ESET Security Report
Latinoamérica 2017

ENJOY SAFER TECHNOLOGY™

Contenido

Introducción

Tal como venimos realizando desde hace varios años, durante 2016 ESET ha participado en diversos eventos relacionados a la Seguridad de la información en todo Latinoamérica. En dichas jornadas, llevamos adelante encuestas a los asistentes (ejecutivos, gerentes y administradores de IT de empresas) para que puedan compartir con nosotros sus experiencias y opiniones en torno su trabajo diario.

Con esa información, los especialistas de seguridad del Laboratorio de Investigación de ESET Latinoamérica confeccionaron el ESET Security Report 2017, un documento que busca mostrar cuál es el panorama de seguridad de las empresas en toda la región.

A lo largo de este informe podrán encontrar cuáles fueron los principales incidentes de seguridad en las empresas durante todo el año anterior, así como también poder observar qué controles se implementan para proteger las redes corporativas y cómo estos datos se relacionan con las preocupaciones que los profesionales de tecnología dicen tener en torno a la seguridad de sus activos informáticos.

Este año contamos con la participación de más de 4 mil ejecutivos y profesionales de IT de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela.

Confiamos en que este análisis proveerá un diagnóstico del estado de la seguridad de la información en empresas de Latinoamérica y esperamos que sea de utilidad para que los responsables de seguridad de las empresas puedan compararse y revisar sus prácticas a partir de la lectura de este informe.

+4000

Participantes de la encuesta

13

Países incluídos

01 // Preocupaciones

¿Cuáles son las preocupaciones principales respecto a la Seguridad de la Información en las empresas de Latinoamérica?

En esta sección del ESET Security Report 2017 nos centraremos en analizar cuáles son aquellas situaciones y riesgos que más preocupan a las empresas de Latinoamérica, pues este es el primer paso para comenzar a diagnosticar el estado de la seguridad general de la región.

Naturalmente, el objetivo de las organizaciones es atender estas inquietudes para intentar eludir proactivamente las diversas problemáticas que puedan comprometer el negocio. Sin embargo, ¿puede que existan diferencias entre la percepción que tienen sobre su propia seguridad y lo que sucede respecto al resto de las empresas o mercados?

Desde una mirada global, y analizando los datos obtenidos, podríamos intuir que las preocupaciones están disminuyendo, por lo cual no sería sorprendente que quizá esto se traduzca en el aumento de incidentes en el futuro. Más adelante, desarrollaremos puntualmente acerca de los incidentes, pero en las sucesivas líneas profundizaremos en las inquietudes de seguridad mayormente presentes en las empresas.

27%

Phishing

56%

Malware

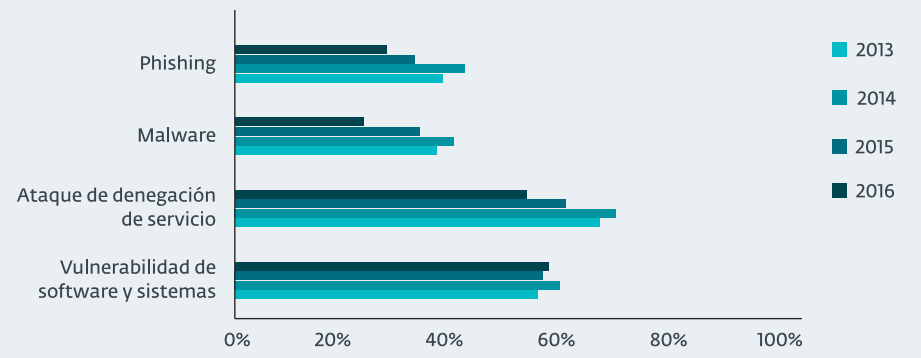
52%

Vulnerabilidad de software y sistemas

Al analizar las preocupaciones, vemos que la infección por **códigos maliciosos** está en el **primer lugar con un 56% de las respuestas**. Podemos decir que las preocupaciones se corresponden con la realidad, específicamente con el grado de sofisticación que tiene el malware y el retorno económico que genera; y que sigue en aumento. Un ejemplo del grado de tecnicismo presente es el troyano BlackEnergy, capaz de infectar los sistemas de control industrial SCADA, logrando provocar la **interrupción del servicio energético en la región de Ivano-Frankivsk, en Ucrania**. De manera análoga, el grupo de amenazas persistentes avanzadas **(APT)** financieras conocido como **Carbanak** llegó a los titulares cuando se descubrieron sus operaciones, por las que aparentemente robó varios cientos de millones de dólares de **instituciones financieras**.

