ESET Security Report
Latinoamérica 2016

ENJOY SAFER TECHNOLOGY™

CONTENIDO

Introducción 03

01 **¿Cuáles son las preocupaciones de los encargados de la seguridad en empresas de Latinoamérica?** 04

1.1 Vulnerabilidades de software y sistemas 05
1.2 Malware 06
1.3 Acceso indebido a la información 07

02 **¿Qué incidentes de seguridad padecieron las empresas durante 2015?** 08

2.1 Malware 09
2.2 Phishing 11

03 **¿Cuáles son las medidas de seguridad aplicadas en las empresas latinoamericanas?** 14

3.1 Controles tecnológicos 14
3.2 Prácticas de gestión 15
3.3 Estándares y mejores prácticas 16
3.4 Educación y concientización 18
3.5 Roles y responsabilidades en seguridad 19
3.6 Presupuesto para la seguridad 20

Conclusiones 21

Introducción

Durante 2015 ESET Latinoamérica participó en diversos eventos corporativos, relacionados con la industria de Seguridad de la Información, a lo largo de toda la región. Una actividad realizada en estas jornadas consta de entregar encuestas a los asistentes- que son ejecutivos, gerentes y administradores de IT de empresas- con el propósito de conocer el estado de la seguridad en las compañías latinoamericanas.

Seguidamente, los datos son analizados y presentados en el ESET Security Report 2016, el informe que muestra el panorama de la seguridad en las empresas y que presenta cuáles son las principales preocupaciones de los encargados de tomar decisiones y brindar protección a los activos más importantes en las empresas, así como los incidentes de seguridad que más han afectado a las organizaciones en el último año.

El documento también presenta un estudio sobre las principales medidas de seguridad que se aplican para preservar la confidencialidad, integridad y disponibilidad de la información; desde controles tecnológicos o prácticas de gestión, hasta iniciativas de educación y concientización en temas de seguridad.

Además, presenta el análisis sobre la manera en la que son designadas las responsabilidades de seguridad dentro de las organizaciones, el presupuesto que se les asigna a estas áreas, así como una comparativa con los resultados del año anterior.

Resulta importante destacar que el estudio tomó en consideración 3044 encuestas aplicadas en Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú y Venezuela. Asimismo, quienes respondieron pertenecen a organizaciones de distintos tamaños y rubros, y poseen diferentes responsabilidades vinculadas con la seguridad.

+3000
Participantes de la encuesta

13
Países incluídos

¿Cuáles son las preocupaciones de los encargados de la seguridad en empresas de Latinoamérica?

58%
Vulnerabilidades de software

54%
Malware

46%
Acceso indebido a datos

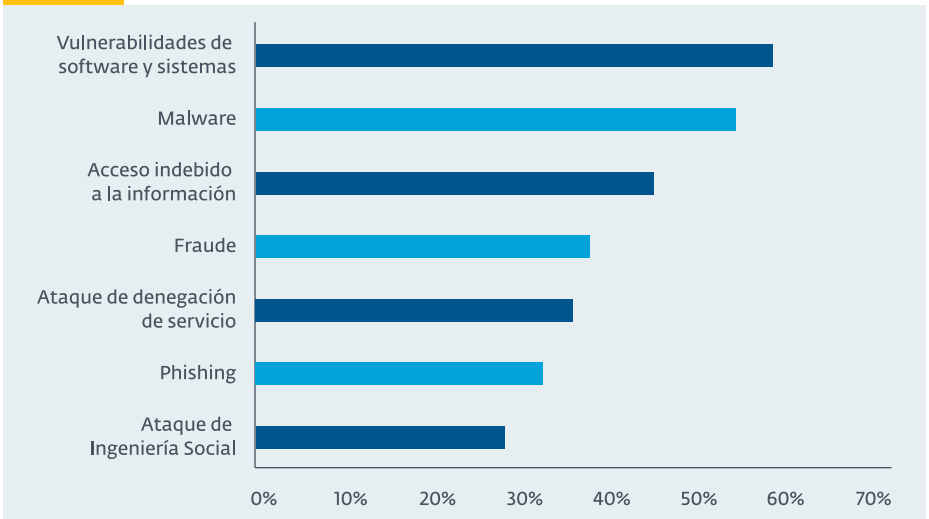
Las preocupaciones de los equipos de seguridad en las empresas pueden determinarse a través de distintos factores, como las tendencias en materia de amenazas informáticas o los incidentes de seguridad más comunes. La atención proactiva de estas inquietudes contribuye a evitar la materialización de los riesgos asociados a la Seguridad de la Información.

Por ello, resulta relevante conocer las amenazas que pueden afectar con más frecuencia al negocio. De acuerdo con los resultados de la encuesta, la principal preocupación son las "Vulnerabilidades de software y sistemas" con el 58% de las respuestas afirmativas, seguido por el "Malware" (54%) y, en el tercer puesto, el "Acceso indebido la información" (46%).

Al comparar estos resultados con los presentados en el ESET Security Report 2015 es posible ver que dos de las preocupaciones se mantuvieron en el mismo lugar: vulnerabilidades de software y malware.

Esto tiene sentido especialmente al realizar un recuento de los sucesos vinculados con las vulnerabilidades de software (incluyendo las fallas 0-day que no son conocidas por los fabricantes y pueden estar siendo explotadas), junto con las campañas de propagación e infección de códigos maliciosos.

GRÁFICO 1



Preocupaciones en materia de Seguridad de la Información en las empresas de Latinoamérica.

Sin embargo, lo que se destaca durante 2015[1], es que por primera vez desde que se realiza este informe, el fraude informático no ocupa el tercer lugar; ya que fue desplazado por el acceso indebido a la información. Esto se explica desde el aumento de la explotación de vulnerabilidades (la preocupación más importante), que generalmente tiene como consecuencia el acceso indebido, razón por la que ambos riesgos pudieron haber crecido proporcionalmente.

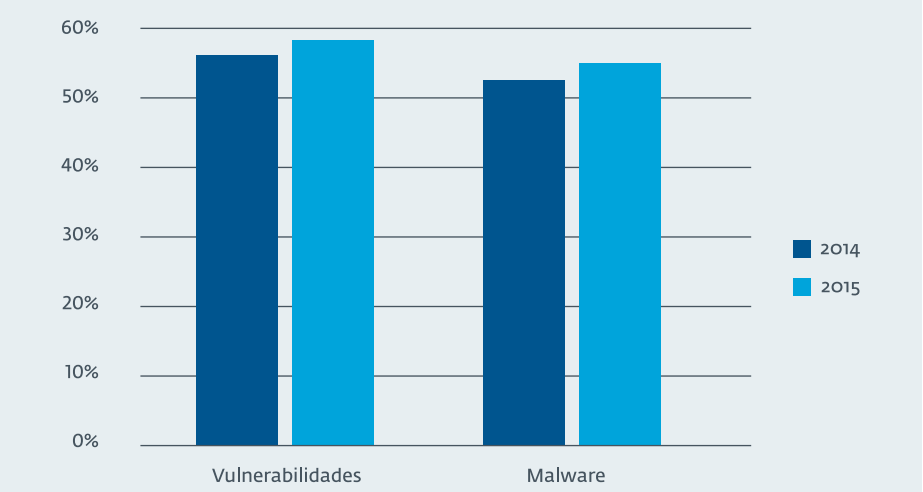
Por otro lado, el aumento en las principales preocupaciones también evidencia un incremento en la concientización de los usuarios. El acceso a mayor y mejor información se traduce en más educación, especialmente sobre las amenazas más comunes de la actualidad. Cabe destacar que este es el primer paso para evitar estos incidentes y, en caso de que no sea posible, que las consecuencias sean las mínimas aceptables.

1.1. Vulnerabilidades de software y sistemas

Desde 2013, las vulnerabilidades de software y sistemas se han posicionado como la principal preocupación de acuerdo con los resultados del ESET Security Report. Este punto se ve reflejado en los casos de vulnerabilidades que se mediatizaron, como Heartbleed[2] (relacionado con una falla de seguridad en OpenSSL), Shellshock[3] (una vulnerabilidad en Bash) o Poodle[4] (que afectaba a SSL 3.0).

