



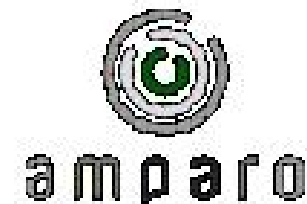
Panorama del cibercrimen en Latinoamérica

Autores:

Patricia Prandini
Marcia Maggiore

Director del proyecto:

Ing. Eduardo Carozo





Agenda

- ◆ Introducción
- ◆ Objetivo del informe
- ◆ Principales dificultades
- ◆ Evolución y marco conceptual de los ciberdelitos
- ◆ Panorama general de las ciberamenazas
- ◆ Impacto Económico
- ◆ Conclusiones
- ◆ Recomendaciones

Introducción

En las sociedades modernas los servicios esenciales para el bienestar de la población y el desarrollo económico de las naciones se sustentan en un empleo creciente de servicios tecnológicos que mejoran la calidad de vida y facilitan las labores cotidianas de las personas y las organizaciones.

En Latinoamérica, como parte de las sociedades modernas, el uso de las tecnologías ha crecido significativamente logrando un incremento del 1.032,8% entre los años 2001 y 2010.

(Fuente: Internet World Stats)

Sin embargo, estas tecnologías presentan importantes desafíos frente a la necesidad de proteger la información de las personas y organizaciones, debido a la creciente presencia de amenazas que invaden Internet.

Objetivo del informe

- ◆ Revisar y exponer el panorama de los ciberdelitos que afectan en mayor medida a los países de la región, compendiando para ello, en todos los casos, la información disponible en bases de datos de acceso público
- ◆ Recoger las opiniones de especialistas en cuanto al estado de la ciberdelincuencia en la región
- ◆ Proyectar una serie de indicadores valorizados que permitan obtener una idea de la magnitud del impacto económico de los incidentes de seguridad en Latinoamérica
- ◆ Generar un marco para estimaciones futuras del impacto del ciberdelito en la región, que pueda ser actualizado y mejorado cuando se disponga de información más precisa
- ◆ Utilizar un enfoque múltiple que comprenda organizaciones, personas, países, gobiernos y en lo posible, datos globales para toda la región

Principales Dificultades

- ◆ La reticencia a informar los incidentes ocurridos por parte de las organizaciones, los países y las personas
- ◆ La existencia de publicaciones con datos disímiles de entidades nacionales o internacionales y escasas cifras de organismos oficiales
- ◆ Las complejidades, y hasta la imposibilidad en ciertos casos, para determinar el impacto global de algunos tipos de ciberataques
- ◆ El encadenamiento de los incidentes informáticos que resultan en un único ataque.
- ◆ La necesidad de utilizar supuestos y de efectuar proyecciones respecto al porcentaje de incidentes reportados, que pueden tornar impreciso el cálculo
- ◆ Las complejidades para cuantificar el efecto económico o financiero sobre personas y organizaciones, tanto en forma individual como agregada
- ◆ La falta de homogeneidad en la metodología de conteo de los incidentes
- ◆ Las dificultades para valorizar factores tales como pérdida de reputación, imagen, etc.

Evolución y marco conceptual de los ciberdelitos

En sus comienzos, lo que hoy se denomina ciberataques fue experimental y no tenía como objetivo realizar un daño sino desafiar a los sistemas operativos de la época.

El primer virus se creó para las computadoras Apple II en 1982. En noviembre de 1988 el "Gusano de Morris" sacó de servicio el 10% de las computadoras VAX y SUN conectadas a INTERNET en los EEUU, unos 60.000 equipos en total.

La actividad siguió desarrollándose y cambiando sus objetivos, transformándose primero en causa de pérdida de información o discos completos, para llegar a hoy donde persigue fines criminales, como la obtención de dinero de manera ilícita.

Evolución y marco conceptual de los ciberdelitos

Hoy las amenazas son más complejas y sofisticadas, más agresivas, mejor dirigidas y con intenciones más claras y concretas, producto de las actividades maliciosas que la vinculan al crimen organizado.

Estas actividades conforman un modelo de negocio delictivo ampliamente explotado a través de Internet y que dio en llamarse ciberdelito o cibercrimen, alimentando una economía clandestina que crece exponencialmente día a día.

