ENJOY SAFER TECHNOLOGY™

ESET Security Report Latinoamérica 2014

Argentina | Chile | Colombia | Costa Rica | Ecuador | El Salvador
Guatemala | Honduras | México | Nicaragua | Panamá | Paraguay
Perú | Venezuela

CONTENIDO

82% Utilizan Antivirus para controlar la seguridad en su empresa

Durante 2013 ESET Latinoamérica ha participado de diversos eventos en toda la región, en los cuales encuestó a 3369 ejecutivos para recopilar información acerca del panorama actual de la Seguridad de la Información en la zona. A través de estos datos se realizó el ESET Security Report Latinoamérica 2014, un informe que detalla y describe la actualidad de las empresas en materia de Seguridad de la Información.

El informe cuenta con datos de empresas de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Venezuela. Asimismo, está dividido en tres ejes fundamentales a través de los cuales se podrá entender el estatus de la Seguridad Informática de las compañías en la actualidad.

Específicamente, el presente de las empresas, sus decisiones e implementaciones respecto a Seguridad Informática y la repercusión de sus determinaciones serán expuestos en "**Actualidad de las empresas**".

En "**Gestión de la Seguridad de la Información en las empresas**" se verá la estructuración de los departamentos encargados de gestionar la seguridad y sus opiniones respecto a los recursos con los que cuentan, en contraste con la realidad de años anteriores.

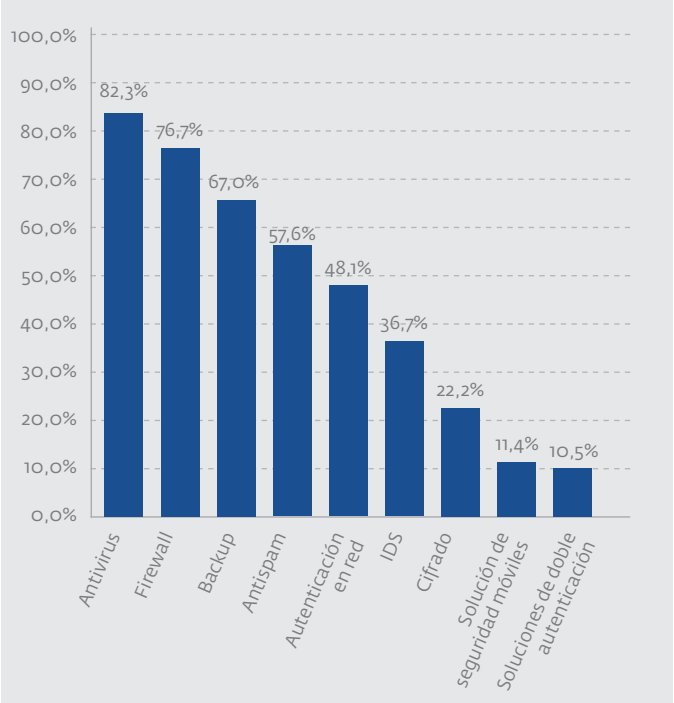
Finalmente, todo lo relativo a incidentes de seguridad y los esfuerzos para evitarlos o paliarlos se expondrá en "**Incidencias en las empresas y enfoques de proactividad**".

Actualidad de las empresas

¿Ven las empresas como prioritarias las protecciones ante incidentes que involucran a sus empleados?
Al consultar los índices de implementación de controles de seguridad en las empresas latinoamericanas (detallados en el **Gráfico 1**), puede verse que los más comunes, como una solución antivirus, *firewall* o *antispam*, son los más adoptados con porcentajes que oscilan entre 82% y 57%. Sin embargo, también se percibe que la utilización de métodos no tan difundidos, como el de Autenticación en red y Sistemas de detección de intrusos (o IDS), es notablemente menor. Llamativamente, estos métodos se encuentran ligados con **la prevención de incidentes relacionados con empleados.**

El aspecto presentado previamente no debe pasar inadvertido. Así como el eslabón más débil termina condicionando la resistencia de toda una cadena, el sector menos resguardado lo hace con la seguridad de una empresa. El hecho de que los métodos para prevención de incidentes relacionados con empleados sean los menos utilizados representa un problema. Las empresas deben ver como prioritaria la implementación de este tipo de medidas de seguridad para prevenir

| Gráfico Nº 1 |
Implementación de Controles



incidentes internos ya que cambiando el enfoque de sus políticas de controles hacia la protección de este tipo de incidentes, lograrán no solo disminuir su cantidad, sino también fortalecer el esquema de seguridad informática de toda la empresa en general.

En este punto, es importante notar que los incidentes internos no necesariamente son intencionales. Un ejemplo simple de esta situación es la de un usuario accidentalmente infectado con *malware* que podría propagar la amenaza a través de una red interna de la empresa.