En este sentido, 2015 no fue menos. Se descubrió Freak[5], una vulnerabilidad en el protocolo de cifrado HTTPS. El mundo de los dispositivos móviles también se vio afectado por vulnerabilidades de mayor impacto; en Android se conoció el caso de Stagefright[6], una falla en esta biblioteca de medios utilizada para gestionar formatos de vídeo o música, y que se podía explotar a través de un mensaje multimedia (MMS).

GRÁFICO 2



Preocupaciones en materia de Seguridad de la Información en los últimos dos años.

1 - ESET Security Report 2015: http://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf
2 - 5 cosas que debes saber sobre Heartbleed. http://www.welivesecurity.com/la-es/2014/04/09/5-cosas-debes-saber-sobre-heartbleed/
3 - #Shellshock, la grave vulnerabilidad en Bash -y todo lo que debes saber. http://www.welivesecurity.com/la-es/2014/09/26/shellshock-grave-vulnerabilidad-bash/
4 - Poodle, la vulnerabilidad en SSL 3.0 y cómo te podría afectar. http://www.welivesecurity.com/la-es/2014/10/15/poodle-vulnerabilidad-ssl-3/
5 - FREAK attack: vulnerabilidad rompe la protección HTTPS. http://www.welivesecurity.com/la-es/2015/03/04/freak-attack-vulnerabilidad-rompe-la-proteccion-https/
6 - Stagefright: comprometiendo Android con solo un mensaje. http://www.welivesecurity.com/la-es/2015/07/28/stagefright-comprometiendo-android-un-solo-mensaje/

En cuanto a iOS, se descubrió Xcodeghost[7], que le permitía a los ciberdelincuentes infectar el compilador (XCode) utilizado para crear las aplicaciones en el sistema operativo móvil de Apple. De esta forma, los desarrolladores incluían código malicioso en sus aplicaciones sin saberlo y, al estar firmadas por el desarrollador legítimo, podrían será alojadas en la App Store sin objeciones.

Los últimos dos casos resultan particularmente relevantes al considerar que los dispositivos móviles son cada vez más utilizados para desempeñar actividades dentro y fuera de las empresas. Del mismo modo, estos incidentes aclaran por qué las vulnerabilidades de software no solo siguen siendo la principal preocupación de las empresas de la región, sino también una tendencia creciente.

1.2. Malware

Los códigos maliciosos se posicionan como la segunda causa de preocupación en las empresas. Esta problemática es sin duda una de las más importantes y cada día adquiere más relevancia, ya que se dejó de lidiar con incipientes amenazas como los virus, para tener que enfrentar software malicioso cada vez más sofisticado, que tiene como propósito principal generar réditos económicos para sus creadores.

Nuevas amenazas relevantes

BOTNETS

RANSOMWARE

En esta línea, es posible indicar que las campañas de malware hacen referencia a la propagación masiva de códigos maliciosos, generalmente utilizadas para robar información de los usuarios, aunque también se han identificado ataques dirigidos que emplean software malicioso para afectar a las empresas. Para ello utilizan vectores comunes de propagación, como correos electrónicos con archivos adjuntos o enlaces que instan a descargar la amenaza, para luego continuar a través de dispositivos USB, o bien, mediante sitios web vulnerados que redirigen a sus visitantes a diferentes tipos de exploits.

En los últimos años, dos tipos de amenazas han cobrado relevancia, por un lado las redes de computadoras zombis (también conocidas como botnets), que tienen un rol preponderante dentro de un modelo utilizado para la compra y venta de servicios dentro del mundo del cibercrimen. Los cientos o miles de computadoras que forman parte de este tipo de redes pueden ser utilizadas para diversas actividades maliciosas como el envío de spam, ataques de Denegación de Servicio, la propagación de más códigos maliciosos o el robo de información.

Por otro lado, el ransomware también adquirió mucha relevancia dentro del cibercrimen. Este tipo de programa malicioso aplica el principio del secuestro para, luego, solicitar un rescate a la víctima. Ya sea a través de impedir el acceso a la información mediante el cifrado de los archivos (criptoransomware) o a los sistemas (ScreenLocker), el cibercriminal se beneficia de manera económica en un tiempo cada vez menor, si se lo compara con el malware que busca robar información para, posteriormente, venderla.

De acuerdo con la información de los laboratorios de ESET a nivel mundial, se identifican más de 200 mil nuevas variantes de códigos maliciosos por día. Por ello, no es casual que se trate de una de las principales preocupaciones para los equipos de seguridad y se mantenga, un año más, en el segundo peldaño.

7 - XCodeGhost: apps para iOS infectadas desde su creación. http://www.welivesecurity.com/la-es/2015/09/21/xcodeghost-apps-ios-infectadas/

1.3. Acceso indebido a la información

En línea con las vulnerabilidades se encuentra el acceso indebido a la información, ya que las debilidades y fallos de programación identificados en el software son utilizados, entre otros motivos, para acceder a los sistemas. Una vez logrado este propósito, los cibercriminales comúnmente intentan robar datos confidenciales.

Un agravante que se ha dado en los últimos tiempos es el delito conocido como "haxposición"[8] : un término que surge de la combinación del hacking y la exposición de datos, y representa una amenaza emergente con importantes implicaciones para el correcto funcionamiento de los negocios. La idea central es que la intrusión a un sistema no termina con el robo de datos, sino que involucra la exposición de esa información, lo que se traduce en daños a la imagen de la organización víctima.

Los casos emblemáticos de 2015 son, sin duda, la filtración de información confidencial de Hacking Team[9] que tuvo como resultado la publicación de las empresas y gobiernos que habían adquirido su herramienta de espionaje, con las implicaciones éticas que esto conlleva.

Asimismo, se encuentra el caso de Ashley Madison[10], el ataque al sitio de citas extramatrimoniales que puso en evidencia a 37 millones de usuarios registrados, entre ellos funcionarios públicos, profesionales, padres y madres cuyos affairs se hicieron públicos.

Casos resonantes

HACKING TEAM

ASHLEY MADISON

8 - ¿Sabes qué es la haxposición? Conoce a esta amenaza emergente. http://www.welivesecurity.com/la-es/2016/02/10/que-es-haxposicion-amenaza-emergente/

9 - Filtran 400GB de información confidencial del grupo Hacking Team. http://www.welivesecurity.com/la-es/2015/07/06/filtran-400gb-de-informacion-confidencial-del-grupo-hacking-team/

10 - Caso Ashley Madison: la cronología de los hechos. http://www.welivesecurity.com/la-es/2015/08/31/caso-ashley-madison-cronologia/

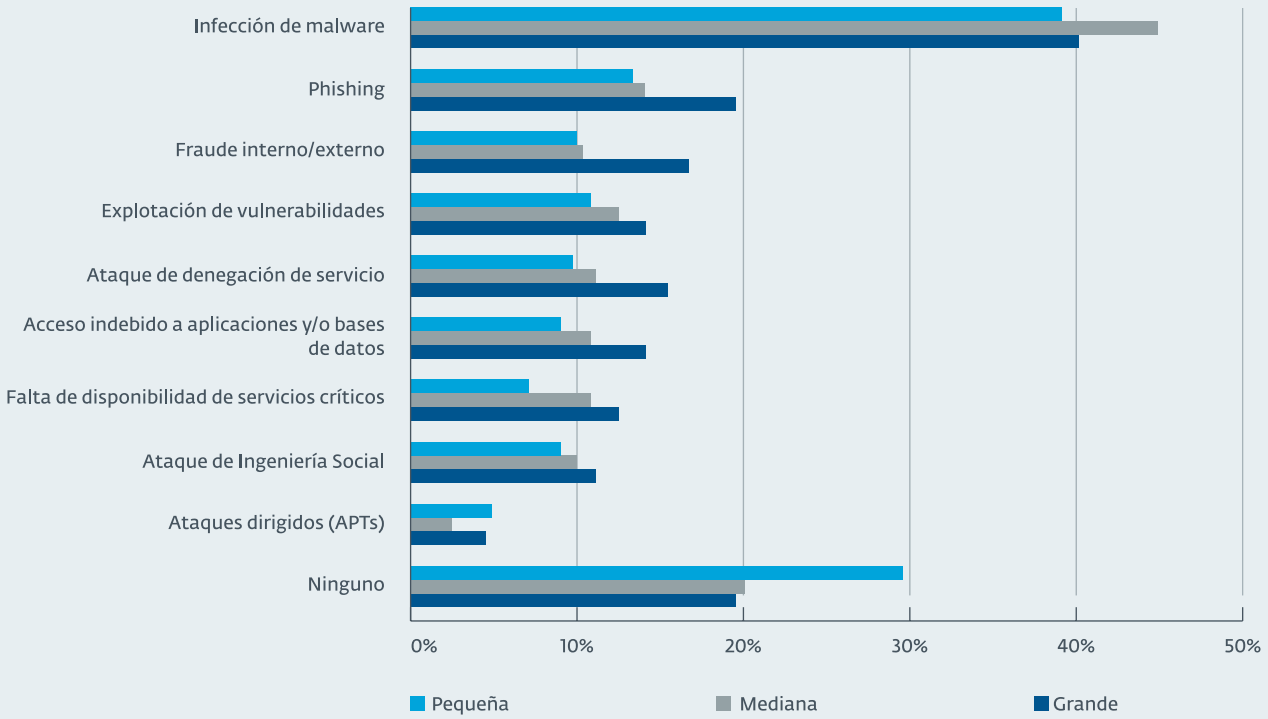
¿Qué incidentes de seguridad padecieron las empresas durante 2015?