Los delincuentes explotan las debilidades de las tecnologías, los vacíos en la legislación y la falta de concientización de los usuarios, así como el alcance global de Internet y su rápida expansión, factores que facilitan la comisión de viejos delitos con nuevas herramientas.

Evolución y marco conceptual de los ciberdelitos

El siguiente cuadro es una adaptación del publicado por la Australian Crime Commission y compara algunos delitos tradicionales con sus equivalentes en el mundo de las tecnologías.

Delitos tradicionales	Ciberdelito equivalente
Fraude	Fraude en línea, subasta fraudulenta, estafa por solicitud de adelanto de fondos a través de Internet
Hurtos menores/daño malicioso	Hackeos, ataques de software malicioso, denegación de servicios
Ofensas contra menores	Sitios web pornográficos, creación de perfiles falsos con fines pedófilos
Lavado de dinero	Sistemas fraudulentos de pago en línea, mulas, engaño nigeriano (Nigerian scam)
Robo	Robo de identidad, phishing, piratería de software, películas y música, robo de Propiedad Intelectual en soporte electrónico
Acoso	Ciberacoso a adultos y menores

Evolución y marco conceptual de los ciberdelitos

Algunas de las particularidades de este tipo de actividades son la facilidad con que pueden borrarse las evidencias y las dificultades para identificarlas y preservarlas cuando no se es un especialista o no se cuentan con las herramientas adecuadas y la desmaterialización de las fronteras nacionales.

En este contexto, se habilita al delincuente a acceder a su blanco sin prácticamente moverse de su silla, a miles de kilómetros de sus eventuales víctimas. Adicionalmente, puede utilizar distintos caminos y recorridos en su afán de dificultar cualquier rastreo.

Estas características conforman un nuevo desafío para las fuerzas de seguridad, la justicia y los gobiernos, ya que es necesario modernizar la legislación, contar con personal especializado que pueda tratar este tipo de delitos y concientizar a la población. Asimismo, sólo es posible resolverlos a través de la colaboración internacional

Panorama General de las Ciberamenazas

Los ciberdelitos son cometidos utilizando como herramientas o “armas” las tecnologías de la información.

Los ciberdelincuentes, utilizando los servicios de expertos o bien por cuenta propia, construyen software malicioso para atacar a organizaciones e individuos con diferentes objetivos.

Este software malicioso conforma las ciberamenazas a las propias tecnologías de información (sus servicios, datos, transacciones, etc.).

Conocer y medir estas ciberamenazas permite generar los mecanismos para combatirlas y evitar los delitos que de ellas proceden.

A continuación se expondrá algunos resultados de las investigaciones realizadas por diferentes organizaciones.

Panorama General de las Ciberamenazas

Dado que las cifras que son utilizadas en las mediciones son generalmente expresadas en porcentajes, se presenta algunos datos de la actividad en Internet durante 2010, para dar una idea de su magnitud.

- 255 millones – Sitios web (diciembre de 2010)
- 1.97 mil millones – Usuarios de Internet en del mundo (junio de 2010)
- 204.7 millones – Usuarios de Internet en América Latina y el Caribe
- 1.88 mil millones– Usuarios de correos electrónicos en el mundo
- 294 mil millones – Promedio diario de envío de correo electrónico
- 600 millones – Personas en Facebook

Fuente: Pingdom

Panorama General de las Ciberamenazas

Situación global analizando las amenazas en su conjunto

Source	2010		2009	
	Overall Rank	Overall Percentage	Overall Rank	Overall Percentage
United States	1	19%	1	20%
China	2	16%	2	9%
Germany	3	5%	5	5%
Brazil	4	4%	4	5%
United Kingdom	5	4%	3	6%
India	6	4%	7	3%
South Korea	7	4%	9	3%
Italy	8	3%	10	3%
Taiwan	9	3%	6	4%
Russia	10	2%	8	3%

Fuente: Symantec Corporation

Latinoamérica se encuentra entre los cinco (5) o diez (10) primeros puestos en el mundo, representada por Brasil. En el caso de Panda Software que toma los primeros veinte (20) puestos, incluye Argentina, Bolivia, Ecuador, Chile, Perú y México.

