridad nacional en relación a un delito transnacional sea eficaz, es preciso montar para cada caso una operación conjunta desde cero, un proceso que tiene un alto coste en tiempo y dinero. Existe la Interpol, pero no parece estar muy especializada en acciones policiales contra la ciberdelincuencia.

Como destaca Richard Clayton, del Laboratorio Informático de la Universidad de Cambridge en el Reino Unido: "La Interpol es un mecanismo de traspaso de faxes. Sus competencias propias en investigación son muy limitadas actualmente y no tiene vocación de liderazgo. Aunque sus mecanismos se pueden utilizar a efectos de coordinación, no establece prioridades por sí misma ni decide cuándo y dónde desplegar recursos de una forma más eficaz".

Por tanto, ahí esta la razón para crear una fuerza global especializada en investigación sobre ciberdelincuencia transnacional que vaya más allá de lo contemplado en el tratado y garantice la acción. Ayudaría a este objetivo el seguimiento y la coordinación de la ciberdelincuencia a través de las fronteras y la agilización en los tiempos de respuesta.

Continúa Clayton: "La idea básica es crear un organismo de coordinación central constituido por miembros con dedicación completa de todas las autoridades relevantes. Básicamente, tendría un doble papel: primero, contribuir a alcanzar el consenso o, cuando menos, un alto nivel de respaldo en cuanto a los delitos que se deben tratar; y en segundo lugar, ser capaz de actuar como nexo con las autoridades locales para proporcionar el apoyo logístico adecuado para determinadas operaciones y transmitir la capacidad o incapacidad para ayudar a garantizar que la planificación central es razonablemente eficaz. Saber si todo funcionaría en la práctica dependería de la capacidad de liderazgo del organismo coordinador, junto con el apoyo suficiente y visible de los políticos en los estados relevantes. Pero, si al menos existiese respaldo entre los integrantes del G8, sería más fácil conseguir el control de los principales nidos de delincuencia".

Sin embargo, dado el número de organismos burocráticos que ya están implicados en la ciberdelincuencia, quizás la prioridad sería racionalizar y coordinar las organizaciones existentes.

CAPÍTULO CUATRO
Pasos a seguir

A pesar de que el Convenio sobre la Ciberdelincuencia del Consejo de Europa actúa como modelo de legislación global allí donde no se ha adoptado directamente, y aunque la mayoría de las jurisdicciones relevantes ya cuentan con leyes al respecto, la legislación no es suficiente para reducir la ciberdelincuencia hasta niveles aceptables.

Cuando las leyes son demasiado específicas para la tecnología, se quedan obsoletas rápidamente, su eficacia depende en gran medida del éxito de las investigaciones y acusaciones correspondientes y se encuentran con el problema de la naturaleza transnacional de la ciberdelincuencia.

Se necesita una solución global que vaya más allá de las leyes penales.

Se debe animar a los países a llegar al máximo nivel de convergencia en la legislación, además de poner el máximo esfuerzo en la cooperación internacional.

La necesidad de un planteamiento colectivo y holístico para combatir la ciberdelincuencia

Los programas de alfabetización audiovisual para los consumidores no son suficientes para asegurar que los usuarios priorizan la seguridad sobre la comodidad o la consecución de sus objetivos a corto plazo

Los expertos recomiendan que se consideren e implementen los siguientes pasos tanto a nivel local como internacional:

- Incremento significativo de la **formación y los recursos disponibles para los ciberagentes, los fiscales y los jueces**, junto con la simplificación de los procesos de recogida de pruebas y acusación formal.
- Incentivos legales o de corregulación para los **proveedores de servicios de Internet (ISP)** para que sigan buenas prácticas en el diseño de redes y operaciones; incentivar a los ISP a cambio de trabajar con otros proveedores de servicios y con los clientes para mejorar los niveles de seguridad. También se debe animar a los ISP a colaborar más estrechamente con la policía como los guardianes de Internet.
- **Obligación de revelar brechas en la seguridad**. No podemos esperar que un mercado garantice la seguridad de sus productos y servicios sin la información necesaria que permita a los clientes medir los niveles de seguridad. Las nuevas normas de la UE son un primer paso, pero necesitan extenderse más allá del sector de las telecomunicaciones y ser examinadas a fin de garantizar que no se implantan sólo a modo de ejemplo y evitar el "cansancio" de los clientes ante los temas de seguridad.