La segunda sección del ESET Security Report 2016 se centra en conocer los principales incidentes de seguridad que afectaron a las empresas. Para ello se han considerado los eventos indeseados e inesperados más comunes, que tienen una probabilidad significativa de comprometer las operaciones de las organizaciones y atentar contra la confidencialidad, integridad o disponibilidad de la información.

Como ya fue señalado, existe una relación entre las preocupaciones y los incidentes, por ello no es de extrañar que el malware aparezca como la segunda preocupación en la categoría anterior y como la principal causa de incidentes en las empresas durante 2015.

El gráfico 3 presenta el porcentaje de incidentes de seguridad clasificados por el tamaño de las empresas. Los resultados indican que, en promedio, la "Infección por malware" ocupa el primer lugar con el 40% de respuestas afirmativas, mientras que en segunda posición se ubican los casos de "Phishing" con el 16% y en la tercera el "Fraude interno/externo" con el 13%.

GRÁFICO 3



Incidentes de Seguridad de la Información en las empresas de Latinoamérica (por tamaño de empresa).

Ahora bien, ¿por qué las vulnerabilidades de software son la principal preocupación a pesar de que el malware es la principal causa de incidentes? Para responder este interrogante es necesario aclarar que el malware es masivo y la explotación de vulnerabilidades es menos frecuente. Sin embargo, este último incidente es más difícil de detectar y, de ocurrir, puede impactar con mucha mayor fuerza en la organización. Por esta razón, sigue siendo la principal preocupación.

Un dato interesante es que casi el 30% de las empresas pequeñas afirmó no haber padecido ningún incidente de seguridad, mientras que en el resto de las categorías, las empresas medianas y grandes reportaron un mayor número de incidentes.

Esto puede analizarse desde dos perspectivas: por un lado, que las empresas de mayor tamaño resulten ser un objetivo más relevante para los atacantes dejando de lado a las más pequeñas; o bien, que las empresas pequeñas son atacadas al igual que el resto, pero resulta más difícil que puedan identificar este tipo de amenazas (y en consecuencia erradicarlas), ya que en la mayoría de las veces buscan pasar inadvertidas.

En promedio, el 22% de los encuestados afirmó no haber padecido un incidente de seguridad dentro de la empresa en la que trabajan, un dato que se redujo respecto a los años anteriores (23% en 2014 y 25% en 2013). Pero al mismo tiempo indica que el promedio de las empresas que sí padecieron un incidente se incrementó respecto a los años anteriores, pasando de 75% en 2013 a 78% en 2015.

40%
Malware

16%
Phishing

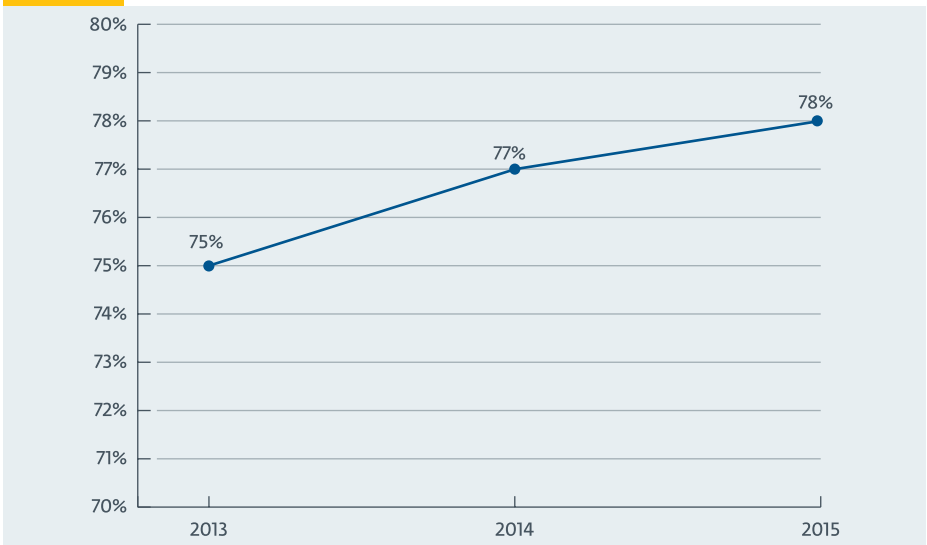
13%
Fraude interno/externo

22%
Ningún incidente reportado

2.1. Malware

Como se mencionó anteriormente, los códigos maliciosos se han convertido en amenazas que han crecido en cantidad, complejidad y diversidad. 2015 comenzó con una nueva oleada de ransomware a través de la aparición de CTB-Locker[11], con la particularidad de que podía ser descargado al equipo de la víctima utilizando un TrojanDownloader, es decir, un código malicioso del tipo troyano encargado de descargar y ejecutar una segunda amenaza encubierta.

GRÁFICO 4



Porcentaje de las empresas que reportaron incidentes

11 - CTB-Locker, el ransomware ataca de nuevo. http://www.welivesecurity.com/la-es/2015/01/20/ctb-locker-ransomware-ataca-nuevo/

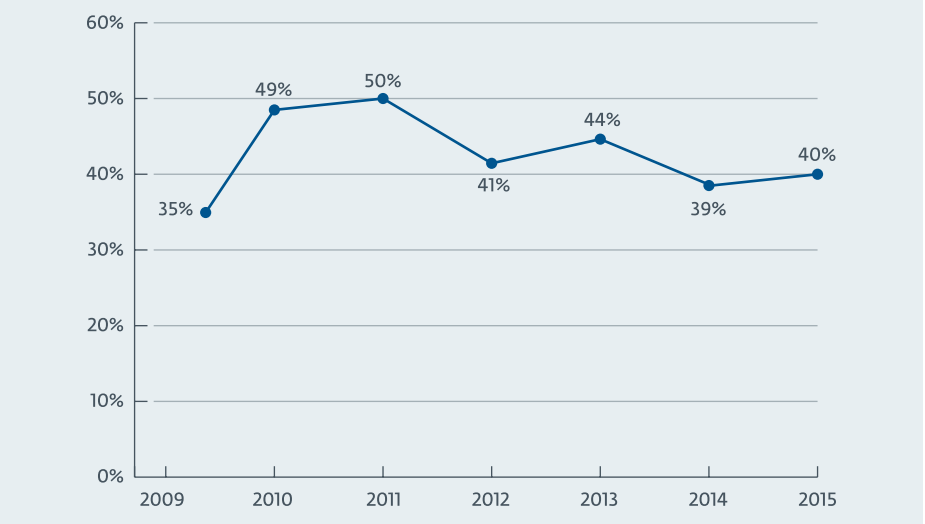
Con el paso de los meses, aparecieron nuevas versiones para plataformas móviles como el "Virus de la policía" para Android, o versiones para sistemas operativos Linux y Mac. El caso más reciente es una variante que ahora busca afectar servidores web[12].