Panorama General de las Ciberamenazas

Situación Latinoamericana analizando las amenazas en su conjunto

Overall Rank		Source	Overall Percentage		2010 Activity Rank				
2010	2009		2010	2009	Malicious Code	Spam Zombies	Phishing Hosts	Bots	Network Attack Origin
1	1	Brazil	44%	42%	1	1	1	1	1
2	3	Mexico	12%	13%	2	7	2	6	2
3	2	Argentina	10%	13%	6	4	5	2	3
4	4	Colombia	7%	8%	3	3	3	8	4
5	5	Chile	6%	7%	5	5	4	4	5
6	10	Uruguay	4%	1%	20	2	15	7	8
7	6	Venezuela	3%	3%	4	10	7	10	6
8	7	Peru	3%	3%	7	6	8	3	7
9	9	Dominican Republic	1%	1%	8	8	18	5	10
10	11	Panama	1%	1%	14	16	6	14	15

Fuente: Symantec Corporation

Panorama General de las Ciberamenazas

Situación Latinoamericana analizando las amenazas en su conjunto

Overall Rank		Source	Overall Percentage		2010 Activity Rank				
2010	2009		2010	2009	Malicious Code	Spam Zombies	Phishing Hosts	Bots	Network Attack Origin
1	1	Brazil	44%	42%	1	1	1	1	1
2	3	Mexico	12%	13%	2	7	2	6	2
3	2	Argentina	10%	13%	6	4	5	2	3
4	4	Colombia	7%	8%	3	3	3	8	4
5	5	Chile	6%	7%	5	5	4	4	5
6	10	Uruguay	4%	1%	20	2	15	7	8
7	6	Venezuela	3%	3%	4	10	7	10	6
8	7	Peru	3%	3%	7	6	8	3	7
9	9	Dominican Republic	1%	1%	8	8	18	5	10
10	11	Panama	1%	1%	14	16	6	14	15

Fuente: Symantec Corporation

Panorama General de las Ciberamenazas

Código malicioso – Situación global

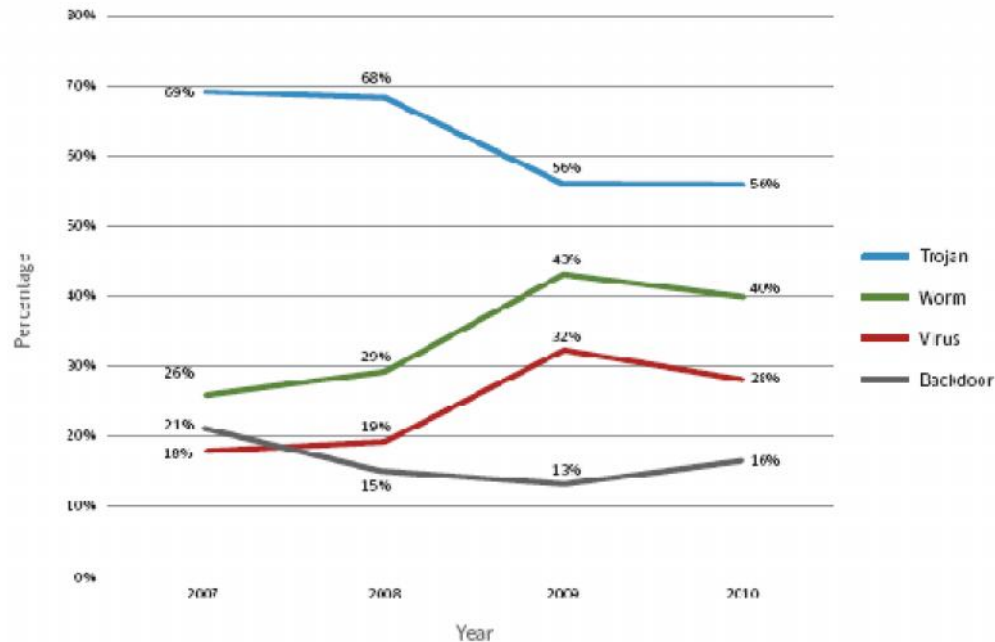


Figure 17. Prevalence of malicious code types by potential infections, 2007-2010
Source: Symantec Corporation

Troyanos bancarios en Latinoamérica

País	Porcentaje
Brasil	5,99
Colombia	2,30
Méjico	1,73
Ecuador	1,72
Guatemala	1,50
Chile	1,35
Argentina	1,13
Perú	0,62