  En EE. UU., existen medidas provisionales a nivel estatal para la notificación de fugas de datos. Decenas de estados han aprobado leyes diferentes. Se necesita un estándar sencillo y directo de notificación de fuga de datos para ayudar a las empresas a responder de forma coherente y sin complicaciones, así como para garantizar a los ciudadanos el máximo nivel de protección, independientemente del estado del que provengan. Además, las empresas que guardan información personal confidencial deberían cumplir un estándar de seguridad común para que se reduzcan las posibilidades de fuga de datos.
- Responsabilidad legal para **las empresas y organismos gubernamentales** cuando los clientes sufren pérdidas de seguridad relacionadas con Internet, excepto en los casos de clara negligencia por parte de los clientes.

  En concreto, a los bancos se les deben ofrecer fuertes incentivos legales y comerciales, para que introduzcan más tecnología de seguridad y mejores sistemas para la detección del fraude, o inevitablemente recortarán los presupuestos en seguridad, ahora que se ven obligados a luchar contra la falta de liquidez y la crisis económica. Una clara opción por la responsabilidad premiaría a los bancos que se toman en serio la seguridad, reduciría enormemente los problemas que han sufrido los clientes y, por lo tanto, incrementaría la tranquilidad y la confianza en las operaciones on line, vitales para que el comercio electrónico y la Administración electrónica funcionen en el futuro.
- **Formación continua para el consumidor**, a través de programas específicos. Sin embargo, los sistemas deben ser diseñados de forma que sea difícil para los usuarios cometer errores de seguridad. No podemos esperar que el usuario medio de Internet se convierta en un experto en seguridad. Los programas de alfabetización audiovisual para los consumidores no son suficientes para asegurar que los usuarios priorizan la seguridad sobre la comodidad o la consecución de sus objetivos a corto plazo.
- Responsabilidad limitada para los **proveedores de software** si no siguen buenas prácticas de seguridad en el diseño y el funcionamiento de sus sistemas. No podemos detener el avance del malware hasta que los sistemas operativos y las aplicaciones clave, especialmente los navegadores y los programas de correo electrónico, sean significativamente más seguros.
- Utilización del **poder de instigación de los gobiernos** para demandar estándares de seguridad en el software y en los servicios notablemente más altos; por ejemplo, incentivar las mejoras en seguridad que beneficiarán a los usuarios privados. Las autoridades gubernamentales encargadas de la protección de la información deberían seguir el ejemplo de la Agencia de Seguridad Nacional de EE. UU. a la hora de colaborar con las empresas de software para incrementar los niveles de seguridad del software de forma significativa.

COLABORADORES

EUROPA Y ORIENTE MEDIO

Dr. Ian Brown – Investigador en el Oxford Internet Institute, Universidad de Oxford, Reino Unido

El Dr. Ian Brown es investigador titular en el Oxford Internet Institute de la Universidad de Oxford y Catedrático honorífico en el London University College. Su labor se centra en cuestiones relativas a políticas públicas en materia de información e Internet, en particular, la privacidad, los derechos de autor y la democracia electrónica. También trabaja en ámbitos más técnicos, como la seguridad de la información, las redes y la informática en la asistencia sanitaria.

Es miembro de la junta de gobierno de las sociedades Royal Society of Arts y British Computer Society, y asesor de las organizaciones Privacy International, Open Rights Group, Foundation for Information Policy Research y Greenpeace. Ha sido consejero del Gobierno de Estados Unidos, JP Morgan, Credit Suisse, la Comisión Europea y la Oficina del Comisario de Información del Reino Unido.

En 2004, fue elegido como una de las 100 personas de mayor influencia en el desarrollo de Internet en el Reino Unido durante la pasada década.

Lilian Edwards – Profesora de Derecho de Internet en la Universidad de Sheffield, Reino Unido

Lilian Edwards está al frente de un programa de investigación y formación en la Universidad de Sheffield centrado en el derecho relacionado con Internet, la Web y las nuevas tecnologías.