En el mismo sentido, la proliferación de malware del tipo bot ha afectado particularmente a Latinoamérica, donde se han detectado amenazas como Dorkbot, Neurevt o Dridex. Durante el año pasado se identificaron diferentes oleadas de malware en países de la región, como el caso de los troyanos bancarios propagados en Brasil a través del uso de malware CPL (Control Panel Application)[13]. En la misma línea, se vieron las campañas de propagación de malware a través de VBA/TrojanDownloaders[14], en la mayoría de los casos con un enfoque hacia usuarios mexicanos.

También se conoció la "Operación Liberpy"[15], una campaña de propagación e infección de malware, que afectó a varios países de Latinoamérica, enfocándose particularmente en los usuarios de Venezuela. El Laboratorio de Investigación de ESET Latinoamérica desmanteló esta botnet que se dedicaba a robar información de los usuarios.

En el mismo sentido, ESET ha colaborado para interrumpir la actividad de la botnet Dorkbot[16] a través del redireccionamiento del tráfico de sus servidores de C&C (sinkhole), que desde 2011 había afectado a usuarios latinoamericanos. ESET compartió el análisis técnico, información estadística, dominios, así como direcciones IP de los servidores de Comando y Control conocidos con Microsoft, CERT.PL y diversas agencias policiales de todo el mundo.

GRÁFICO 5



Infecciones por malware entre 2009 y 2015.

12 - Sitios cifrados: el ransomware CTB-Locker ahora busca afectar servidores web. http://www.welivesecurity.com/la-es/2016/03/01/sitios-cifrados-ransomware-ctb-locker-servidores/
13 - Nuevo paper de ESET: CPL malware y troyanos bancarios al acecho en Brasil. http://www.welivesecurity.com/la-es/2015/05/07/paper-eset-cpl-malware-brasil/
14 - Macro malware a la mexicana: falsos documentos bancarios y botnets. http://www.welivesecurity.com/la-es/2015/06/11/macro-malware-mexico-falsos-documentos-bancarios-botnets/
15 - Operación Liberpy: keyloggers en Latinoamérica. http://www.welivesecurity.com/la-es/2015/07/14/operacion-liberpy-keyloggers-latinoamerica/
16 - Interrupción de la botnet Dorkbot tras un esfuerzo conjunto. http://www.welivesecurity.com/la-es/2015/12/04/interrupcion-botnet-dorkbot-esfuerzo-conjunto/

Los sucesos anteriores evidencian que los códigos maliciosos se han mantenido como uno de los causantes más relevantes de incidentes de seguridad en las empresas latinoamericanas. Tal como puede observarse en el Gráfico 4, un dato no menor es que la cantidad de empresas que han reportado incidentes ha ido creciendo en los últimos años. Asimismo, otros resultados también muestran esta tendencia, con cambios ligeros en los últimos siete años. En 2009 el 35% de los encuestados afirmó haber sufrido infecciones por malware, mientras que en 2015 el número aumentó al 40% (Gráfico 5).

Al analizar los resultados de la encuesta para conocer en qué países las empresas se vieron más afectadas por códigos maliciosos, Nicaragua ocupa el primer lugar con el 58.3% de las respuestas afirmativas, seguido de Guatemala con el 55.8% y Ecuador con 51.9%, tal como se puede observar en el gráfico 6.

Asimismo, el Gráfico 6 muestra los resultados completos de la encuesta, donde Argentina (29.7%), Chile (29.2%) y Venezuela (24.1%) resultaron los países menos afectados por casos de malware en las empresas.

2.2. Phishing

Es destacable que en esta nueva ocasión el phishing aparezca en el segundo lugar de los incidentes de seguridad más frecuentes, ya que a pesar de ser una técnica cada vez más conocida y relativamente fácil de detectar, logra su objetivo a través de la aplicación efectiva de técnicas de Ingeniería Social. En otras palabras, sus creadores buscan explotar vulnerabilidades en las personas.

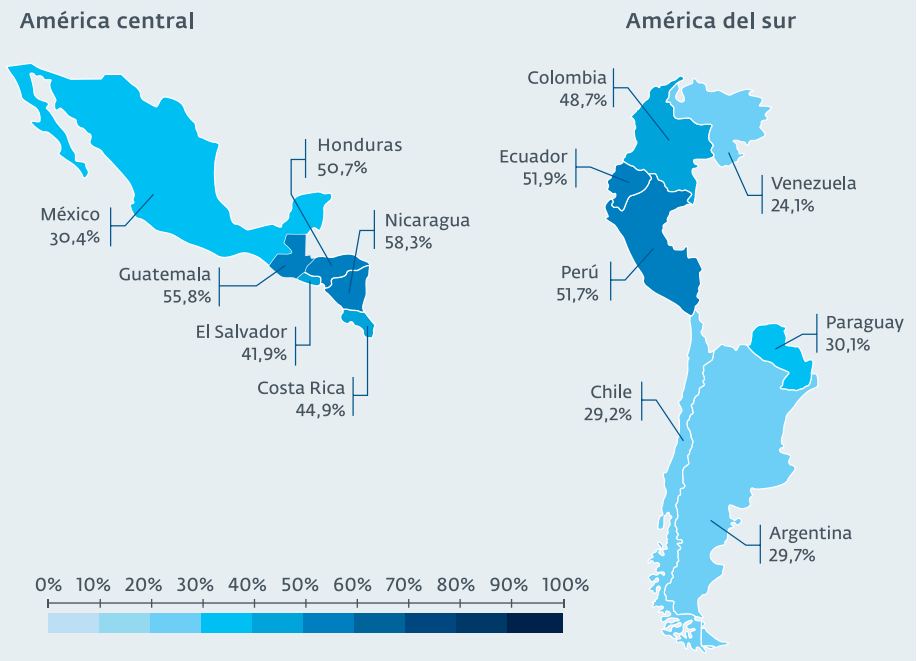
Países más afectados por Malware

NICARAGUA
58,3%

GUATEMALA
55,8%

ECUADOR
51,9%

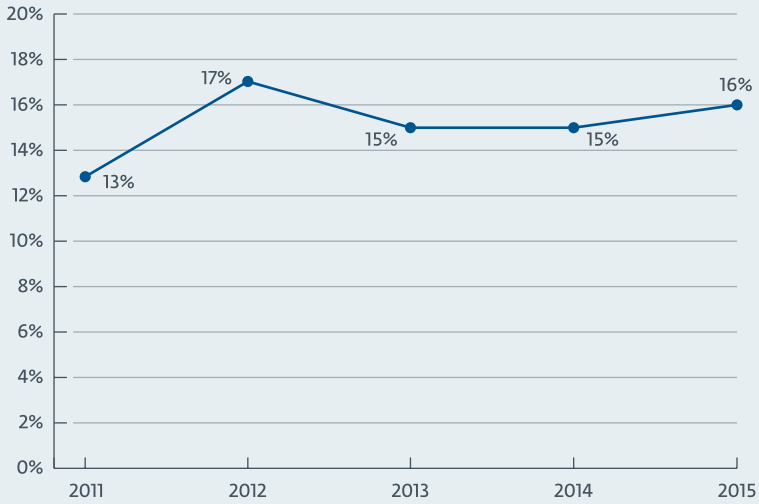
GRÁFICO 6



Empresas afectadas por infecciones de malware (por país).

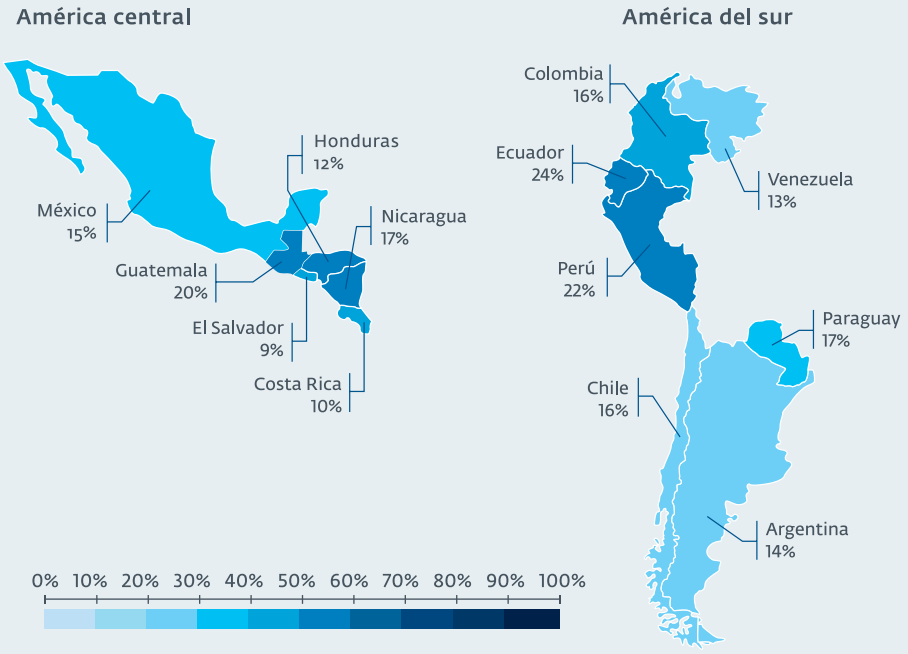
Continuamente se observan campañas enfocadas a obtener contraseñas e información confidencial de los usuarios a través de la suplantación de entidades reconocidas en los países en cuestión, principalmente de instituciones bancarias. Este tipo de técnicas buscan llegar a la mayor cantidad posible de potenciales víctimas, aunque en los últimos años, han cambiado este propósito.