Por otra parte, es importante destacar a otro importante protagonista de este panorama. El **ransomware** alcanzó un 32% de las respuestas, un indicador que se condice con los hechos que atestiguamos desde hace tiempo, donde fue la causa de incidentes graves en todo tipo de usuarios y plataformas.

GRÁFICO 1.1 *Principales preocupaciones*



Ransomware

Esta amenaza no solamente ataca indiscriminadamente a diferentes industrias, sino que también emigró desde computadoras a smartphones y a otros dispositivos inteligentes de la Internet de las Cosas. Esta situación es muy sensible y alertó a todos los especialistas quienes preludian la llega del Ransomware de las Cosas (RoT, por su sigla en inglés). Este código malicioso continúa desarrollando nuevas técnicas de extorsión: además de reclamar un pago de la manera "clásica", ahora vemos nuevas variantes que ofrecen la recuperación de la información cifrada al infectar a más usuarios. Esto expande aún más la cantidad de vectores de infección utilizando a la víctima como cómplice.

Para las empresas, las **botnets** parecen estar muy presentes, aunque sea de un modo indirecto, ya que estas redes están ligadas a varias preocupaciones. Este tipo de software malicioso permite robar información sensible como credenciales financieras de manera inadvertida para luego realizar un **fraude**. Del mismo modo, puede alcanzar cualquier tipo de documento almacenado que sea de interés, realizando así un **acceso indebido a la información**.

Asimismo, las empresas también manifiestan preocupaciones relacionadas a la **denegación de servicios (23%)**, que justamente en muchos casos son ocasionados por redes del tipo botnet. Precisamente durante 2016 fuimos testigos de Mirai, una botnet enfocada en la **Internet de las Cosas**, y con la cual los ciberdelincuentes se aprovecharon de estos novedosos y desprotegidos dispositivos para implementar algunos de los ataques de denegación de servicio distribuido (DDoS) más masivos de toda la historia. La consecuencia fue la caída de miles de servidores y de los sitios más importantes del mundo.

Estas grandes familias de códigos maliciosos comparten muchas similitudes con otros tipos de malware, principalmente durante el origen de una infección. Nos referimos, particularmente, a los vectores de propagación que continúan siendo correos electrónicos con archivos adjuntos o enlaces que instan a descargar la amenaza; dispositivos de almacenamiento USB; o bien sitios web que redirigen a sus visitantes a diferentes tipos de exploits.

La segunda problemática que más preocupa a las empresas alcanza un 52% de las respuestas y está ligada a la explotación de vulnerabilidades; amenaza que en 2015 estuvo en el primer lugar. Curiosamente, la cantidad total de vulnerabilidades reportadas anualmente ha ido disminuyendo en los últimos años. Sin embargo, son los reportes de vulnerabilidades críticas los que en los últimos años han crecido, lo

GRÁFICO 1.2 *Comparativa de preocupaciones de acuerdo al tamaño de empresa*

Empresas	Año	Malware	Fraude	Vulnerabilidad de software y sistemas	Ataque de denegación de servicio	Phishing	Acceso indebido a la información
Grandes	2015	52%	38%	60%	37%	34%	46%
	2016	55%	29%	53%	28%	28%	36%
Medianas	2015	60%	35%	60%	32%	34%	50%
	2016	56%	25%	49%	21%	27%	38%
Pequeñas	2015	55%	39%	58%	26%	28%	45%
	2016	57%	32%	51%	15%	22%	30%

que ofrece un asidero para ver que esta preocupación siga estando muy presente entre los usuarios.

Además, durante 2016 se han descubierto cientos de fallas de seguridad que afectaron tanto a plataformas **Microsoft**, como a diversas **aplicaciones** que son utilizadas masivamente. Muchas de ellas ganan protagonismo siendo bautizadas con nombres característicos; nos referimos a **Badlock** (CVE-2016- 2118) que afectó a Samba; **HTTPoxy** (CVE- 2016-5387); y **DROWN**.