Sus materias de interés giran principalmente en torno al derecho relacionado con Internet, la Web y las tecnologías de comunicación, desde una perspectiva europea y comparativa. En la actualidad, su trabajo de investigación se centra en el papel de los intermediarios y los proveedores de servicios de Internet, la protección de la información y la privacidad on line, la ciberdelincuencia y la ciberseguridad, la "Web 2.0" y la ley, IP digital y el comercio electrónico. Ha sido coeditora de dos ediciones de su libro *Law and the Internet* (El derecho e Internet) (la tercera edición está prevista para principios de 2009), que tuvo un gran éxito de ventas, y de una tercera colección de ensayos *The New Legal Framework for E-Commerce in Europe* (El nuevo marco jurídico del comercio electrónico en Europa). Su trabajo sobre la privacidad del consumidor on line obtuvo el premio Barbara Wellbery en 2004 a la mejor solución al problema de la privacidad y los flujos de datos internacionales. Es asesora de las organizaciones BILETA, ISPA y FIPR, y del grupo de defensa de los derechos on line. Además, ha sido consejera de la Comisión Europea y de la Organización Mundial de la Propiedad Intelectual (OMPI).

Matthew Bevan – Ex-pirata informático y consultor informático

Mathew Bevan es un pirata informático británico de Cardiff, Gales. En 1996 fue arrestado por perpetrar ataques de piratería informática contra redes del Estado en EE. UU. con el pseudónimo de Kuji. Tenía 21 años cuando se introdujo en los archivos del laboratorio de investigación de la Base Aérea Griffis en Nueva York. Se propuso demostrar una supuesta teoría de la conspiración relacionada con ovnis y para ello utilizó como única herramienta un Commodore Amiga cargado con un programa de manipulación telefónica, llamado Roxbox. Según el agente especial Jim Christy, que en la época trabajaba en la Oficina de Investigaciones Especiales de la Fuerza Aérea, fue uno de los dos piratas informáticos de los que se dijo que "estuvieron a punto de iniciar la tercera guerra mundial". En la actualidad dirige su propia empresa de consultoría informática.

Sharon Lemon – Subdirectora del área de Delincuencia Electrónica de la Agencia contra el Crimen Organizado (SOCA, Serious Organised Crime Agency), Reino Unido

La Subdirectora Sharon Lemon de la Agencia contra el crimen organizado (SOCA, Serious Organised Crime Agency) dirige los departamentos de delincuencia electrónica y técnicas delictivas.

Sharon comenzó su carrera en la Policía Metropolitana y ha prestado servicio en numerosos departamentos importantes del centro de Londres en todos los rangos. En 1999 pasó a formar parte de la Brigada Nacional contra el Crimen (NCS, National Crime Squad). Ha desempeñado varios cargos relevantes, incluido el de Directora del Equipo de Investigación contra las Armas de Fuego y la Pedofilia On Line (Firearms and the Paedophile On-Line Investigation Team)– precursor del Centro de Protección On Line y Contra la Explotación de Menores (Child Exploitation and Online Protection Centre). Asimismo, tuvo un papel fundamental en la formación de la Virtual Global Taskforce (VGT), una alianza internacional de agencias encargadas de la aplicación de la ley formada por Australia, Canadá, Interpol, el Reino Unido y Estados Unidos.

Hasta abril de 2006, Sharon dirigió la primera unidad de ámbito nacional responsable de la investigación de los delitos tecnológicos (National HiTech Crime Unit, NHTCU). Desde entonces ha desarrollado el departamento de delincuencia electrónica de la SOCA gracias al impulso de una serie de intervenciones alternativas para complementar las acciones judiciales tradicionales. Más recientemente, ha añadido a sus responsabilidades la de dirigir el Departamento de Técnicas Delictivas, encargado de desarrollar métodos innovadores de obstaculizar las actividades del crimen organizado aprovechando las debilidades de las redes criminales y anticiparse a las amenazas criminales futuras.

Bob Burls – Agente de la Unidad de Delitos Informáticos de la Policía Metropolitana de Londres, Reino Unido

La Unidad de Delitos Informáticos es un centro avanzado en relación con los delitos informáticos y la ciberdelincuencia en el marco de la Ley sobre el uso indebido de la informática (Computer Misuse Act) de 1990, en particular la piratería informática, la creación y propagación de virus con fines maliciosos y software de falsificación. La unidad incluye un agente especializado en el análisis forense informático y ofrece asesoramiento para la recuperación de pruebas informáticas a los agentes.

Peter Sommer – Profesor visitante del Grupo de Integridad de Sistemas de Información de la London School of Economics (LSE) y profesor asociado en la Open University, Reino Unido

Su principal área de interés en la investigación es la fiabilidad de las pruebas digitales, una materia que comprende la informática forense y el comercio electrónico. Ha prestado su colaboración en el diseño de los cursos orientados a las ciencias sociales de la LSE sobre la gestión de la seguridad de la información.