GRÁFICO 7



Casos de phishing en los últimos 5 años.

GRÁFICO 8



Empresas afectadas por phishing (por país).

El uso de ataques de phishing con objetivos específicos, lo que se ha denominado *spear phishing*, cobró más relevancia en los últimos tiempos. Se trata de una técnica similar al phishing tradicional, con la diferencia de que no busca tener un alcance masivo, por el contrario, el falso mensaje está dirigido a un grupo u organización específico.

El cambio de paradigma adquiere importancia si se tiene en mente a los investigadores que afirmaron haber encontrado suficiente información y evidencia para determinar que la fuga de información confidencial de Sony[17], en 2014, tuvo su origen en un ataque dirigido de spear phishing. Este incidente alcanzó a varios administradores de sistema con correos electrónicos bien elaborados que suplantaban el proceso de autenticación de Apple ID, lo que desencadenó la fuga de información sensible (correos confidenciales y hasta películas no estrenadas) y la propagación de amenazas a los empleados.

De acuerdo con los resultados del ESET Security Report, durante los últimos cinco años el phishing se mantuvo como una amenaza constante que comienza a cobrar relevancia nuevamente, sobre todo si se considera que continuamente aparecen campañas que buscan engañar a los usuarios[18] y que, en ocasiones, se trata de ataques dirigidos.

Al analizar los resultados de las encuestas, es posible ver que los países más afectados por casos de phishing son Ecuador (24%), seguido por Perú (22%) y Guatemala (20%); el mapa completo de la región se puede ver en el gráfico 8.

Como lo muestra el Gráfico 8, los países menos afectados son Honduras con 12%, Costa Rica con 10% y El Salvador con el 9%.

Países más afectados por Phishing

ECUADOR
24%

PERÚ
22%

GUATEMALA
20%

17 - Investigadores afirman que el ataque a Sony se debió a un spear phishing. http://www.welivesecurity.com/la-es/2015/04/24/afirman-ataque-sony-phishing/

18 - Nuevo caso de phishing afecta a usuarios de Santander. http://www.welivesecurity.com/la-es/2015/09/15/caso-phishing-afecta-usuarios-santander/

¿Cuáles son las medidas de seguridad aplicadas en las empresas latinoamericanas?

77%
Software antivirus

71%
Firewall

63%
Backup de información

Los recursos que son asignados para la implementación de controles de seguridad e iniciativas orientadas a mejorar y aumentar las medidas de protección son, generalmente, el resultado de un estudio de los aspectos antes descritos: las preocupaciones e incidentes de seguridad registrados, que al mismo tiempo pueden estar acompañados de evaluaciones de riesgos.

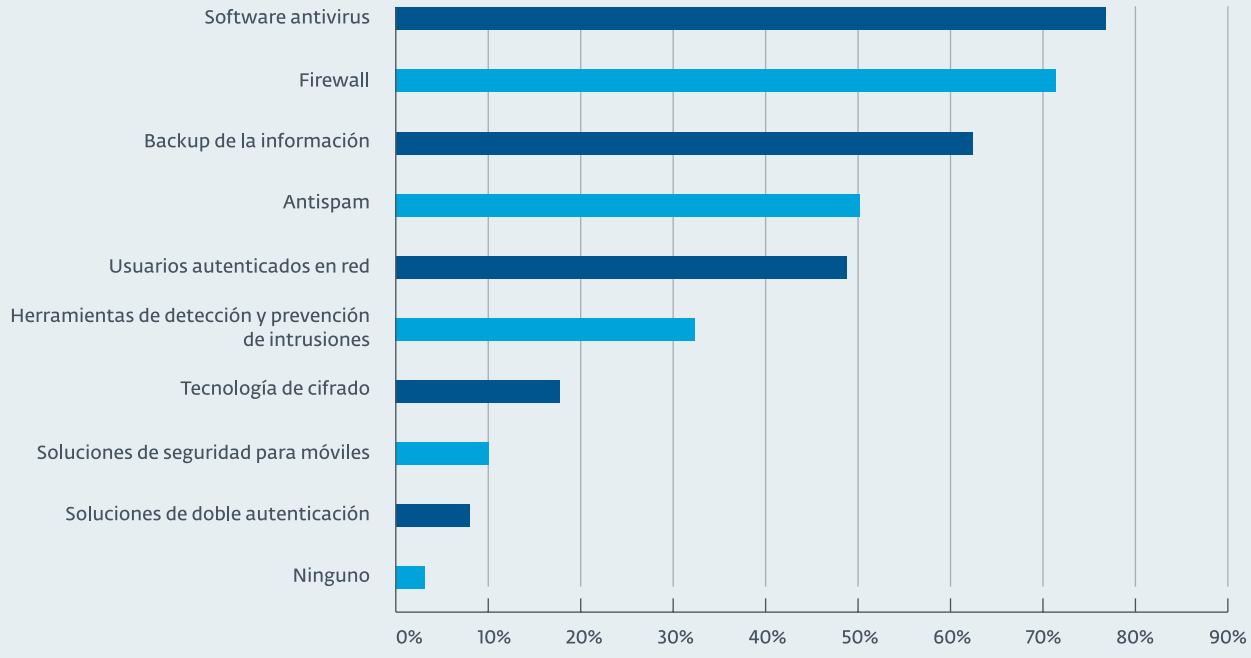
Es importante subrayar que el propósito de los controles es la mitigación de los riesgos que pueden comprometer la información más sensible o crítica dentro de las organizaciones.

Ante este escenario, los controles tecnológicos, las prácticas de gestión, así como la educación y concientización en temas de seguridad, juegan un papel determinante para alcanzar las metas en materia de Seguridad de la Información.

3.1. Controles tecnológicos

De acuerdo con los resultados de la encuesta, las empresas en Latinoamérica destinan recursos para la implementación de soluciones de software antivirus en primer lugar con el 77% de las respuestas afirmativas, seguido de firewalls con 71% y respaldos de información con 63%.

GRÁFICO 9



Controles de seguridad tecnológicos utilizados en las empresas de la región.

Es interesante observar que el principal control tecnológico de seguridad es el antivirus y que, a su vez, la causa más importante de incidentes continúa siendo el malware. Esto tiene sentido si se considera, entre otras razones, que un 23% de las empresas no utilizan una solución de seguridad contra códigos maliciosos.

Además, de acuerdo con los equipos de soporte técnico, los incidentes de seguridad relacionados con malware ocurren por una inadecuada gestión de las soluciones de seguridad, la falta de actualizaciones tanto del software como de las firmas de malware, la presencia de equipos aislados sin protección o, incluso, el uso de malas prácticas, como deshabilitar la herramienta para realizar acciones que ponen en riesgo la información y los sistemas.

Otro punto a destacar es que, de acuerdo con información histórica del ESET Security Report, en los últimos siete años los tres controles de seguridad principales continúan siendo el software antivirus, el firewall y los respaldos de información.

Cada control ha tenido incrementos considerables desde 2010, aunque es claro que todavía es necesario contar con medidas de seguridad que permitan reducir aún más la cantidad de incidentes registrados en las empresas de la región.