Robo de información

A nivel corporativo, ya se encuentra instaurado el concepto de Industria 4.0, es decir que a medida que una empresa avanza en la incorporación de nuevas tecnologías, también deben preocuparse cada vez más por tener una infraestructura mejor protegida, ya que no es recomendable la idea simplista de "conectar y usar". Más aún, de nada sirve contar con los mejores controles tecnológicos si no se los gestiona correctamente para que sean eficientes.

En este sentido, las organizaciones que no estén dispuestas en invertir en seguridad no deben obnubilarse por la moda de utilizar tantos dispositivos online, ya que gran parte de estos nuevos sistemas conectados se ejecutan mediante software que puede ser vulnerable; más aún cuando tomamos conciencia de que los protocolos y las estructuras se diseñaron sin la noción de que en un fututo trabajarían en un entorno conectado y expuesto a Internet.

Por último, y cerrando el podio, **el robo de información** es considerado por un 43% de las empresas como una gran preocupación. Múltiples vectores de ataque permiten que esta sea una de las problemáticas más relacionadas con la confidencialidad y la privacidad de la información. Tanto los códigos maliciosos y la explotación de vulnerabilidades, como el phishing, los empleados disconformes o la sobrexposición de datos en redes sociales son las herramientas iniciales para que los ciberdelincuentes conviertan esta preocupación en un incidente real.

Es vital, entonces, tener programas de concientización sobre el valor de la información para los usuarios, de manera que no solo puedan conocer al respecto, sino que también obtengan las mejores prácticas para evitar incidentes. Estas tareas representan uno de los controles no tecnológicos más relevantes, por lo que en las próximas secciones ampliaremos con estadísticas al respecto.

Luego de reflexionar sobre estos puntos, concluimos que las preocupaciones en materia de seguridad se mantienen alineadas de manera similar tanto para pequeñas empresas, como para las más grandes. Si bien durante el último año hubo un leve descenso de las preocupaciones y un enroque en los primeros puestos, no se deben disminuir los esfuerzos de las áreas de seguridad para que estas no se materialicen en incidentes reales. En esta línea, es necesario enfocarse en tratar a las preocupaciones como riesgos para mitigar el potencial impacto negativo.

Pero este último enunciado es lo ideal; por lo que a continuación veremos cuáles fueron los incidentes que efectivamente sufrieron las empresas, para evaluar si sus preocupaciones están bien atendidas y cuentan con sus correspondientes controles.

02 // Incidentes de seguridad en empresas latinoamericanas

La segunda sección del ESET Security Report tiene como propósito conocer cuáles fueron los principales incidentes de seguridad que afectaron a las empresas latinoamericanas durante 2016. Para obtener esta información han sido considerados los eventos indeseados e inesperados que comprometieron las operaciones de las organizaciones y atentaron contra la confidencialidad, integridad y/o disponibilidad de la información.

Malware

Ransomware

Desde la primera publicación de este informe en 2012, los códigos maliciosos se han posicionado como la principal causa de incidentes de seguridad en las compañías de la región, con un importante crecimiento en 2016, lo que le permite ocupar nuevamente la primera posición al obtener el 49% de las respuestas afirmativas en las encuestas. Esto significa que prácticamente **una de cada dos** empresas latinoamericanas que participaron en este estudio fueron víctimas de algún tipo de malware.

Debido a la proliferación del ransomware, en esta ocasión el ESET Security Report cuenta con una categoría de incidentes exclusiva para este tipo de malware que aplica el principio del secuestro de información en el ámbito digital. Aunque también se trata de un tipo de infección por software malicioso (como la primera categoría), el cifrado de archivos con fines de extorsión merece una mención aparte debido a las repercusiones que ha tenido para las **organizaciones en el último tiempo**.

Por ello, sobresale que en su primera aparición como una categoría de incidentes, el ransomware se haya posicionado en el segundo lugar de los resultados de las encuestas con un 16%, desplazando al phishing hacia la tercera posición con 15%, que históricamente había ocupado el segundo puesto en las ediciones pasadas de este informe. Al comparar los resultados con el informe anterior, observamos que el mencionado phishing mantiene el 15% de respuestas afirmativas durante los dos últimos años, al igual que los ataques dirigidos (APT) con el 4%.