En la última legislatura fue asesor especialista del Comité de Investigación de Comercio e Industria de la Cámara de los Comunes del Reino Unido en su análisis de la política y la legislación del país en materia de comercio electrónico. Formó parte del estudio de previsión de la Oficina de Ciencia y Tecnología del Reino Unido, denominado Cyber Trust, Cybercrime (Confianza cibernética y ciberdelincuencia). Es miembro de varios paneles de asesoramiento del Gobierno del Reino Unido. Se han suscrito recientemente varios contratos de investigación para la Autoridad de Servicios Financieros del Reino Unido y el Plan de acción para una utilización más segura de Internet (Safer Internet) de la Comisión Europea. En la actualidad forma parte de la Red de excelencia europea FIDIS y es también miembro del Grupo de referencia (mecanismo de revisión) de otra iniciativa de la Comisión Europea, el proyecto PRIME.

Peter Sommer es examinador externo del Royal Military College of Science y asesor en diversos comités de seguridad y de otra índole dedicados a la ciberdelincuencia y las respuestas de emergencia. Ha sido asesor de Centrex, que imparte cursos de formación sobre delincuencia mediante el uso de altas tecnologías a los cuerpos de seguridad del Reino Unido, y de TWED-DE, un ejercicio financiado por el Departamento de Justicia de Estados Unidos para impulsar la formación sobre pruebas digitales. Ha impartido también seminarios a las fuerzas de seguridad del Reino Unido y Estados Unidos sobre pruebas en Internet y cuestiones de relacionadas con la inteligencia.

Formó parte del comité de programación de la conferencia anual sobre seguridad FIRST 2000 celebrada en Chicago.

Peter Sommer es asesor y analista de sistemas informáticos para destacadas empresas aseguradoras. Su primer encargo lo recibió en 1985 y entre los casos de los que se ha ocupado se incluyen el de los piratas informáticos Datastream Cowboy/Rome Laboratory, el caso de difamación en Internet Demon contra Godfrey, la "Operación Cathedral" de la National Cathedral School, la "Operación Ore" y otros muchos casos de delitos tan diversos como asesinato múltiple, falsificación, piratería de software, fraude bancario, duplicación de tarjetas de crédito y venta de secretos oficiales.

El miembro del Consejo asesor de la fundación "Foundation for Information Policy Research", un grupo de estudio con sede en el Reino Unido.

Richard Clayton – Laboratorio de Informática de la Universidad de Cambridge, Reino Unido

El Laboratorio de Informática de Cambridge es el departamento de informática de la Universidad de Cambridge. El Diploma en Informática de Cambridge fue la titulación del primer curso del mundo impartido en esta materia, y comenzó en 1953. Richard Clayton es un destacado investigador en seguridad y un veterano colaborador de los grupos de trabajo de políticas de seguridad en el Reino Unido.

Philip Virgo – Secretario General del EURIM, Reino Unido

Philip ha estado ligado al EURIM desde su refundación en enero de 1994. Fue el primer Director Ejecutivo y ocupa el cargo de Secretario General desde 1996. Ejerció además el cargo de Director Financiero de PITCOM entre 1982 y 2006, y continúa formando parte del consejo y del comité de programación. Fue asesor externo de la Unidad de Alta Tecnología del Barclays Bank (1983-89), Director de la campaña "Women in IT" (1989-92), asesor de tecnología de la información en el West London TEC (1991-2), asesor especialista del Comité de Información de la Cámara de los Comunes (1993-4), ha sido asesor estratégico del Instituto para los Sistemas de Información de Gestión (IMIS, anteriormente IDPM) desde 1993 y ha pertenecido a varios comités y juntas consultivas.

Matthew Pemble – Arquitecto y asesor de seguridad, Reino Unido

Matthew es un experimentado arquitecto de seguridad y director de operaciones y ha trabajado para un gran número de organizaciones no gubernamentales y comerciales internacionales, así como para el Gobierno del Reino Unido. Gran parte de su trabajo reciente ha estado centrado en combatir el fraude on line y otros ataques contra el comercio electrónico y los sistemas bancarios. Tras haber dirigido el Equipo de Respuesta a Incidentes de Seguridad de la Información para el Royal Bank of Scotland Group durante cinco años, en la actualidad ha vuelto al sector de la consultoría y trabaja en la unidad de seguridad de una empresa independiente de testing de software. Matthew es miembro de la junta de gobierno de la British Computer Society y miembro fundador del Instituto de Profesionales de Seguridad de la Información. Es Licenciado en Ingeniería por la Universidad Heriot-Watt de Edimburgo, posee el título de Ingeniero Europeo, de Ingeniero Colegiado y tiene las acreditaciones en seguridad de sistemas CISSP, CFE y CISM.