3.2. Prácticas de gestión

En cuanto a prácticas para la gestión de la Seguridad de la Información, el primer lugar lo ocupa el desarrollo y publicación de políticas de seguridad (68%), como una medida para generar un entorno que dicte los lineamientos generales para proteger la información y otros activos. En el segundo y tercer lugar se ubican las auditorías internas/externas (36%) y la clasificación de la información (30%).

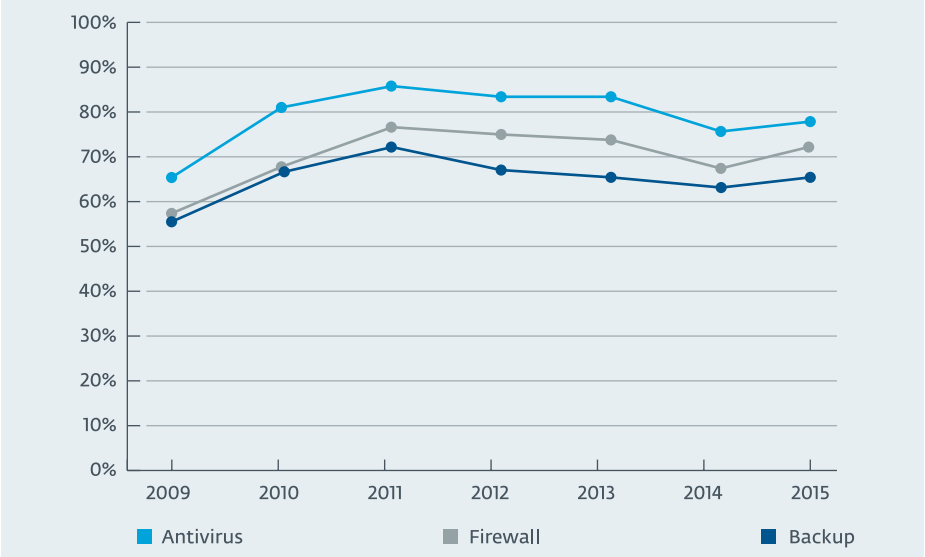
68%
Políticas de seguridad

36%
Auditorías internas/ externas

30%
Clasificación de información

Al revisar las prácticas de gestión clasificadas por tamaño de las empresas, es preciso destacar que las grandes organizaciones son las que más controles han aplicado; particularmente las políticas de seguridad, auditorías, clasificación de información y/o planes de continuidad del negocio.

GRÁFICO 10



Cambios en los controles de seguridad más utilizados en las empresas de la región.

En este sentido, también sobresale el hecho de que cerca del 20% de las empresas pequeñas no aplica este tipo de prácticas, lo que resulta razonable si se entiende que, en ocasiones, no se cuenta con los recursos necesarios para crear y mantener áreas dedicadas de forma exclusiva a la gestión de la Seguridad de la Información. El resultado de esta realidad es que las responsabilidades recaen en puestos o áreas que tienen otros roles.

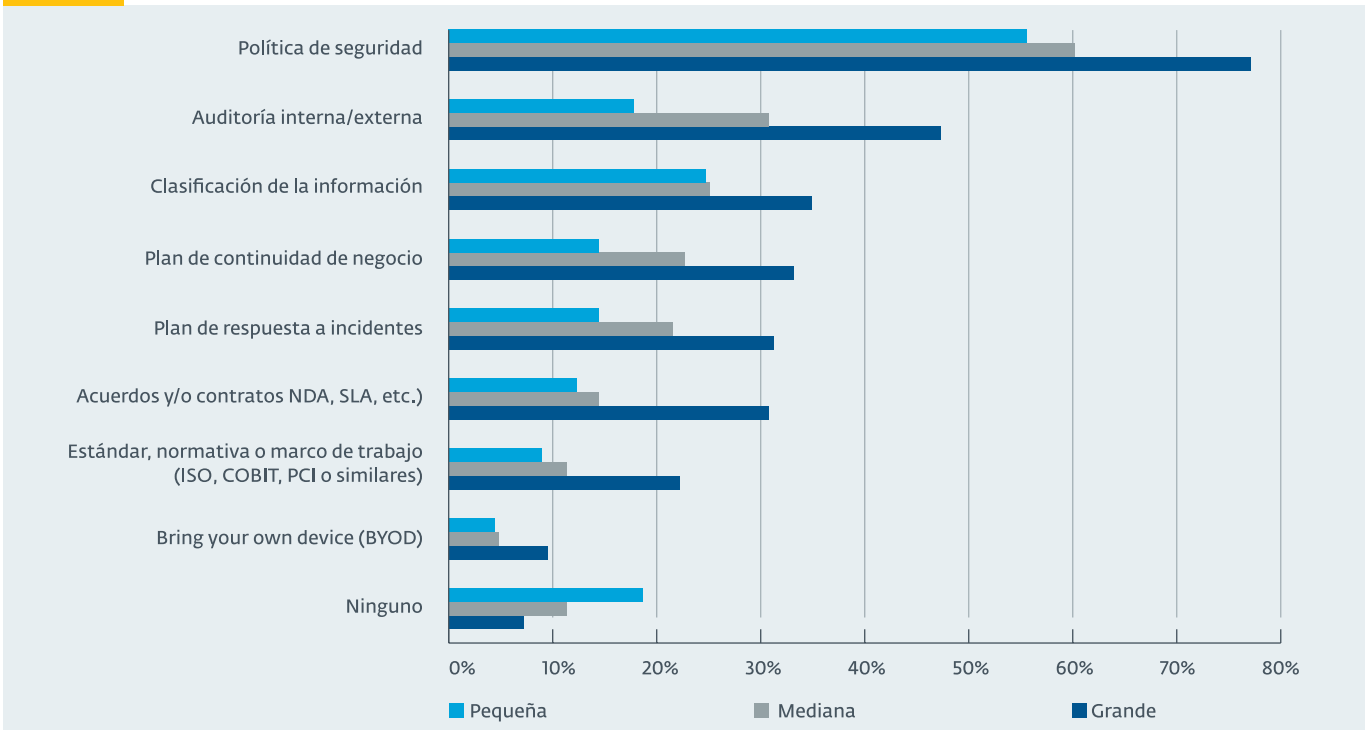
En las prácticas de gestión consideradas en la encuesta, se destaca que todas incrementaron de un año al otro y que, por el contrario, la no aplicación de dichas prácticas se redujo del 14% en 2014 al 11% en 2015. Esto sin duda expone que la Seguridad de la Información adquirió mayor relevancia dentro de las empresas, ya que una inadecuada gestión puede derivar en consecuencias adversas, incluso de gran impacto para el negocio.

3.3. Estándares y mejores prácticas

El cumplimiento de normas y prácticas es esencial para lograr una correcta gestión de la Seguridad de la Información en las organizaciones. Estas actividades están relacionadas ciertos estándares previamente establecidos y que son aplicables a las empresas de acuerdo a sus funciones y características.

En el ámbito de la Seguridad de la Información algunos requisitos deben ser cumplidos de manera obligatoria, por ejemplo, las legislaciones de acuerdo al negocio de cada organización. En el mismo sentido, las empresas comprometidas con la protección de la información propia o de terceros, cumplen con estándares o normas de seguridad que se pueden adoptar voluntariamente.