Por el contrario, todas las demás categorías disminuyeron sus porcentajes: la explotación de vulnerabilidades pasó de 12% en 2015 a 10% en 2016; los ataques de denegación de servicio de 11% a 9% en el mismo periodo; el acceso indebido a aplicaciones y bases de datos bajó de 11% a 9%; la falta de disponibilidad de servicios críticos pasó de 10% en 2015 a 8% en 2016; y por último los fraudes internos tuvieron las caída más notoria en el mismo periodo, pasando de 12% a 7%.

Una de las posibles razones por las cuales las categorías de incidentes han reducido sus porcentajes (a excepción del malware) es que los ciberdelincuentes han encontrado en los códigos maliciosos y especialmente en el ransomware, un negocio muy lucrativo que genera réditos económicos con mayor rapidez. Tan es así, que otras plataformas como los **teléfonos inteligentes** se ven cada vez más afectados por estas amenazas, e incluso se pronostica que más dispositivos puedan verse comprometidos con el denominado **Ransomware de las Cosas (RoT)**.

En resumen, ya sea que se trate de ransomware o algún otro tipo de malware, los códigos maliciosos continúan siendo la principal causa de incidentes de seguridad en las empresas de Latinoamérica, tal como se aprecia en el **gráfico 2.1**.

Además, es notorio que en esta ocasión más organizaciones reportaron no haber padecido algún incidente de seguridad, con un incremento importante pasando de 20% en 2015 a 31% en 2016.

Afirmó no haber sufrido incidentes de seguridad

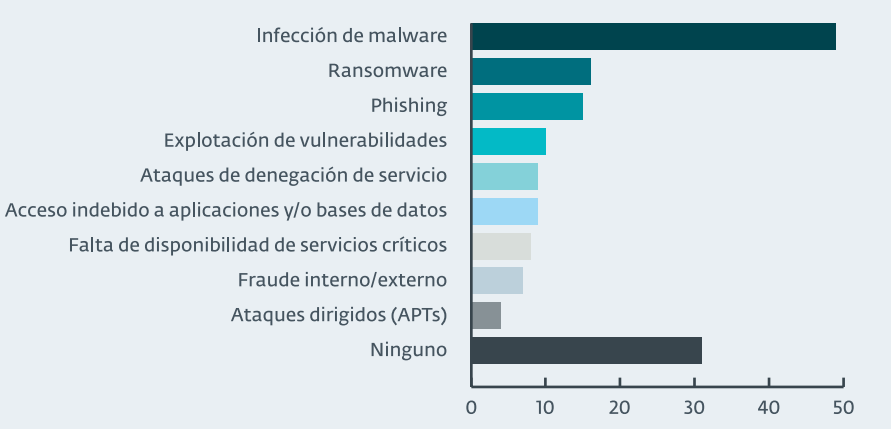
Seguidamente, y al revisar los resultados de incidentes reportados por categoría de empresa pequeña, mediana o grande, observamos que las posiciones no se modifican respecto a los promedios del gráfico anterior y mantienen concordancia con los porcentajes promedio, es decir, aquellos que fueron analizados sin considerar el tamaño de la organización.

Sin embargo, destaca que las empresas clasificadas como grandes son las que registran un mayor porcentaje en todas las categorías de incidentes (a excepción de las infecciones por malware); contrariamente con lo que sucede para la categoría de ningún incidente, donde el mayor porcentaje reportado corresponde a las empresas pequeñas, alcanzando casi el 40%. Aunque este dato resulta alentador, puede ser analizado desde diferentes perspectivas.

Una idea nos conduce a pensar que las empresas grandes presentan un mayor porcentaje de incidentes debido a que pueden resultar ser un objetivo más relevante para los atacantes por los recursos que poseen. Además, es importante dar cuenta de que tienen una mayor exposición a las amenazas informáticas debido a la infraestructura tecnológica que manejan y, al mismo tiempo, las detecciones son más frecuentes ya que pueden contar con las herramientas idóneas para identificar los ataques y amenazas, a diferencia de las organizaciones pequeñas.