¿La facilidad actual de conexión a Internet repercute en la gestión de Seguridad de las empresas?
Uno de los aspectos notables de los últimos años es el aumento de la conectividad. Los usuarios de computadoras portátiles, *tablets*, *smartphones* y demás *gadgets* tienden a estar conectados todo el tiempo (o gran parte de él), para poder interactuar de forma más fluida con las Redes Sociales, comunicarse con gente de su entorno o demás funcionalidades, como encontrar un lugar específico en el mapa o realizar la búsqueda en Google.

Muchos empleados de empresas tienen este perfil, de modo que al ir a trabajar utilizan Internet desde las redes donde trabajan, o incluso conectan sus dispositivos móviles a sus computadoras corporativas. Es necesaria, entonces, una política en materia de *Bring your own device* (BYOD por su sigla en inglés) que establezca los parámetros de

42% De las empresas no tienen una política de BYOD definida

uso. No obstante, no todas las empresas deciden implementarla, ya que tiene tanto aspectos positivos como negativos.

Por eso, en un contexto en donde la proliferación del *malware* para dispositivos móviles aumenta constantemente y donde los ataques de Ingeniería Social también se hacen presentes, las empresas deben tomar recaudos para protegerse ante incidentes que quizás no las afecten de forma directa, pero sí indirectamente a través de sus empleados.

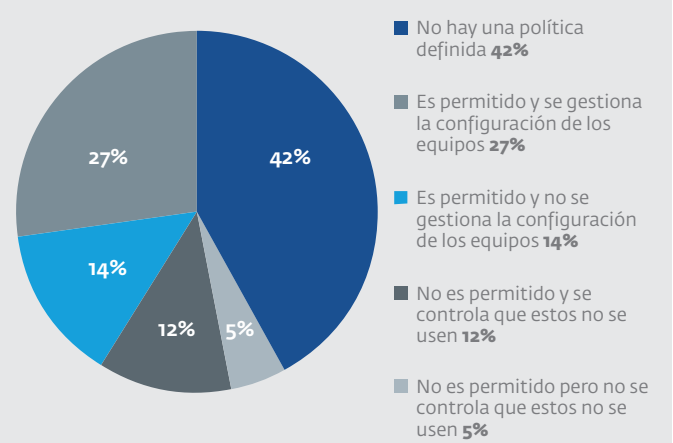
Tal como ESET detalló en el informe de **"Tendencias 2014: el desafío de la privacidad en Internet"**[1], la utilización de dispositivos portátiles con conexión a Internet aumenta en cantidad y de formas curiosas, que hace diez años atrás quizás no eran siquiera imaginables. La utilización de relojes inteligentes o *wearables* (dispositivos con conexión a Internet que se "usan", como ropa o accesorios) incrementa, y es necesario comenzar a revisar qué controles definen las políticas de seguridad empresariales actuales. Si el ámbito de este tipo de controles sigue sin organizarse de forma sólida y sigue incrementándose el uso de dispositivos que demanden una conectividad constante, todo esto podría hacer que surja un nuevo vector de riesgo para la seguridad de las empresas latinoamericanas.

La información recopilada refuerza lo afirmado previamente, ya que no sólo en el **Gráfico 1** puede verse que las soluciones de seguridad para móviles están entre las menos elegidas, sino que también en el **Gráfico 2** se comprueba que el 42% de los encuestados no tiene una política de BYOD definida. Luego, con el 27% figuran las compañías que permiten el uso de equipos personales y gestionan su configuración; mientras que el tercer puesto es ocupado por empresas que permiten el uso, pero no gestionan la configuración, con el 14% del total.

Si se consideran estos aspectos, y que la opción de no permitir BYOD y controlar que no se usen los dispositivos está en anteúltimo lugar, puede verse que las decisiones más restrictivas son las menos preferidas. De todos modos, es importante aclarar que este tipo de posturas no necesariamente son las más seguras: la adopción de la metodología de gestión más adecuada dependerá de su contexto de aplicación, como por ejemplo a qué se dedica la empresa en cuestión, su tamaño, etc.