Fuente: ESET Latinoamérica – abril/11

Panorama General de las Ciberamenazas

Spam – Situación global

Continent	% of global spam
Europe	39.3%
Asia	33.9%
South America	13.4%
North America	9.5%
Africa	3.2%
Oceania	0.7%

Table 1 2010 spam sources

Fuente: Symantec Corporation

De la información relevada surge que Latinoamérica ocupa el segundo lugar como región emisora de spam, representada por Brasil, mientras que Colombia se encuentra en el 10º lugar. Sin embargo, cabe señalar que Brasil ocupó el primer lugar en el mundo, como país origen de botnets emisoras de spam en el 2009, con el 13% del total. Mientras que en 2010 estuvo entre los 12 primeros.

Situación en Latinoamérica

Rank		Source	Percentage	
2010 LAM	2010 Global		2010 LAM	2010 Global
1	4	Brazil	41%	7%
2	12	Colombia	14%	2%
3	16	Argentina	12%	2%
4	21	Chile	8%	1%
5	28	Mexico	5%	1%
6	33	Peru	5%	1%
7	37	Dominican Republic	4%	1%
8	46	Venezuela	2%	< 1%
9	53	Guatemala	1%	< 1%
10	63	Uruguay	1%	< 1%

Panorama General de las Ciberamenazas

Phishing – Situación global

1er. semestre 2009: Brasil, 7mo.
 2do. semestre 2009: Honduras, 2do; Méjico, 4to.; Brasil, 10mo.
 1er. semestre 2010: Brasil, 5to.
 2do. semestre 2010: Brasil, 3ro.

Phishing – Situación en Latinoamérica

Crecimiento entre el primer semestre/2009 y segundo del 2010						
TLD	TLD Ubicación	# único de sitios de Phishing	Nombres de Dominio únicos usados para phishing	Dominios registrados	# Total de dominios maliciosos registrados	Comentarios
br	Brasil	207,49	170,34	35,75	2000	No existe información sobre Puerto Rico.
co	Colombia	177,42	95,45	1948,26	400	
ar	Argentina	-3,86	-6,92	19,68	200	
ec	Ecuador	158,33	160	26,98	100	

Fuente: Antiphishing Working Group

Panorama General de las Ciberamenazas

Botnet – Situación global

Entre mediados de 2009 y principios de 2011, se estima un crecimiento de aproximadamente un 85% en la cantidad de botnet activas.

Esto representa millones de usuarios afectados por esta amenaza. Este valor se sustenta tan solo si se toman simplemente tres de las botnet que han sido dadas de baja durante 2010: Waledac (80 mil usuarios afectados), Mariposa (13 millones) y Bredolab (30 millones).

Fuente: Shadow Server

Fuente: Symantec Corporation

Cabe señalar que varios países de Latinoamérica se encontraron entre los TOP 20 de máquinas infectadas por la red Mariposa, compuesta por **más de 13 millones** de direcciones IP infectadas distribuidas en **190 países** al rededor del mundo. Ellos son: **México**, con el 12,85% (2do. Puesto), **Brasil**, con el 7,74% (3er. Puesto), **Colombia**, con el 4,94% (5to. Puesto), **Perú**, con el 2,42% (11mo. Puesto), **Chile**, con el 1,74% (décimo 4to puesto), y **Argentina**, con el 1,10% (décimo 8vo puesto) del total.

Fuente: Info Spyware

Situación en Latinoamérica

Rank			Source	Percentage		
2010 LAM	2009 LAM	2010 Global		2010 LAM	2009 LAM	2010 Global
1	1	5	Brazil	56%	54%	8%
2	2	13	Argentina	18%	18%	3%
3	3	22	Peru	7%	7%	1%
4	4	24	Chile	6%	6%	1%
5	5	32	Dominican Republic	3%	5%	< 1%
6	6	33	Mexico	3%	4%	< 1%
7	7	34	Uruguay	2%	2%	< 1%
8	8	36	Colombia	2%	1%	< 1%
9	9	53	Puerto Rico	1%	< 1%	< 1%
10	12	65	Venezuela	< 1%	< 1%	< 1%