James Blessing – Director de Operaciones, Entanet International y miembro del consejo de la Asociación de Proveedores de Servicios de Internet (ISPA), Reino Unido

James Blessing es Director de Operaciones de Entanet International, parte del grupo de servicios de comunicación y distribución de tecnología de la información Entagroup. Profesional de TI innovador y creativo, cuenta con más de diez años de experiencia en el desarrollo de tecnologías de Internet y desempeña un papel activo en la industria de Internet. Ha sido miembro del consejo de la Asociación de Proveedores de Servicios de Internet (ISPA) desde 2004 y es jefe de la división de banda ancha de dicha asociación. James fue elegido para el consejo directivo del consorcio Enum Consortium del Reino Unido en marzo de 2008.

Peter Milford – Jefe de Asuntos Reguladores, NewNet, Reino Unido

Peter se incorporó a la empresa en abril de 2001 como miembro del equipo directivo de NewNet con responsabilidades en asuntos reguladores y empresariales.

Antes de incorporarse a NewNet, Peter desempeñó el cargo de Director Ejecutivo del proyecto Hampshire On-Line Learning, y con anterioridad fue Director de Recursos de Aprendizaje en St. Vincent College, Gosport.

Peter fue trasladado temporalmente a BT plc entre 1995 y 1997 para desarrollar servicios on line para la educación. Es Licenciado en Física y Tecnología de la Información, tiene un Máster en Derecho (Propiedad Intelectual), un diploma de posgrado en Tecnología para la Educación, es Físico Colegiado y miembro del Instituto de Física y de la British Computer Society.

5 5622350479 658. 7895200.02. 33695 454868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656 546 78952 565.369 21 77787 4651

54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568

4528782 45 4582 688.54 58 89 8 4568 44 822.656 54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656

Dr. Marco Gercke – Catedrático, Universidad de Colonia y experto en el Convenio sobre la Ciberdelincuencia para Naciones Unidas y el Consejo de Europa, Alemania

El Dr. Marco Gercke es abogado del Colegio de Abogados alemán. Enseña Derecho relacionado con la ciberdelincuencia y Derecho Penal Europeo en la Universidad de Colonia y es profesor asociado de Derecho Penal Internacional en la Universidad de Macao.

Marco es ponente habitual tanto a nivel nacional como internacional y autor de más de 50 publicaciones con la ciberdelincuencia como tema central. Sus principales áreas de investigación son los aspectos internacionales de la ciberdelincuencia (en especial los retos de la lucha contra la ciberdelincuencia y las respuestas legales) y el análisis del derecho comparativo en relación con la implementación de normas internacionales. Sus últimas investigaciones se han centrado en las actividades de las organizaciones terroristas en Internet, el robo de identidad, el blanqueo de capitales en Internet y las respuestas legales al uso creciente de tecnología de cifrado. Es Secretario del Departamento de Derecho Penal de la Sociedad Alemana para el Derecho y la Informática y miembro del grupo de expertos de alto nivel de la Unión Internacional de Telecomunicaciones. Asimismo, trabaja como experto para el Consejo de Europa, la Unión Internacional de Telecomunicaciones y otros organismos internacionales.

Marc Vilanova – Miembro de e-la Caixa CSIRT, España

Marc Vilanova es miembro del Equipo de Respuesta a Incidentes de Seguridad Informáticos (CSIRT) en e-la Caixa, sociedad participada íntegramente por "la Caixa", una de las Cajas de Ahorro más importantes de Europa. Además es miembro del Anti-Phishing Working Group (APWG) y del Forum for Incident Response and Security Teams (FIRST).

Anteriormente fue Consultor y Auditor de Seguridad TI en GMV Soluciones Globales Internet S.A., así como voluntario en el Instituto para la Seguridad y las Metodologías Abiertas (ISECOM).

Haim Vismonski – Abogado, Ministerio de Justicia, Israel

Haim Vismonski es abogado en el Ministerio de Justicia y Subdirector de la Oficina del Fiscal del Estado.