| Gráfico Nº 2 |

Gestión de BYOD en la empresa



Prácticas de Gestión

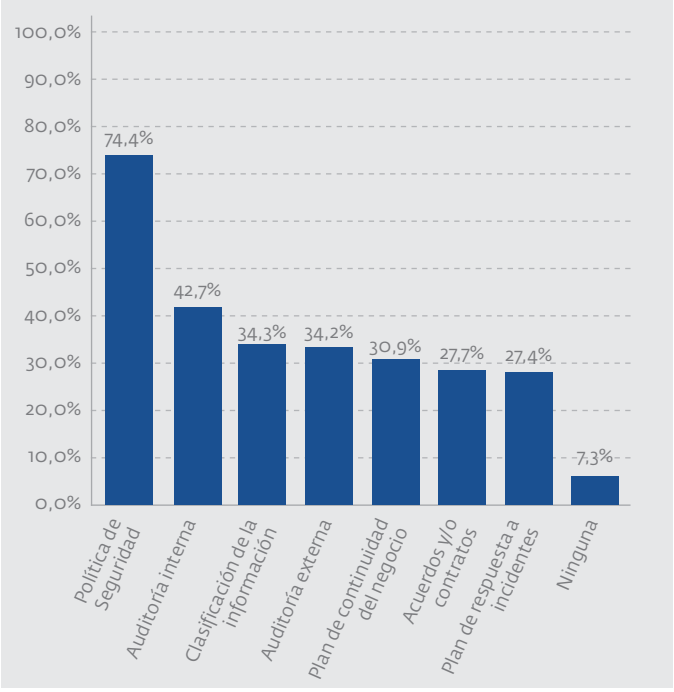
A través del análisis de las prácticas de gestión que implementan las empresas de la región, queda en evidencia que la gran mayoría (74,4% del total) implementa una política de seguridad, como expone el **Gráfico 3**. La auditoría interna también es frecuente en casi la mitad de las empresas. Este aspecto, sin embargo, no es sorpresivo, ya que estas prácticas han sido de las más adoptadas a lo largo de los años.

La adopción de planes de continuidad del negocio (30,9%) y de respuesta a incidentes (27,4%) se encuentran entre las tres prácticas menos adoptadas. Este no es un dato menor, ya que permite deducir que las empresas no ven primordial la capacidad reactiva ante incidentes.

Lo analizado previamente remarca un factor de riesgo: las empresas no solo deben prepararse para que no ocurran incidentes, sino también definir planes de emergencia ante imprevistos. No existe

| Gráfico Nº 3 |

Prácticas de Gestión en las empresas de Latinoamérica



1. http://www.welivesecurity.com/wp-content/uploads/2014/02/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

85% De las empresas latinoamericanas cuentan con un departamento de IT

un conjunto de controles preventivos que eviten por completo la ocurrencia de incidentes.

Una óptima implementación de los controles más rigurosos de seguridad no exime de futuros incidentes ya que, por ejemplo, una vulnerabilidad del tipo *0-day* podría ser explotada sin problemas en un ambiente como este. Un ejemplo claro de esto ha sido el reciente caso del *bug* Heartbleed, una vulnerabilidad de OpenSSL que afectó a un gran número de empresas de forma inesperada.

A raíz de esto es necesaria la implementación de prácticas de gestión relacionadas con controles reactivos. De otra forma, las empresas pueden estar correctamente preparadas para evitar incidentes, pero ante la ocurrencia de uno (que siempre es un riesgo latente) podrían quedar indefensas debido a la falta de reacción.

Actividades de educación en la empresa

El ESET Security Report del año pasado remarcó la disminución de actividades de educación dentro de las empresas latinoamericanas. En este sentido, en 2012 el porcentaje de empresas que realizaban regularmente actividades de concientización se redujo casi un 10%. Consecuentemente, las que no realizaban actividades de este tipo aumentaron.

Este año se observa que más de la mitad de las empresas (el 68% de acuerdo al **Gráfico 4**) lleva a cabo actividades de concientización al menos de forma ocasional, lo que marca un incremento respecto al año pasado, donde más del 20% no las llevaba a cabo.

El incremento de actividades de concientización en las empresas latinoamericanas es sumamente positivo, ya que ayuda a enfrentar la necesidad de implementar más controles para evitar incidentes que involucren a sus empleados.
La educación es fundamental para evitar incidentes de seguridad: un trabajador que sabe cómo crear contraseñas robustas y que las cambia de forma periódica ayudará a la empresa a estar más segura. Por el contrario, uno que no conozca estos recaudos y utilice simplemente las claves que le resulten más cómodas podrá representar un vector de riesgo.

Claramente, este tipo de actividades ayudará a elevar al nivel de seguridad general de la compañía, ya que habría menos posibilidades de que los empleados incurran en incidentes accidentalmente.