Panorama General de las Ciberamenazas

También existen otros tipos de actividades maliciosas

- Códigos maliciosos multi-plataforma. Infectan a diferentes SO y a los de los dispositivos móviles como iPhone, Android.
- Búsquedas en la Web que llevan a sitios maliciosos utilizando técnicas de Blackhat SEO.
- Bots para redes sociales.
- Falsos antivirus (rogueware). Se trata de aplicaciones que se hacen pasar por soluciones antivirus que ofrecen explorar gratuitamente las computadoras, pero que no sólo no lo son sino que infectan los equipos.
- Explotación de vulnerabilidades, también en aplicaciones como Adobe. Aparición del Stuxnet.
- Denegación de servicio, fuertemente orientado a infraestructuras críticas.

Panorama General de las Ciberamenazas

Según informes de las compañías consultadas respecto a las tendencias para el corriente año

- Dispositivos móviles como blanco de masivos ataques, incluso a través de botnets
- Crecimiento de las botnets
- Consolidación de las redes sociales como herramienta para los delincuentes
- Spam sobre los muros de las redes sociales
- Crecimiento de los ataques dirigidos a industrias e individuos específicos, así como los ataques de DOS sobre las infraestructura crítica
- Crecimiento del uso de URLs cortas y subdominios por parte de los phishers

Impacto Económico

Diversos pronunciamientos de gobiernos, empresas líderes y organizaciones internacionales llevan a asegurar que la magnitud del ciberdelito es realmente preocupante y a plantear escenarios de ataques cibernéticos, con consecuencias gravosas para la población.

Diversas publicaciones señalan a Latinoamérica como origen y blanco de incidentes.

Para dimensionar la magnitud del problema, un ejercicio imprescindible es estimar el impacto económico de estos ataques, que efectiva o potencialmente podrían afectar tanto a organizaciones como a individuos en la región.

Sin embargo, intentar determinar este impacto es una labor compleja por diversos motivos y cualquier afirmación se basará necesariamente en una serie de supuestos justificados, ante la imposibilidad de acceder a datos concretos sobre la ocurrencia del incidente y sus características.

Impacto Económico

Estimar el impacto económico no es una tarea sencilla. Algunas de las dificultades que se presentan son:

- Ausencia de datos sobre la cantidad real de casos registrados
- Dificultades para establecer los costos indirectos y dimensionar la población afectada
- Bajo nivel de seguimiento y registro del tiempo y los recursos asignados al momento enfrentar un ataque
- Problemas para determinar sus consecuencias en el tiempo, todo lo cual dificulta la posibilidad de conocer el gasto total de remediación y compensación por las pérdidas registradas
- Escaso volumen de datos de casos de ataques o fallas reportados

Impacto Económico

Los costos a tener en cuenta para la medición pueden ser catalogados de la siguiente manera:

- Costos preventivos, que incluyen el costeo de las medidas de seguridad física, lógica y organizacionales y de las implementaciones para el cumplimiento del marco regulatorio y legal
- Costos de remediación, incurridos como consecuencia inmediata de los incidentes de seguridad, que abarcan las pérdidas directas que sufren las personas y las entidades, incluyendo aquéllas asociadas a las pérdidas de imagen, competitividad, etc.
- Costos de respuesta posteriores, como por ejemplo, las indemnizaciones a las víctimas
- Costos indirectos, vinculados por ejemplo, a la pérdida de confianza en las transacciones electrónicas y su impacto en el gobierno y el comercio electrónicos

Impacto Económico

Objetivo del análisis

Proveer un marco para la medición del impacto económico del ciberdelito en Latinoamérica, que pueda ser actualizado y mejorado cuando se disponga de información más precisa y de análisis más profundos

Las estimaciones y proyecciones globales que siguen se realizan en base a una serie de supuestos y especulaciones, ante la ausencia de datos concretos y representativos.