No obstante, las PyMEs también se han convertido en un objetivo de los ciberdelincuentes y pueden ser afectadas de igual manera o, quizá, más que el resto de las organizaciones. Lamentablemente, en ocasiones no cuentan con los mecanismos ni la tecnología para detectar, bloquear y erradicar los ataques y amenazas que buscan pasar inadvertidos para los encargados de las áreas de tecnología y de seguridad; lo que se podría traducir en un desconocimiento real de si se han sufrido incidentes o no. De todos modos, el punto anterior tampoco debería tomarse como

GRÁFICO 2.1 *Incidentes de seguridad en empresas de Latinoamérica (2016)*



una regla, sobre todo cuando se presentan códigos maliciosos que resultan muy evidentes una vez que han comprometido los sistemas o la información.

2.1. Malware

En esta edición del ESET Security Report el malware se destacó por haber causado la mayor cantidad de incidentes de seguridad, por lo que no es de extrañar que también se haya convertido en la principal fuente de preocupación para los encargados de proteger los activos en las organizaciones. Esto se debe, entre otras razones, a la cantidad de reportes conocidos últimamente, la información en los medios de comunicación o incluso al papel protagónico que ha jugado el ransomware. Esta relación va en aumento, tal como se muestra a continuación.

Más empresas afirmaron haber sufrido infecciones con malware

El gráfico 2.1.1 presenta la evolución de los incidentes de seguridad relacionados con malware desde 2009 hasta 2016. En 2014 el 39% de los encuestados afirmó haber sufrido infecciones por malware, mientras que en 2015 el número aumentó al 40%; para 2016 el porcentaje ascendió a 49%. Es evidente que en los últimos años se presenta una tendencia creciente, debido en gran medida a la cantidad de códigos maliciosos que se desarrollan en la actualidad, los métodos empleados para su propagación y las ganancias económicas que obtienen los cibercriminales que los desarrollan y/o financian.

GRÁFICO 2.2 *Comparativa de incidentes sufridos por tamaño de empresa*

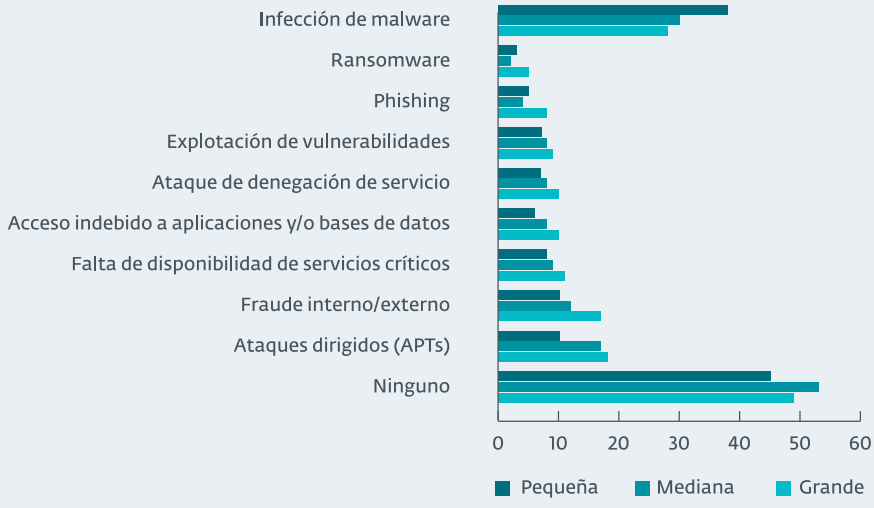
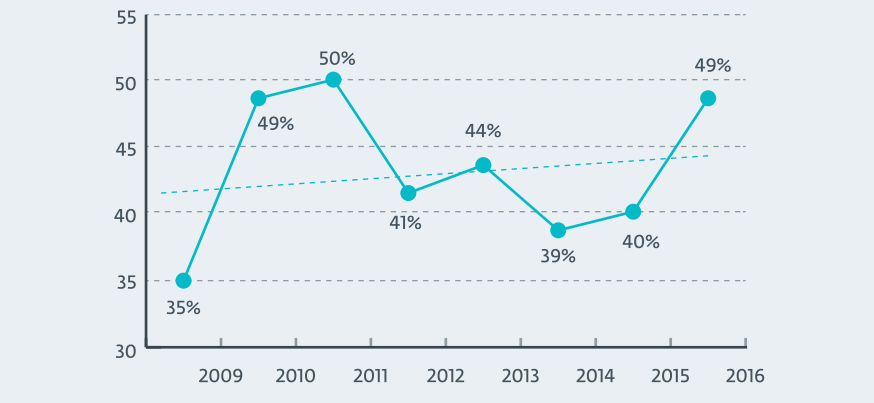