Gestión de la Seguridad de la Información

Dependencia del área de Seguridad de la Información en empresas

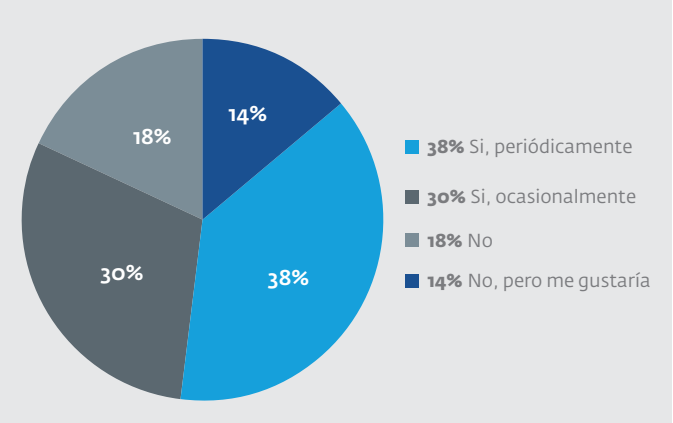
En este contexto han sucedido cambios significativos respecto a años anteriores. En el reporte anterior, el área de Seguridad de la Información no se encontraba implementada en alrededor del 60% de las empresas encuestadas. En aquellas en las cuales sí estaba presente, se encontraba relacionada mayoritariamente al área de Operaciones o el de IT, y en la minoría de los casos poseía un área exclusiva.

Este año la situación cambió: el 85% de las empresas latinoamericanas encuestadas cuentan con un área dedicada que mayoritariamente se encuentra vinculada con el departamento de IT.

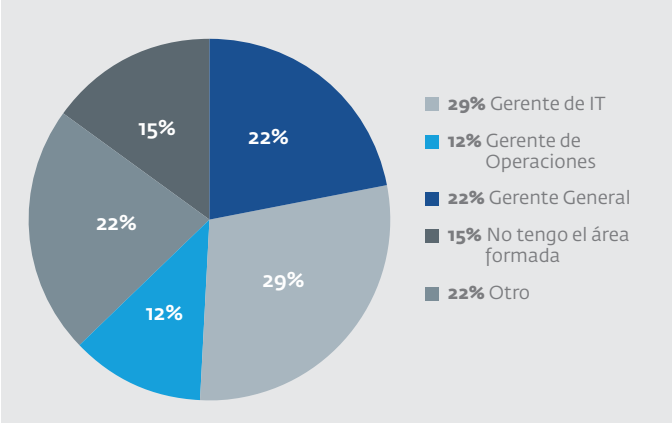
El dilema del presupuesto

De acuerdo a lo expuesto en la sección anterior, puede determinarse que las empresas suelen ver al área de IT como la más adecuada para contener a la de Seguridad de la Información. Este modelo es válido para empresas de pequeña o mediana envergadura, pero no es el óptimo para las de gran tamaño o de constante crecimiento, donde este área se encuentra relacionada con otras. En este tipo de com-

| Gráfico Nº 4 |
¿Lleva adelante actividades de concientización en su empresa?



| Gráfico Nº 5 |
Dependencia del área de Seguridad Informática



55% No consideraban necesario asignar dinero al área de Seguridad de la Información

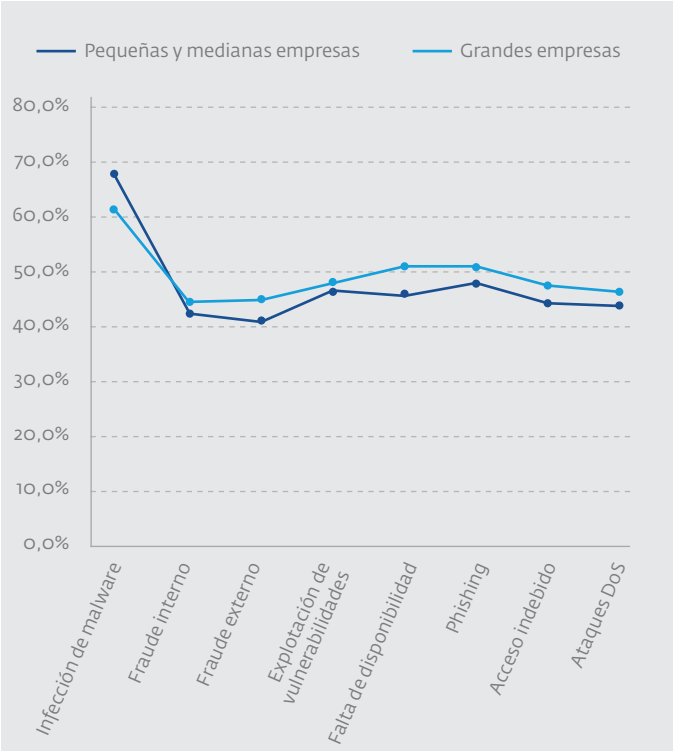
pañías se plantean problemáticas distintas y más complejas que exigen un departamento independiente que se encargue de solucionarlas, y trabaje exclusivamente para lograr una empresa segura.