GRÁFICO 11

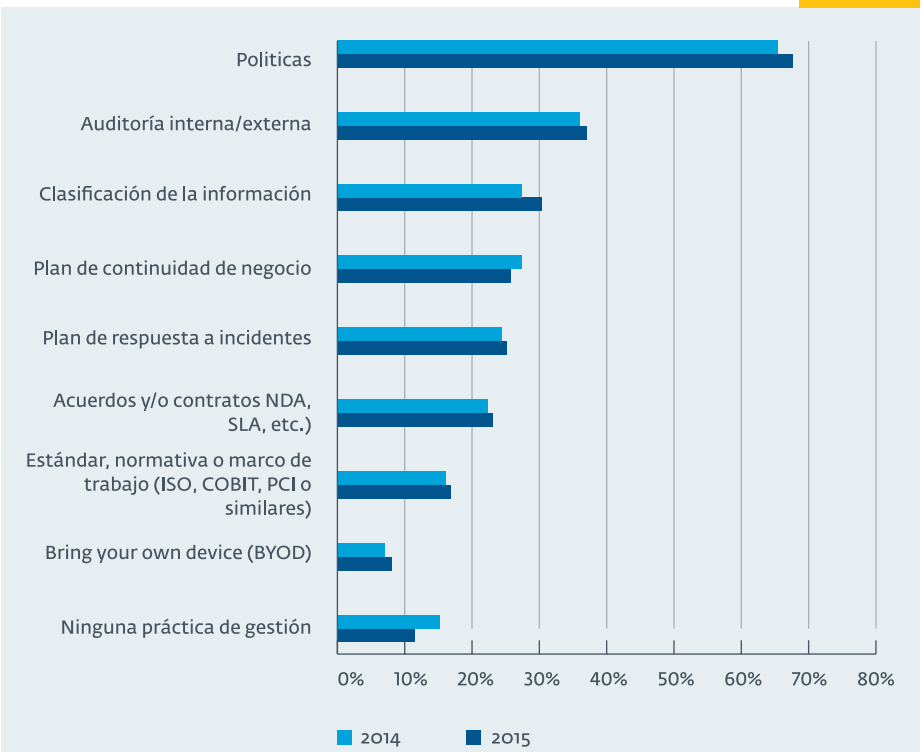


Prácticas de gestión aplicadas en las empresas de Latinoamérica (por tamaño de empresa).

De acuerdo con las encuestas, casi el 42% de los encuestados afirmó que debe cumplir con algún estándar o marco de trabajo, como ISO 27001 o PCI. Si bien estas obligaciones no determinan la ausencia de incidentes de seguridad, dejan ver que en la mayoría de los casos efectivamente se gestiona la Seguridad de la Información, además de que continuamente se revisan y actualizan los controles.

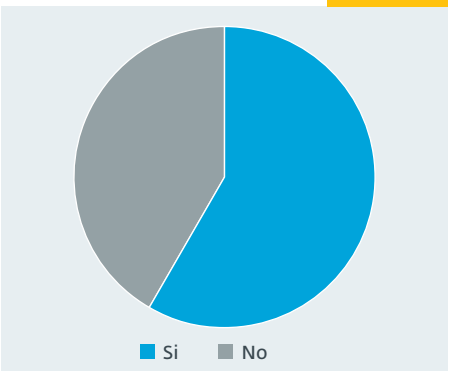
Asimismo, el 23% de los encuestados afirmó encontrarse alineado con los principios de seguridad establecidos en ISO 27001; 8% lo hace con PCI y un 69% con algún otro framework como ITIL, estándares de NIST, COBIT, ISO 20000 o leyes aplicables en los países en los cuales se realizaron las encuestas.

GRÁFICO 12



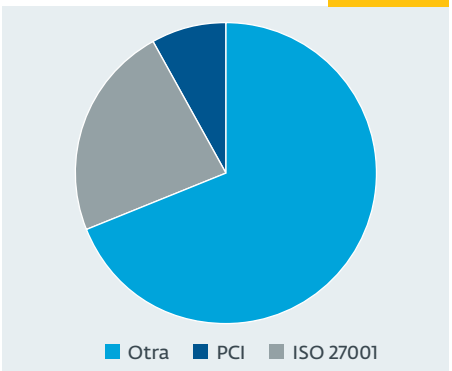
Cambios en las prácticas de gestión de la seguridad en los últimos dos años.

GRÁFICO 13



Porcentajes de las empresas que cuentan con algún estándar, normativa o marco de trabajo.

GRÁFICO 14



Estándares, normativas o marcos de trabajo que cumplen las empresas en Latinoamérica.

3.4. Educación y concientización

El factor humano es un elemento fundamental para la protección de la información. Conocer los riesgos de seguridad a los cuales se expone la información y concientizar a los usuarios para el uso seguro de la tecnología es una tarea primordial, ya que muchas amenazas buscan explotar vulnerabilidades en las personas a través de la aplicación de técnicas de Ingeniería Social.

En las encuestas se consultó si dentro de las empresas se realizan actividades de educación y concientización en materia de Seguridad de la Información y los resultados pueden observarse en la siguiente tabla:

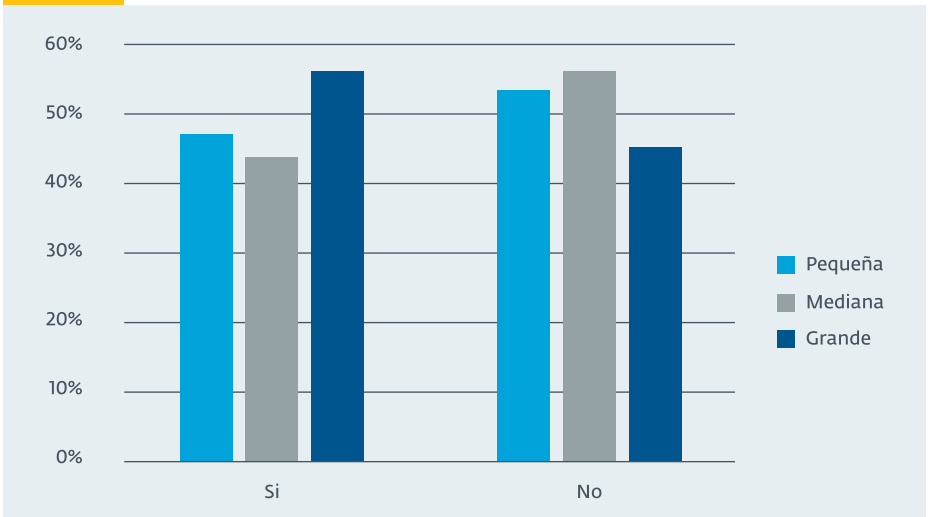
2014	2015	
41%	16%	Periódicamente
38%	35%	Ocasionalmente
12%	19%	No las llevo cabo
9%	30%	Planeo hacerlo al corto plazo

Realización de actividades de educación y concientización de usuarios.

Como se puede ver, hubo una reducción de estas actividades respecto a 2014, sin embargo, se destaca que alrededor del 35% de las organizaciones, sin importar su tamaño, llevan a cabo iniciativas de educación y concientización de manera ocasional. Y un porcentaje similar no las aplica, aunque planea hacerlo en el corto plazo.

Si bien es ideal que las actividades educativas sean constantes, es importante destacar que un gran porcentaje de las empresas lo hace al menos ocasionalmente y entiende que es necesario para mitigar el impacto de las amenazas informáticas. Aunque los porcentajes son parecidos en torno a los diferentes tamaños de empresas se destaca que el 55% de las empresas grandes lleva a cabo actividades de concientización.

GRÁFICO 15



Porcentajes de las empresas que realizan actividades de concientización para sus empleados (por tamaño de empresa).

Por otro lado, sobresale que en las empresas pequeñas y medianas el porcentaje de aquellas que no llevan a cabo actividades de concientización supera a las que sí las realizan.

3.5. Roles y responsabilidades en seguridad

Los resultados del ESET Security Report 2016 también exponen que más del 50% de los encuestados afirmaron que el área de Seguridad de la Información de sus empresas depende de la gerencia de TI. Aunque las mejores prácticas indican que el área de seguridad debe ser independiente para brindar objetividad e imparcialidad, claramente es una condición limitada a los recursos con los que cuenta cada organización.

Un dato interesante, es que solo el 9% de los encuestados afirmó que no cuenta con un área conformada o roles responsables para la Seguridad de la Información. Este dato evidencia que el 91% restante sí considera este aspecto, lo que ratifica la importancia que adquiere la protección de la información en las empresas latinoamericanas.

Cuando se analiza el porcentaje de empresas que sí cuentan con roles responsables de la seguridad, es interesante notar que el 51% deposita en la Gerencia de TI la toma de decisiones en este aspecto, mientras que el 16% cuentan con una Gerencia específica para esta función.

GRÁFICO 16

Estándares, normativas o marcos de trabajo que cumplen las empresas en Latinoamérica.

Además, cerca el 18% de las empresas pequeñas afirmó no contar con un área de seguridad conformada, lo que puede ser relacionado con el hecho de que los incidentes no sean reportados al no haber mecanismos para identificarlos y, en el peor de los casos, erradicarlos.