GRÁFICO 2.1.1 *Comparativa anual de infecciones por malware en Latinoamérica (2009-2016)*



53%

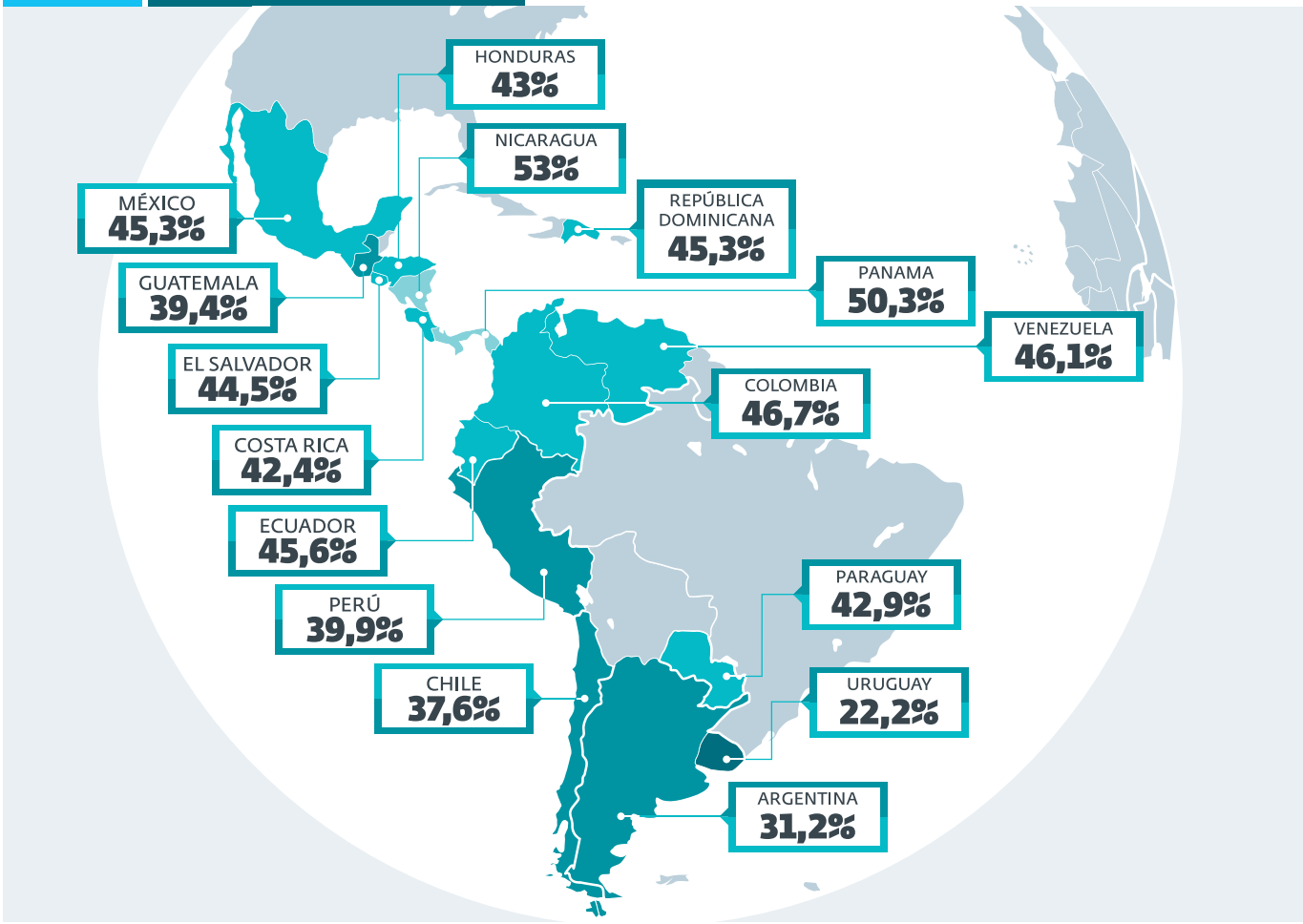
Nicaragua fue el país con mayor porcentaje de empresas infectadas