La información disponible demuestra que pequeñas y medianas empresas sufrieron en primera medida incidentes de infecciones de *malware*, puntualmente un 67,10% de las empresas encuestadas. Los casos de *phishing* y explotación de vulnerabilidades ocupan los lugares siguientes, habiendo afectado al 48, 43% y 47,35% de las empresas respectivamente. Si bien las empresas grandes también sufrieron incidentes de infección de *malware* y *phishing*, el tercer lugar corresponde a la falta de disponibilidad (afectando al 51,35% de las empresas), y no la explotación de vulnerabilidades.

Si bien un área dedicada específicamente a la Seguridad de la Infor-

| Gráfico Nº 6 |

Comparativa Incidentes en 2013



mación demandaría más presupuesto, la mayor parte de los encuestados están de acuerdo en la necesidad de acercarse a un modelo de como este, aún cuando signifique más gasto.

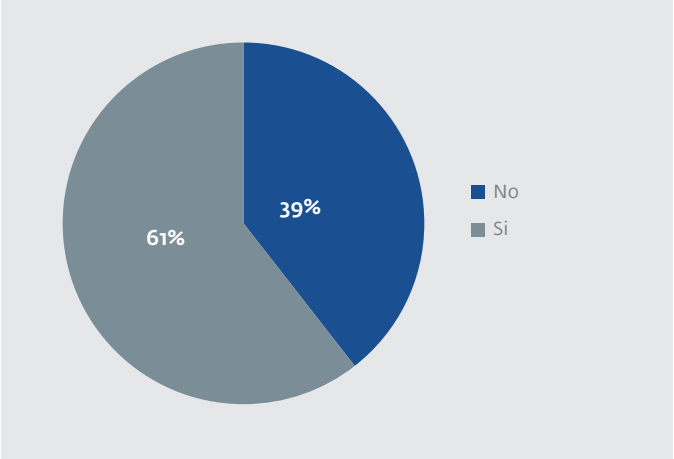
Variación del presupuesto utilizado entre 2012 y 2013

En el reporte anterior se vio que alrededor del 55% de las empresas no consideraban que el dinero asignado al área de Seguridad de la Información fuese el necesario.

Este año, por el contrario, se vieron cambios en materia de asigna-

| Gráfico Nº 7 |

¿Es necesaria una transición a un nuevo modelo aunque implique aumentar el presupuesto del área?

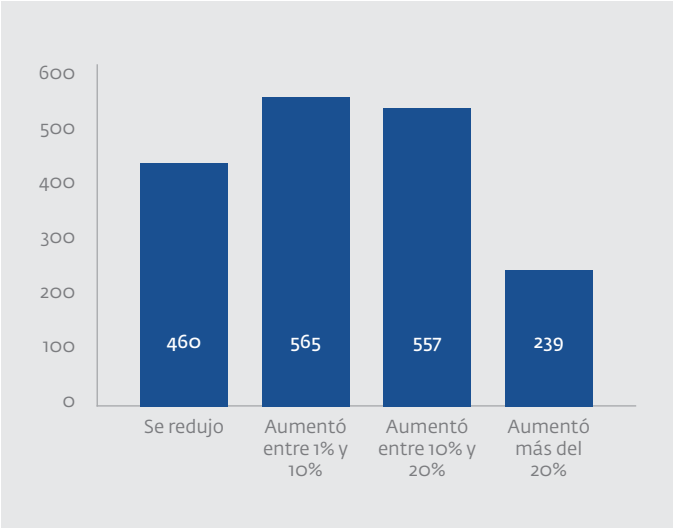


ción de recursos al área: mayoritariamente sufrió aumentos entre el 1% y el 20%. Subas mayores al 20% se presentan en significativamente menos casos, de acuerdo al **Gráfico 8**. No obstante, una cantidad considerable de las empresas también notó que el presupuesto disminuyó, pero en contraposición a la cantidad de empresas que percibieron aumentos de recursos el balance general es positivo.

Estos resultados también representan un aumento de acuerdo al

| Gráfico Nº 8 |

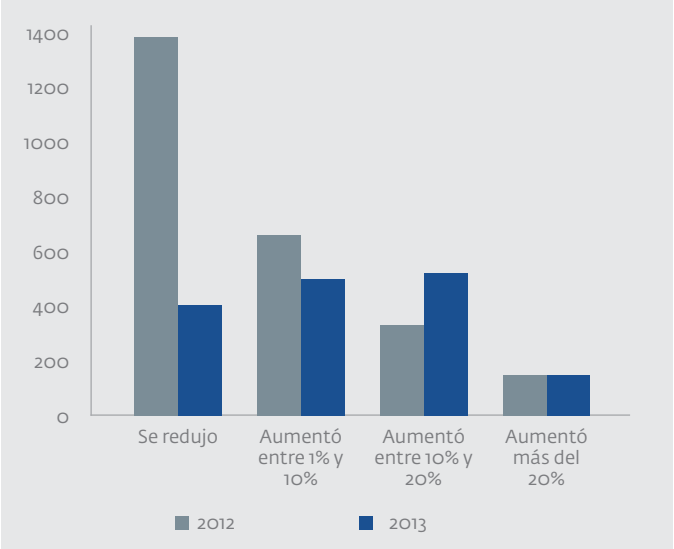
Variación del presupuesto para Seguridad Informática