En pos de dicho objetivo se ha trabajado exclusivamente sobre los siguientes delitos:

- Fraudes bancarios y phishing y sus consecuencias para las personas
- Fraudes bancarios y phishing y sus consecuencias para los bancos
- Fraude en comercio electrónico
- Robo de identidad

Impacto Económico

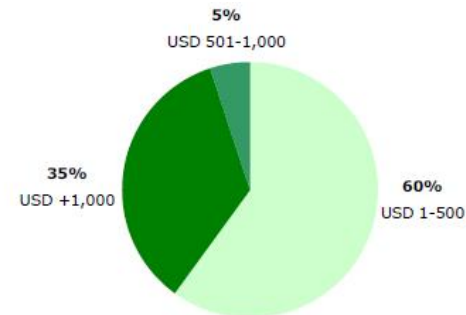
Para llevar a cabo las estimaciones se utilizaron cálculos que, en su mayoría, son adaptaciones de proyecciones similares efectuadas para investigaciones de otras regiones o países. En todos los casos en que fue posible, se utilizaron valores de la región o bien se tomaron indicadores de otras áreas, corregidos por la realidad local. Estas perspectivas fueron revisadas con los especialistas. Las fuentes fueron verificadas y sopesadas, privilegiando siempre las más reconocidas por tratarse de entidades internacionales, organismos nacionales o bien empresas de trayectoria del sector. Ante más de una fuente posible de similar nivel de confianza, se utilizó la más conservadora. De igual forma, se privilegiaron los datos más recientes ya que se ha comprobado que los ataques cibernéticos van cambiando y reinventándose a medida que aparecen medidas para neutralizarlos.

Las estimaciones se basan en supuestos y evaluaciones fundamentadas más que en datos reales, dado que no se encuentran accesibles bases completas de incidencia del ciberdelito. Por lo tanto, los valores que se exponen deben ser interpretados como guías ilustrativas, más que como datos concretos de su impacto económico en la región.

Impacto Económico

Fraude financiero - Informes

- Brasil - Habría alcanzado aproximadamente los u\$s 245 millones durante el primer semestre de 2010 (Fuente: FEBRABAN)
- Colombia – El 42% de los bancos reportó algún tipo de fraude durante el 2010 (Fuente: Gemalto)
- Chile – Las pérdidas superaron los u\$s 5 millones y los fraudes crecieron un 40% durante 2010 (Fuentes: Gemalto y Policía de Investigaciones de Chile)
- México – La cifra total atribuible a fraudes podría rondar los u\$s 60 millones en 2010 (Fuente: Comisión Nacional Bancaria)
- Latinoamérica - Monto promedio de fondos robados por incidente de fraude (Fuente: Frost and Sullivan)



Fuente: marketteam; Frost & Sullivan

Impacto Económico

Fraude financiero – Estimación de costos para los clientes

- Datos recolectados en el transcurso de tres meses, sobre clientes bancarios ubicados en Europa y los EEUU, indica que un 0.47% son víctimas de ataques de phishing cada año (Fuente: Trusteer)
- Un 43% de la población adulta de la región se encuentra bancarizada (Fuente: Federación Latinoamericana de Bancos)
- Diversos estudios señalan que la pérdida promedio por cuenta comprometida es de u\$s 1.000 (Fuentes: Frost and Sullivan, The Bismark Tribune, etc.)

Tomando entonces la cantidad de clientes bancarios en Latinoamérica corregido por el factor que señala la proporción de quienes finalmente resultan engañados y proveen sus datos, multiplicado por la pérdida promedio, es posible concluir que:

Las pérdidas anuales por phishing en Latinoamérica rondarían los 761 millones de dólares estadounidenses como valor agregado de las pérdidas de cada cliente engañado.

Impacto Económico

Fraude financiero – Estimación de costos para los bancos

Un estudio señala que los bancos son atacados en promedio a través de 16 sitios web maliciosos por semana. Por otro lado, varios estudios señalan que el costo total para un banco de un ataque de phishing rondaría los u\$s 50.000 o entre u\$s 50 y 60 por cada cuenta afectada.

Considerando que se estima que existen en la Región cerca de 2.500 bancos, es posible concluir que:

Las pérdidas totales agregadas para los bancos de Latinoamérica al afrontar los costos del phishing serían de 93.000 millones de dólares estadounidenses por año.

Impacto Económico

Fraude en el comercio electrónico - Informes

Un estudio de VISA señala que el comercio electrónico en Latinoamérica alcanzó durante el año 2009 un volumen de u\$s 21.800 millones.

Este crecimiento se debe a diversos motivos, entre los que se encuentran el uso cada vez mayor de Internet, conexiones más veloces de banda ancha, una creciente confianza del consumidor, una mayor cantidad de comerciantes que utilizan este canal de venta y una mayor difusión de uso de los medios de pago electrónicos.