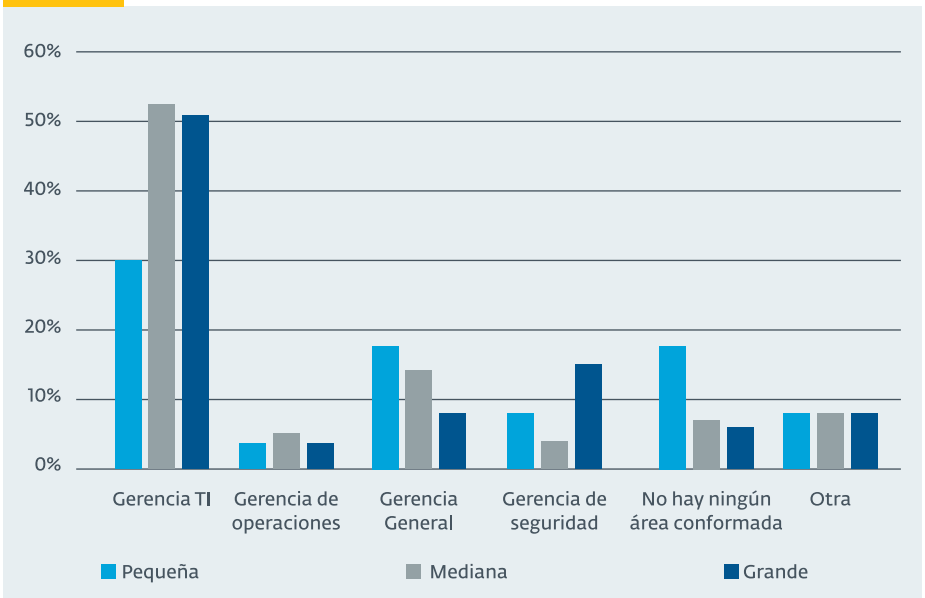
3.6. Presupuesto para la seguridad

En cuanto a los presupuestos para la seguridad, casi el 50% de los encuestados afirmaron que su presupuesto para dichas actividades se incrementó entre el 1% y el 10%.

Estos datos demuestran que cada vez se adquiere más conciencia sobre la importancia de la seguridad de los datos en los negocios, y de que un incidente podría comprometerlos seriamente. Por este motivo, es necesario destinar más recursos para protegerlos.

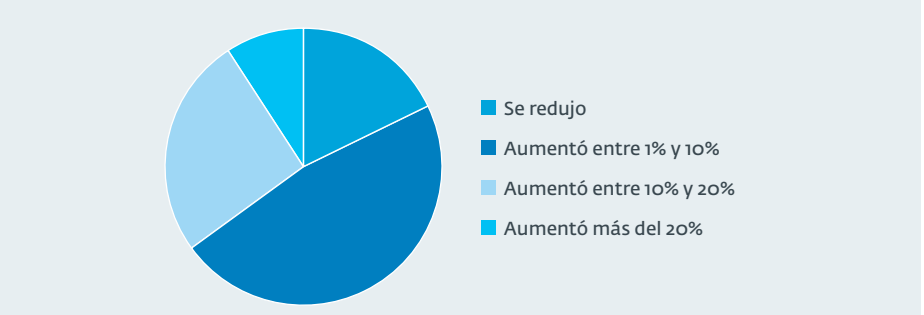
Por otro lado, solo el 9% de los encuestados afirmó que su presupuesto aumentó más del 20%, mientras que para el 18% se redujo respecto a 2014. En total, el 82% de los encuestados respondió que su presupuesto se incrementó en los últimos 12 meses.

GRÁFICO 17



Roles y responsabilidades de la seguridad en las empresas (por tamaño de empresa).

GRÁFICO 18



Variaciones de los presupuestos para las áreas de seguridad respecto al año anterior.

Conclusiones

El propósito principal del ESET Security Report es ofrecer **un claro panorama sobre el estado de la seguridad en las empresas latinoamericanas**. En este sentido, desde 2009, cada edición concentra la información relacionada con las principales preocupaciones en materia de Seguridad de la Información, los incidentes más frecuentes y de mayor impacto, así como las medidas de protección que se llevan a cabo en las empresas de la región.

Este año **se destacan algunas similitudes que se han sostenido a lo largo de los años** (y que es lógico que así sea, sobre todo si se las relaciona con los principales sucesos conocidos), como la preocupación por las **vulnerabilidades** de software, o bien la aparición de los **programas maliciosos como la principal causa de incidentes por séptimo año consecutivo.**

Sin embargo, sobresalen **algunas variables interesantes** respecto a cómo está evolucionando tanto el escenario de los ataques como el estado de seguridad en las empresas. Por ejemplo, **el phishing sigue creciendo** y se ubicó en el segundo lugar como el causante de incidentes de seguridad. A pesar de que se trata de una amenaza fácilmente detectable, continúa siendo efectiva; una prueba de ello son los registros de spear phishing utilizados en ataques dirigidos.

Al mismo tiempo, **el acceso indebido a la información se posicionó por primera vez en el podio de las preocupaciones** desplazando al fraude al cuarto lugar. Además, en estos rubros los fraudes internos/externos se posicionaron como la tercera causa de incidentes.

En cuanto a las medidas de protección, y en línea con lo que sucede hace algunos años, **los principales controles tecnológicos siguen siendo los productos antimalware, firewalls y soluciones de backup**. No obstante, es importante aclarar que se los debe acompañar con prácticas de gestión y campañas de educación, es decir, enfocándose en la tecnología, procesos y colaboradores.

Por todo lo anterior, cabe destacar también que **las prácticas de gestión han aumentado en todas las categorías**, lo que también representa una reducción en la cantidad de empresas que no aplican medidas para administrar su seguridad. Este hecho es una probable consecuencia del aumento de los presupuestos asignados para las áreas de seguridad, que se incrementó para el 82% de los encuestados respecto del año anterior. En la misma línea, el 91% de ellos afirmó contar con un área o responsable de seguridad en sus empresas.

Por otro lado, el cumplimiento de estándares y buenas prácticas ascendió a cerca del 42% de los encuestados, quienes afirmaron que en sus empresas se deben alinear a normativas de marcos de trabajo como ISO 27001, ITIL, COBIT o bien alguna legislación obligatoria.

Por último, **casi la mitad de las organizaciones encuestadas realiza iniciativas de educación y concientización en temas de Seguridad de la Información para su personal**. Sin duda, una tarea fundamental para hacer frente a las amenazas informáticas.

Una vez más, **es posible ver una lenta, pero sostenida mejora en el nivel de madurez de la Seguridad de la Información corporativa en la región**, lo que certifica que muchos de los esfuerzos para promoverla son eficientes. No obstante, **todavía existe un importante espacio para mejoras y aprendizaje en la búsqueda de la mitigación de los riesgos de seguridad de la actualidad.**

Fundada en 1992, ESET es una compañía global de soluciones de software de seguridad que provee protección de última generación contra amenazas informáticas y que cuenta con oficinas centrales en Bratislava, Eslovaquia, y de Coordinación en San Diego, Estados Unidos; Buenos Aires, Argentina y Singapur. En 2012, la empresa celebró sus 20 años en la industria de la seguridad de la información. Además, actualmente ESET posee otras sedes en Londres (Reino Unido), Praga (República Checa), Cracovia (Polonia), Jena (Alemania) San Pablo (Brasil) y México DF (México).

Desde 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.

El interés y compromiso en fomentar la educación de los usuarios en seguridad informática, entendida como la mejor barrera de prevención ante el cada vez más sofisticado malware, es uno de los pilares de la identidad corporativa de ESET. En este sentido, ESET lleva adelante diversas actividades educativas, entre las que se destacan la Gira Antivirus que recorre las universidades de toda la región, el ciclo de eventos gratuitos ESET Security Day y ACADEMIA ESET, la plataforma de e-learning de seguridad de la información más grande en habla hispana.

Además, el Equipo de Investigación de ESET Latinoamérica contribuye a WeLiveSecurity en español, el portal de noticias de seguridad en Internet, opiniones y análisis, cubriendo alertas y ofreciendo tutoriales, videos y podcasts. El sitio busca satisfacer a todos los niveles de conocimiento, desde programadores aguerridos hasta personas buscando consejos básicos para asegurar su información en forma efectiva.

Para más información visite: **www.welivesecurity.com/la-es**

/ESETLA /@ESETLA /company/eset-latinoamerica

ENJOY SAFER TECHNOLOGY™