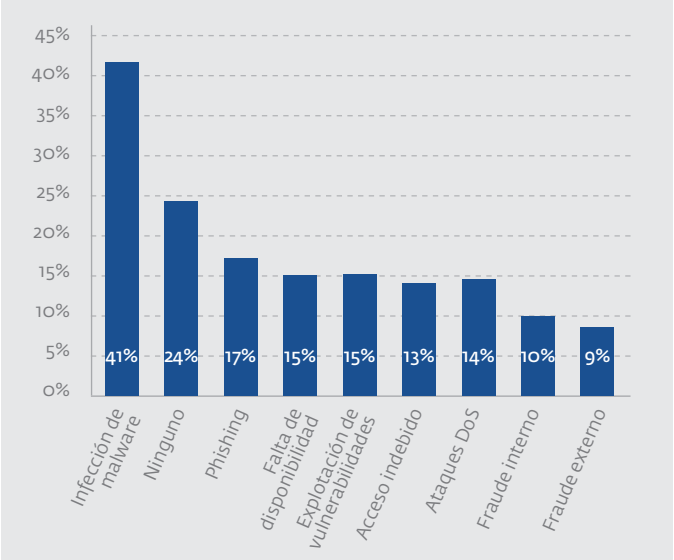
año pasado, donde el valor más significativo denotaba la reducción de presupuesto para el área. De aquí se puede hacer un balance sumamente positivo, en base a los detalles del **Gráfico 9**.

42% Fueron incidentes de Infección de malware

| Gráfico Nº 9 |
Variación de presupuesto 2012/2013



| Gráfico Nº 11 |
Incidentes en los últimos 12 meses



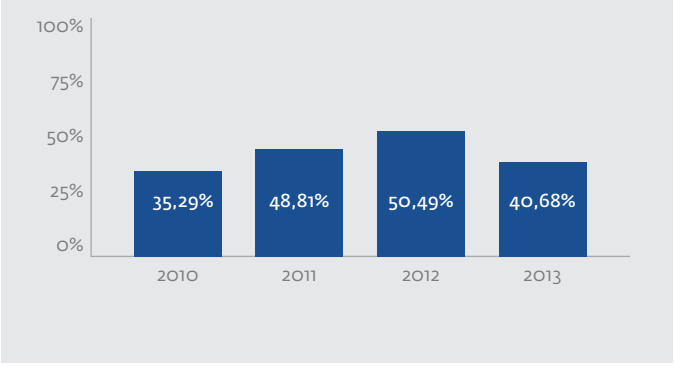
Incidencias y enfoques de proactividad

Las empresas pueden mejorar su enfoque proactivo ante las futuras incidencias

En materia de incidencias de seguridad, las infecciones de *malware* siguen ocupando el primer puesto con la mayor cantidad de ocurrencias (**Gráfico 11**). Este hecho no se presenta como algo inesperado, ya que en los ESET Security Report de años previos hemos visto que el porcentaje de este tipo de incidencias se mantenía en los primeros lugares.

Desde 2010 hasta 2012 se percibía que la cantidad de infectados por *malware* aumentaba, sin embargo, en 2013 sucedió algo atípico: disminuyó. El historial a lo largo de los años puede observarse en el **Gráfico 10**.

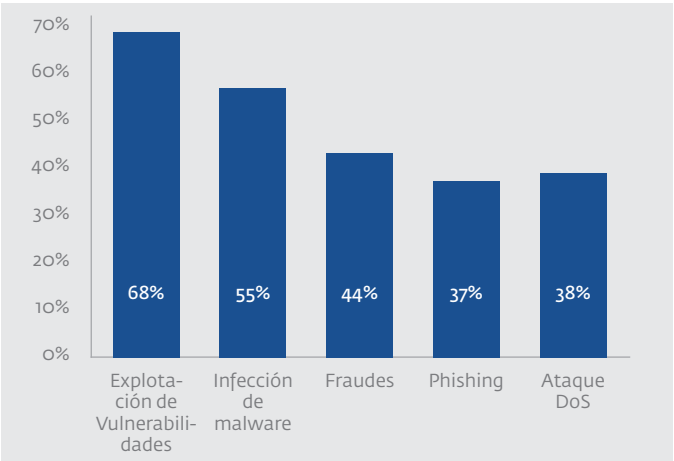
| Gráfico Nº 10 |
Infecciones de malware en los últimos cuatro años



Continuando con el análisis de incidencias, se puede observar que los casos de fraude son los de menor ocurrencia en el último año. Curiosamente, los casos de acceso indebido representan un número considerable debido a que este tipo de incidentes son de los más fáciles de prevenir (a diferencia por ejemplo de las infecciones de *malware*).