Ferenc Suba – Presidente, CERT, Hungría

Desde 2004, Ferenc Suba es el enviado especial del Ministerio de Informática y Telecomunicaciones; Director General de CERT-Hungría, el equipo de respuestas a emergencias informáticas del Gobierno, y Vicepresidente de la Junta de Gobierno de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

Erka Koivunen – Director del CERT-FI, Finlandia

Erka Koivunen es un profesional con gran experiencia en el campo de la seguridad de la información. En la actualidad está al frente del CERT-FI, la autoridad nacional de seguridad de la información finlandesa. Su área de experiencia es la respuesta a incidentes y la coordinación de repuestas.

ESTADOS UNIDOS

Eugene H. Spafford – Profesor de Informática en la Universidad de Purdue y Director Ejecutivo del CERIAS (Centro de Educación e Investigación en Seguridad y Garantía de la Información)

Eugene H. Spafford es una de las más antiguas y reconocidas eminencias en el campo de la informática. Sus logros han sido constantes como asesor y consultor jefe en cuestiones de seguridad, educación y política de ciberdelincuencia e informática en diversas empresas importantes, organizaciones de seguridad, instituciones académicas y agencias gubernamentales, entre las que se incluyen: Microsoft, Intel, Unisys, las Fuerzas Aéreas de EE. UU., la Agencia Nacional de Seguridad, la Oficina de Contabilidad del Gobierno, el FBI, la Fundación Nacional para la Ciencia, el Departamento de Energía y dos Presidentes de Estados Unidos. Con una experiencia de casi tres décadas como investigador e instructor, Spafford ha trabajado en ingeniería de programas, informática distribuida fiable, seguridad de redes y hosts, análisis forense digital, política informática y diseño de planes de estudio de informática. Varias de sus aportaciones llevan el calificativo de "por primera vez" en algunas de estas áreas.

Andrea Matwyshyn – Profesora adjunta de Derecho y Ética Empresarial, Wharton School, Universidad de Pensilvania

Andrea Matwyshyn es Profesora adjunta de Derecho y Ética Empresarial de la Universidad de Pensilvania. Sus investigaciones se centran en el ámbito de la seguridad de la información en las empresas y la gestión de riesgos, política y contratos, y la regulación de las tecnologías de la información. Algunos de los proyectos en los que trabaja actualmente incluyen la transformación de la estructura corporativa y su relación con la revolución de las tecnologías de la información y la vulnerabilidad de los datos, así como las estrategias legales para combatir los delitos relacionados con la información.

Anteriormente fue Profesora adjunta de Derecho en la Universidad de Florida y Directora Ejecutiva del Centro para la Investigación de la Información (CIR).

CANADÁ

Mary Kirwan – Directora Ejecutiva de Headfry Inc. y periodista, antigua fiscal contra la ciberdelincuencia

Mary Kirwan es una abogada internacional irlandesa y consejera de gestión de riesgos. Puede ejercer la abogacía en tres continentes y tiene una amplia experiencia en litigios y gestión directiva.

Durante varios años ha trabajado en pleitos comerciales en Toronto, Canadá, donde trabajó en algunos casos muy notorios de delitos comerciales e internacionales de los llamados "de guante blanco", evasión de impuestos y fraude. Además, ocupó el cargo de Fiscal Federal en la División de Escuchas Telefónicas y Blanqueo de Capitales del Departamento de Justicia de Toronto.

Posee una Licenciatura en Alemán e Irlandés (Gaélico) del Trinity College Dublin, y tiene varias certificaciones en seguridad de tecnologías de la información, incluida la CISSP. Tiene un Máster

68 44 822.656 546 78952 565.369 21
8.45 5 48 4528782 45 4582 688.54 58 89 8 4568

4528782 45 4582 688.54 58 89 8 4568 44 822.656 54868.45 5

en Negocios y Sistemas de Información de Gestión (MIS) por la Michael Smurfit Graduate School of Business del University College Dublin, Irlanda.

Mantiene una participación activa en las asociaciones de abogados Toronto Computer Lawyers Association y American Bar Association (ABA), en la sección de ciencia y tecnología (Science & Technology [SciTech]). Ha contribuido a numerosas publicaciones de la ABA en los campos de las tecnologías de la información, la seguridad de la información y la biotecnología. Es Presidenta del Comité de Pagos de Comercio Electrónico y Ciencia y Tecnología de la ABA, y miembro del equipo publicaciones de SciTech. Sus intereses particulares se centran en el ámbito de la banca electrónica, el fraude en pagos, los mercados de tarjetas de débito y cajeros automáticos a nivel mundial y en el desarrollo de métodos de pago.