La actividad maliciosa en los países latinoamericanos se observó de manera continua durante el año pasado, donde algunos territorios se vieron más afectados por distintas razones, como las prácticas de seguridad aplicadas e, incluso, que las campañas de malware tenían como foco a usuarios específicos. De acuerdo con los resultados de las encuestas aplicadas para este informe, Nicaragua ocupa el primer lugar con el 53%, seguido de Panamá con el 50,3% y Colombia con 46,7%, tal como se puede observar en el gráfico 2.1.2, junto con los datos completos del estudio.

Los resultados anteriores pueden explicarse al revisar sucesos registrados el año pasado, como la identificación de un sinnúmero de campañas de malware en Latinoamérica. A principios de 2016 **Remtasu**, una familia de troyanos dedicada a robar información sensible de los equipos de las víctimas, tuvo una importante actividad en Colombia a través campañas que se valían de técnicas de Ingeniería Social. **Neurevt**, otro código malicioso diseñado para el robo de información sensible, siguió operando en México con acciones similares y suplantando instituciones reconocidas de ese país.

Las botnets también continuaron infectando equipos en la región. Tal es el caso **Bondat**, un código malicioso orientado al control de dispositivos que utilizan Windows; esta amenaza se propagó principalmente a través de memorias extraíbles, afectando a países como Perú, México, Colombia y Ecuador. Otro caso fue el de **Cy-**

GRÁFICO 2.1.2 *Infecciones de malware por país (2016)*



bergate, un tipo de malware desarrollado para controlar los sistemas infectados y robar información; su principal actividad se presentó en Centroamérica.

A lo largo del año surgieron otros tipos de códigos maliciosos, como el criptoransomware **Locky**. El Laboratorio de Investigación de Malware de ESET Latinoamérica detectó su presencia en México, Perú, Colombia, Chile, Argentina y Guatemala. Otras variantes conocidas evolucionaron para afectar nuevas plataformas; tal es el caso de **CTB-Locker**, que buscaba cifrar la información en servidores web. Del mismo modo, otros sistemas operativos se convirtieron en blanco de los atacantes, tal como sucedió con el ransomware **KeRanger** que se enfocó en plataformas macOS.

Todos estos casos, junto con los resultados de las encuestas, ponen de manifiesto la problemática que siguen representado los códigos maliciosos, a través de las campañas masivas de propagación e infección utilizando métodos conocidos como archivos adjuntos, correos electrónicos, drive-by download, explotación de vulnerabilidades o dispositivos extraíbles. En este contexto, también se incluyen los ataques dirigidos que utilizan malware para afectar a objetivos específicos; en conjunto conforman una amenaza latente para la seguridad de la información y otros activos de las organizaciones.

Phishing

21%

Ecuador tuvo el porcentaje mayor de empresas afectadas por Phishing

2.2. Phishing

Luego de ver en profundidad los indicadores sobre el malware, ahora es el turno de hablar del phishing, precisamente en una edición donde fue desplazado al tercer puesto, siguiendo a las infecciones por malware y de los casos específicos de ransomware. Los engaños a través de la suplantación de sitios legítimos para el robo de información confidencial son una técnica que continúa siendo vigente y efectiva a pesar de que cada vez es más conocida, relativamente fácil de detectar y del tiempo que lleva siendo utilizada.