Otro informe de la empresa antes citada precisa que en valores monetarios, Brasil representa un 61% del comercio electrónico en Latinoamérica, alcanzando un volumen de más de u\$s 13.000 millones en el 2009.

Este crecimiento se sustenta en el crecimiento de la cantidad usuarios de Internet, los bajos costos de la banda ancha y un uso importante de las tarjetas de crédito y débito en dicho país.

Le siguen México con un 12% de consumo total seguido de Chile con un 5% y luego Colombia y Perú.

Impacto Económico

Fraude en el comercio electrónico – Estimaciones

- Es posible estimar que el fraude como porcentaje del volumen de comercio electrónico se ha estabilizado en Canadá y EEUU en alrededor del 1.4%. (Fuentes: McAfee Inc. Y CyberSource Corporation)
- Los comerciantes en línea mejoraron sus porcentajes frente al fraude, según relevamientos en Canadá y EEUU durante 2010, llegando a un valor estimado de 0.9% promedio de sus ganancias (Fuente: CyberSource Corporation)

Para realizar una estimación en este caso y siendo que no se cuenta con un valor del porcentaje estimado de fraude para la región, se tomará entonces el 0.9% sobre el monto total que generó el comercio electrónico en Latinoamérica en el 2009, siendo éste el valor más conservador. Aplicando este porcentaje es posible concluir que:

El fraude en el comercio electrónico en Latinoamérica podría estar alcanzando los 196 millones de dólares estadounidenses.

Impacto Económico

Fraudes vinculados a la identidad – Informes

- Diversos estudios coinciden en afirmar que el robo de identidad es el delito de mayor crecimiento en el mundo, amparado además en el volumen creciente de datos disponibles, en la facilidad con que se pueden obtener información de usuarios desprevenidos, las insuficientes campañas de prevención, el crecimiento de las redes sociales y sus múltiples usos que exceden lo meramente “social”, y un mercado delictivo cada vez más atractivo para el tráfico de este tipo de información
- Colombia – El robo de información bancaria en el 2010 generó un promedio de 189 denuncias mensuales y se llegó a investigar una fraudes por aproximadamente u\$s 11 millones (Fuente: Grupo de Investigaciones Tecnológicas del Gobierno de Colombia)
- Ecuador – Durante 2009 se realizaron 891 denuncias (Fuente: Policía Judicial de Ecuador)
- México – En los últimos años ha tenido una tendencia creciente llegando a generar pérdidas de las u\$s 9 millones anuales

Impacto Económico

Los valores de la ciberdelincuencia

Ahora bien... ¿Cuán lucrativo es este negocio?

- Es posible obtener todas las herramientas para iniciar una campaña de phishing por u\$s 200. (Fuente: Computerworld)
- Las tarjetas de crédito y la información de cuentas bancarias constituían en el año 2009 el 51% de los bienes promocionados en los canales de la economía clandestina. Las tarjetas se venden en el mercado negro a un valor promedio de u\$s 0,98, cuando se las entrega en cantidad. Una identidad completa puede valer unos u\$s 10. (Fuente: CNN)
- El costo de alquiler de una botnet por hora se cotiza en los foros del mercado negro en aproximadamente u\$s 9. El alquiler diario rondaría los u\$s 67. (Fuente: CIFAS)
- Un 25% de las organizaciones relevadas en un estudio han sufrido la paralización o atraso de una fusión o adquisición, o bien de la implementación de un nuevo producto o solución, a causa de una filtración de datos o por una amenaza creíble de filtración de datos. Sólo la mitad de estas organizaciones adoptaron medidas para prevenir intrusiones futuras. (Fuentes: Estudio de McAfee Inc. Y Science Applications International Corporation)

Conclusiones

La actividad del ciberdelito es totalmente fluctuante y dependerá de las medidas que adopten los usuarios, las organizaciones y los países para enfrentarlo.

Estará condicionada a la conveniencia de los delincuentes y a las herramientas disponibles en cada momento, así como a las oportunidades del mercado, la generación de marcos normativos adecuados a la realidad del ciberdelito y el grado de cooperación que se desarrolle entre organizaciones y entre países.