En la actualidad, se encuentra finalizando dos libros para la ABA cuya publicación está prevista para enero de 2009: una guía para problemas legales relacionados con las tarjetas de crédito y los cajeros automáticos (*Guide to ATM and Debit Card Legal Issues*) para el mercado de masas de EE. UU. y otro titulado The Business Case for Data Security (El lado empresarial de la seguridad de los datos) para su publicación a nivel mundial.

Mary Kirwan es colaboradora habitual del periódico nacional canadiense *Globe and Mail* y ha publicado numerosos artículos sobre temas relacionados con la seguridad de la información, la gestión de riesgos, el cumplimiento normativo, el gobierno corporativo, la aplicación de la ley y los consumidores. Ha intervenido en conferencias en todo el mundo y aparecido en radio y televisión.

Leo Adler – Abogado penalista, Toronto

A pesar de que la actividad profesional de Leo Adler se centra de forma casi exclusiva en el derecho penal, también ha aparecido ante varios consejos, tribunales e investigaciones judiciales y ha sido contratado o consultado en casos relacionados con asuntos de extradición, juicios y vistas administrativas, y cuasi penales en Ontario, Québec, Manitoba, Nuevo Brunswick, los Territorios del Noroeste, Alberta y Columbia Británica, y hasta en la misma Corte Suprema de Canadá. Ha representado a personas arrestadas en EE. UU. en tribunales desde Florida hasta Michigan, Nueva York, California, Carolina del Norte y en otras partes, incluida Europa, y se le ha solicitado asesoramiento en una gran cantidad de casos. Gracias a su experiencia en casos de ADN y otros temas relacionados con el análisis forense, ha podido proporcionar asesoramiento a otros abogados.

Es profesor adjunto en la Osgoode Hall Law School de la Universidad de York, y participa en el Programa de Derecho Intensivo de dicho centro. Muchos de sus casos han sentado precedente legal.

Es miembro de las asociaciones de abogados: Criminal Lawyers Association, National Association of Criminal Defense Lawyers, International Association of Defence Attorneys y Canadian Forensic Society.

AMÉRICA LATINA

Dr. Paulo Marco Ferreira Lima, Brasil

Dr. Paulo Marco Ferreira Lima es Notario Público de la Ciudad de Sao Paulo. Desde 1997 ha sido asesor del Fiscal General en distintas áreas. Ha sido secretario de la Comisión de Proyectos Legislativos para la supervisión de los crímenes digitales.

El Dr. Lima es el autor del libro *Crimes de computador e segurança computacional (Delitos informáticos y seguridad informática*, publicado por Millennium), que salió al mercado en 2007. Es además Profesor en la Universidad de Santos (ciudad del estado de Sao Paulo) en un curso de posgrado. Se licenció en la facultad de derecho de la Universidad de Mackenzie y tiene un Máster en Derecho Penal, un Doctorado en Derecho Penal por la Universidad de Sao Paulo, y está realizando un Doctorado en Derecho Penal Digital por la Universidad de Roma, UNIROMA3.

Adriana Scordamaglia Fernandes Marins, Brasil

La Dra. Adriana Scordamaglia ha sido Fiscal Federal desde 1997 y ha trabajado en el área de actividades criminales del Ministério Público Federal (Fiscalía Federal brasileña) en la 2ª Vara Criminal da Seção Judiciária de São Paulo (Sección 2ª de lo Penal de Sao Paulo). Con anterioridad, trabajó en el Departamento Oficial del Gabinete da 21ª Vara Federal (21ª Agencia Judicial Penal Federal) de 1993 a 1997.

La Dra. Scordamaglia se licenció en la escuela de derecho de las Faculdades Metropolitanas Unidas de Brasil y realizó un posgrado en la Universidad de Lusíada de Oporto, Portugal. En 2008, organizó un taller sobre delitos contra la infancia con la ayuda del ordenador, e impartió un seminario sobre el perfil psicológico del pedófilo. Asimismo, ha participado en el Taller Internacional sobre Legislación de la Ciberdelincuencia celebrado en Bogotá, Colombia, a través del Departamento de Justicia de Estados Unidos.

Renato Opice Blum – Opice Blum Advogados Associados, Brasil

El gabinete Opice Blum Advogados Associados posee una amplia experiencia en Derecho, en particular en tecnología, derecho electrónico, tecnología de la información y sus variantes. Como pionero en estos temas, actúa también en mediaciones, arbitrajes, alegatos orales ante el Tribunal, bioderecho, contratos tecnológicos típicos y ciberdelitos. Opera en todo el territorio de Brasil y cuenta con representantes internacionales en los principales centros financieros, como Miami y Nueva York.