Las empresas también se preocupan por evitar los casos de fraude, aunque como se expuso previamente este tipo de incidentes son los que menos suceden. Los casos de *phishing*, que son los más habituales luego de las infecciones de *malware*, son casi los que menos preocupan a las empresas, delante de los ataques de denegación de

| Gráfico Nº 12 |
Preocupaciones de las empresas en materia de seguridad



68% De las empresas temen la explotación de vulnerabilidades

servicio (ver **Gráfico 12**).

Las realidades que se perciben de cada país no son contrastantes

Al analizar los índices de incidentes por país puede apreciarse en líneas generales que los cambios no son bruscos. Los detalles pueden verse en el **Gráfico 13**.

Se observa que las empresas de Nicaragua y Venezuela mantienen alineadas sus preocupaciones en materia de seguridad respecto a los incidentes sucedidos en los últimos 12 meses. Por otro lado, en El Salvador, Panamá y Colombia la falta de disponibilidad se presenta como el segundo incidente con más ocurrencias, detrás de las infecciones de *malware*. Luego de estas consideraciones, se observa que los demás países se mantienen en los lineamientos ya analizados previamente.

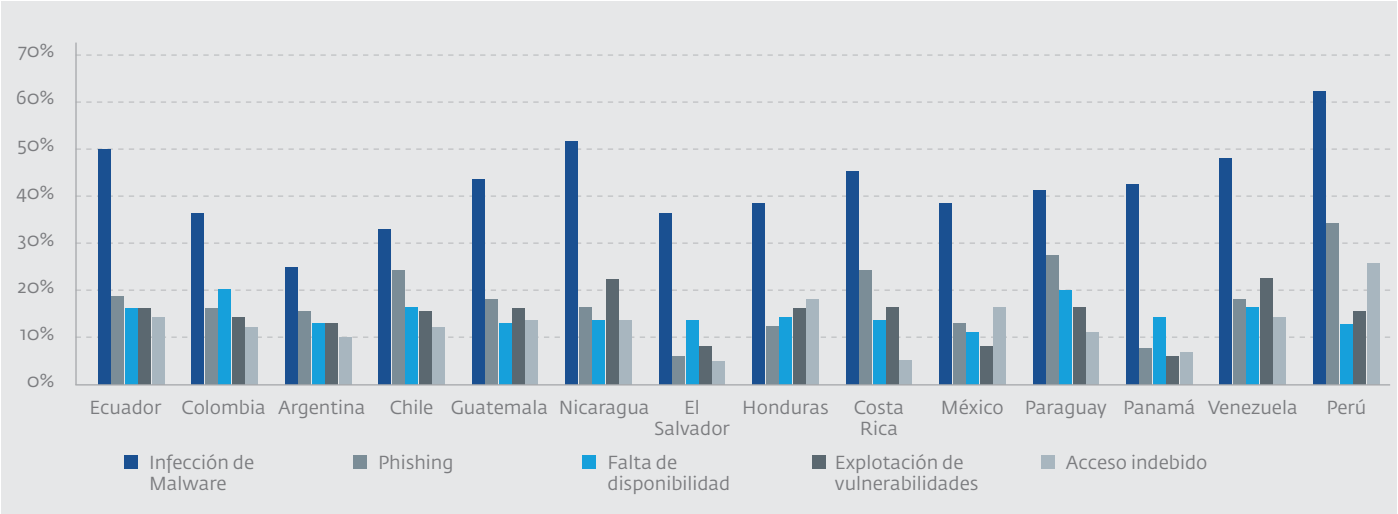
El Análisis de riesgos, la herramienta clave

El criterio de las empresas latinoamericanas no es desacertado, ya que ven a las infecciones de *malware* como un vector de riesgo y las estadísticas demuestran que se encuentra primero en cantidad de incidencias. Sin embargo, les preocupa en mayor medida la explotación de vulnerabilidades (ver **Gráfico 12**), y esto es un poco discorde con lo analizado previamente, ya que no figura ni siquiera en los primeros tres lugares de los incidentes más comunes.