Latinoamérica es parte de este escenario, mostrando en muchos casos un dinamismo superior al promedio en la incorporación de la tecnología a sus sociedades, pero también su condición de origen y blanco de una activa ciberdelincuencia. Brasil, México y Argentina aparecen en los primeros puestos en las listas internacionales de cantidad de computadoras infectadas, casos de phishing o número de sitios web maliciosos. Esto se traduce en pérdidas económicas que afectan a los ciudadanos, los negocios y a los países de la región como a usuarios de otros países ajenos a ella.

Conclusiones

La escasez de datos concretos sobre la cantidad de ataques potenciales o reales, y de sus costos asociados, hace difícil o casi imposible conocer su frecuencia, su verdadera magnitud y la profundidad de su impacto.

Si bien para algunos tipos de incidentes obtener estas cifras es sumamente complejo, para otros es probable que existan y se puedan obtener con relativa facilidad, pero las organizaciones afectadas son reticentes a denunciarlos por temor a que se vea afectada su reputación. En el caso de las personas, persiste el desconocimiento sobre instancias de reporte o la creencia de que poco o nada sucederá en caso de hacerlo.

La vertiginosidad del desarrollo tecnológico en los países de la región y el consiguiente crecimiento inexorable del ciberdelito, hace necesaria la generación de planes de acción que recogiendo sus características culturales y de desarrollo, muestren desde la perspectiva de las personas, las organizaciones y las naciones, que es factible generar un entorno seguro que garantice la maximización del aprovechamiento de los múltiples beneficios de las tecnologías de la información y las comunicaciones, minimizando los riesgos que las acompañan.

Recomendaciones

Para los Gobiernos

- Desarrollar estrategias nacionales sobre ciberseguridad que contemplen la protección de sus infraestructura críticas, un aumento de la capacidad de respuesta a incidentes, campañas de concientización para la ciudadanía, mecanismos de coordinación con el sector privado y con otros países y la generación de un marco normativo adecuado para la penalización de delitos de esta naturaleza
- Mejorar la coordinación y el trabajo conjunto entre los organismos involucrados en la adopción de medidas de seguridad de la información (Policías, Organismos Judiciales, Centros de Respuesta a Incidentes, etc.) y generar organismos o agencias que se dediquen exclusivamente a la ciberseguridad

Para la Academia

- Desarrollar contenidos y programas de formación de profesionales especialistas en seguridad de la información, que la aborden desde distintas visiones: técnica, legal, de educación, etc.
- Desarrollar líneas de investigación que analicen las distintas perspectivas de los ciberataques

Recomendaciones

Para el Sector Privado

- Generar equipos de trabajo dentro de las organizaciones que aborden la seguridad informática con un enfoque múltiple, que permita comprender y resolver los problemas relacionados con la protección de la información desde diversas perspectivas
- Colaborar con los organismos del Gobierno y proponer acciones conjuntas para mejorar la ciberseguridad a nivel nacional

Para los usuarios

- Adoptar un actitud responsable frente al uso de las tecnologías de información, capacitándose para minimizar los riesgos que las acompañan
- Cuidar la información propia y la de otras personas, cualquiera sea el soporte
- Denunciar los incidentes de seguridad ante las instancias que correspondan, permitiendo su seguimiento y contribuyendo así a su resolución
- Enseñar a los menores los peligros de las redes sociales y entrenarlos en una adecuada utilización de las tecnologías de la información

Recomendaciones

Finalmente, una de las mayores dificultades que acompañaron la realización de este informe fue la escasez de información sobre la ocurrencia de los ciberdelitos, sus características y reales consecuencias.

Sin datos es imposible dimensionar la magnitud del problema, estimar el riesgo para asignar prioridades y recursos y adoptar así, decisiones certeras para proteger la confidencialidad, integridad y disponibilidad de la información. La base de este problema es que no se comparten datos. Esta responsabilidad recae tanto en los gobiernos como en las organizaciones y en todos nosotros, como usuarios de información y servicios en línea.

Por lo tanto, resulta fundamental crear mecanismos confiables de reporte y a colaborar compartiendo información, contribuyendo así a un mayor conocimiento colectivo que permita contrarrestar los peligros de las tecnologías de la información y aprovechar a pleno todos de sus beneficios.



Panorama del ciberdelito en Latinoamérica

¡Muchas gracias!