Como miembro de varios organismos institucionales, contribuye a la evolución del derecho relativo al desarrollo tecnológico. Es socio fundador de la Cámara de Comercio Electrónico de Brasil y miembro de la Sociedad brasileña de Informática, entre otras instituciones.

8 4568 44 822.656 546 78952
565.369 21

ASIA-PACÍFICO

Alana Maurushat – Directora en funciones del Centro de Políticas y Derecho del Ciberespacio de la Universidad de Nueva Gales del Sur en Australia

Alana Maurushat es Directora en funciones del Centro, profesora asociada y cursa un Doctorado en la Facultad de Derecho de la UNSW. Ha sido profesora adjunta y subdirectora del Máster de Derecho en Tecnología de la Información y la Propiedad Intelectual de la Facultad de Derecho de Hong Kong. Imparte clases de Investigación Legal Avanzada. Su área actual de investigación se desarrolla en el ámbito de las dimensiones técnicas, éticas y legales del malware informático, que se basa en los proyectos de investigación anteriores sobre el impacto de las tecnologías de vigilancia en la libre expresión y la privacidad. Es investigadora asociada en el proyecto sobre la regulación del malware Regulating Malware.

Peter Guttman – Investigador de seguridad, Universidad de Auckland, Nueva Zelanda

El Dr. Peter Gutmann es investigador del Departamento de Ciencia Informática de la Universidad de Auckland, y está especializado en el diseño y análisis de las arquitecturas de seguridad de cifrado. Contribuyó a la creación del conocido paquete de cifrado con PGP y, más recientemente, ha creado el Cryptlib Security Toolkit, un kit de herramientas de cifrado y seguridad de código abierto e independiente del sistema operativo, intercambio de claves, firmas digitales, gestión de claves y certificados, soporte de tarjetas inteligentes, cifrado de correo electrónico con S/MIME y PGP, SSL y cifrado de sesión ssh, registro con marca de fecha/hora, gestión de autoridades de certificación y otras funciones. Cryptlib, utilizada y reconocida a nivel internacional, es la única aplicación de Nueva Zelanda que ha recibido una certificación de seguridad FIPS 140 del gobierno de EE. UU.

Andrew Adams – Profesor de Ingeniería de Sistemas, Universidad de Reading, profesor asociado de la Meiji University, Japón

Andrew Adams es profesor de la Escuela de Ingeniería de Sistemas de la Universidad de Reading, donde es miembro de los grupos de investigación Informatics Research Group, Informatics Research Centre, y Computer Science and Informatics Subject. Es Presidente del grupo Informatics Research Group y Director de Programa de las titulaciones en Tecnología de la Información.

Ha impartido seminarios en el Laboratorio de Informática de la Universidad de Cambridge, el Oxford Internet Institute, el Departamento de Ciencia Informática de la Universidad de Bath y la Escuela de Derecho de la Universidad de Southampton en el Reino Unido sobre su trabajo en materia de privacidad en Japón, financiado por la Royal Academy of Engineering dentro del plan Global Research Awards, y desarrollado en colaboración con el profesor K. Murata de la Universidad de Meiji y el Dr. Y. Orito de la Universidad de Ehime.

McAfee, S.A.
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España

www.mcafee.com/es

McAfee, Inc., con sede central en Santa Clara, California, es la mayor compañía especializada en seguridad del mundo. Proporciona servicios y soluciones proactivas y probadas que protegen sistemas y redes en todo el mundo, y permiten a los usuarios navegar y comprar a través de la Web con seguridad. Su inigualable experiencia y su compromiso con la innovación permiten a McAfee dotar a usuarios particulares, empresas, sector público y proveedores de servicios de la capacidad de cumplir con la normativa, proteger datos, evitar problemas, identificar vulnerabilidades y controlar y mejorar de manera continua su seguridad. http://mcafee.com

La información de este documento se proporciona únicamente con fines educativos y para la conveniencia de los clientes de McAfee. Nos hemos esforzado por asegurar que la información del *Informe sobre criminología virtual de McAfee* sea correcta; sin embargo, dado que la ciberseguridad cambia constantemente, el contenido de este documento está sujeto a modificaciones sin previo aviso y se proporciona tal cual, sin garantía en cuanto a su precisión o aplicación a una situación o circunstancia en particular.


442 5.4567
1/25/78
89.6 7 15
-926.89
$556,000
56
-12.38