En este sentido, el análisis de riesgos sería apropiado para enfocar de manera óptima los recursos para protegerse de futuras incidencias. De todas formas, es importante reiterar que aunque el enfoque actual pueda recibir mejoras, no es desatinado.

| Gráfico Nº 13 |

Incidentes por país en los últimos 12 meses



Conclusiones

A través de todas las estadísticas presentadas, se puede concluir que las empresas invirtieron más recursos en seguridad y que sus departamentos de Seguridad Informática cobraron más relevancia, no obstante, no toman total conciencia de la magnitud que podrían tener los incidentes internos. Por esta razón, es necesario concientizar y establecer controles sobre lo que se encuentra puertas hacia dentro y representa el capital más importante: sus colaboradores.

La actualidad empresarial latinoamericana presenta empresas que en general implementan los controles de seguridad más habituales y reconocidos. Sin embargo, no realizan actividades para prevenir incidentes relacionados con sus trabajadores; por lo tanto este índice debería incrementarse.

En la misma línea, se observa que las políticas de BYOD no son algo común. La conectividad seguirá incrementándose debido al crecimiento de dispositivos (como los *wearables*), por lo que es necesario que se tomen más en serio para no estar frente a un vector de riesgo para la Seguridad de la Información de la empresa.
Otra área de mejora es la capacidad de reacción. La mayoría de las empresas latinoamericanas cuenta con una política de seguridad definida, pero las que presentan prácticas de gestión ante incidentes es significativamente menor. Es fundamental, entonces, aumentar la prioridad de este tipo de gestiones porque una empresa que no las implemente quedará potencialmente indefensa ante un incidente de seguridad ocurrido.

Por otro lado, el aumento de las actividades educativas en la empresa es interesante, ya que logrará que los incidentes de seguridad disminuyan. Por ejemplo, los casos de *phishing* (que ocupan el tercer lugar en la lista de incidencias) disminuirían gracias a empleados mejor preparados para reconocerlos y reaccionar ante ellos.

En comparación a reportes anteriores, este año se ven cambios en cuanto a la estructura del área de Seguridad Informática ya que ahora está asociada a IT, pero como un departamento exclusivo dedicado a proteger la disponibilidad, integridad y confidencialidad de la información.

Sin embargo, es importante notar que este modelo no es eficiente para empresas de gran envergadura o de crecimiento constante, donde lo que concierne a Seguridad de la Información relaciona a varias áreas a la vez. Por eso, es importante que el enfoque del área en cuestión se encuentre estrictamente ligado hacia las planificaciones de crecimiento de las empresas.

Se ha visto, además, que la explotación de vulnerabilidades y las infecciones de *malware* son las amenazas de mayor preocupación, por lo que todos los esfuerzos se enfocan en ellas. Sin embargo, este plan de acción no es del todo acertado, ya que no se condice con los incidentes reales de 2013. Con pocas variaciones a lo largo de toda la región, los indicadores confirman que el *phishing* también ocupa un lugar considerable (tercer puesto), y que la explotación de vulnerabilidades no tiene tanto peso como el que las empresas perciben.

En general, los esfuerzos de las empresas por protegerse no son errados, aunque podrían optimizarse bastante. Una herramienta muy útil es la realización de análisis de riesgos, ya que determinarán los puntos más débiles de la estructura y que requieren mayor atención.

En conclusión, durante 2013 muchas empresas consolidaron su departamento de Seguridad Informática y aumentaron las actividades periódicas de educación para los colaboradores. Sin embargo, deben intensificar el trabajo de *awareness* interno para asegurar ese vector de riesgo, como también analizar la inclusión de políticas de BYOD. Por último, tanto el plan de reacción ante incidentes, como las gestiones en general pueden recibir mejoras para que los esfuerzos y recursos de las compañías estén alineados a los incidentes más populares en el mundo real, en lugar de aquellos que los preocupan, pero que son menos frecuentes.

ESET Latinoamérica

Con 25 años de trayectoria en la industria de la seguridad de la información, ESET es una compañía global de soluciones de software de seguridad, creadora del legendario ESET NOD32 Antivirus y orientada a proveer protección de última generación contra amenazas informáticas. Actualmente cuenta con oficinas centrales en Bratislava (Eslovaquia) y de Coordinación en San Diego (Estados Unidos) Buenos Aires (Argentina) y Singapur. Además, posee otras sedes en Londres (Reino Unido), Praga (República Checa), Cracovia (Polonia), Jena (Alemania) San Pablo (Brasil) y México DF (México). Desde el 2004, ESET opera para la región de América Latina en Buenos Aires, Argentina, donde dispone de un equipo de profesionales capacitados para responder a las demandas del mercado en forma concisa e inmediata y un Laboratorio de Investigación focalizado en el descubrimiento proactivo de variadas amenazas informáticas.

Juan Díaz de Solís 1270 - 2do. Piso - C.P 1638 - Buenos Aires, Argentina
Tel.: + 54 11 5171 ESET (3738) - Fax.: +54 11 5171-3739 - www.eset-la.com