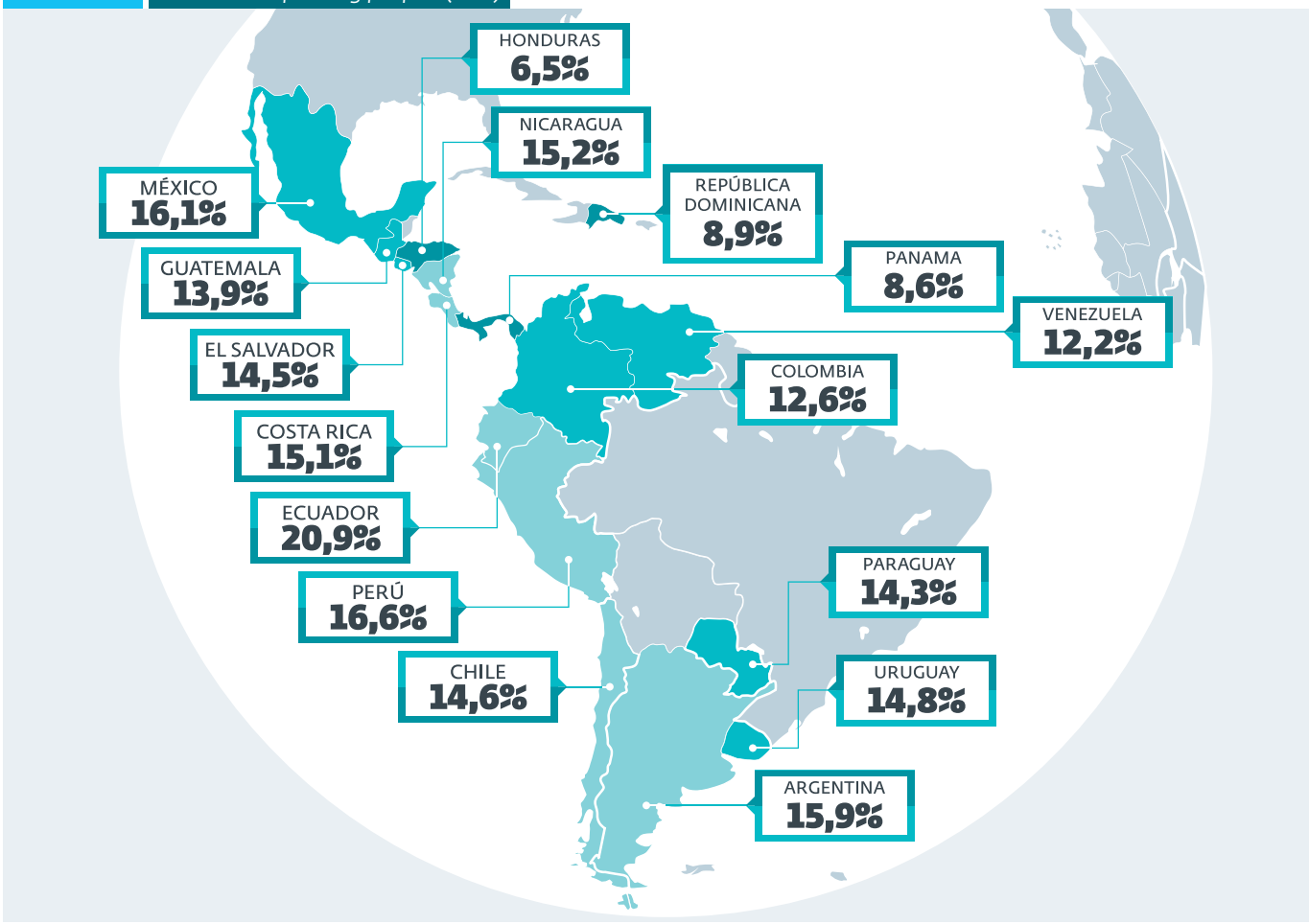
Continuamente, se observan campañas enfocadas en obtener contraseñas, datos bancarios e información confidencial de los usuarios a través de la suplantación de entidades reconocidas en los países donde se desarrollan estas amenazas. Generalmente, los sitios de instituciones bancarias son los más usurpados, aunque ahora prácticamente cualquier sitio que pueda generar una ganancia económica para los cibercriminales puede ser susceptible de falsificación.

Las empresas de los países latinoamericanos no son ajenas a este tipo de campañas que suelen afectarlas y que, generalmente, se incrementan en las épocas de mayor actividad económica en Internet, periodos vacacionales o cuando las marcas realizan ofertas a los usuarios, por lo que los atacantes se suelen valer de estas temáticas para engañarlos.

De acuerdo con los resultados de las encuestas, las empresas que más se vieron afectadas por casos de phishing son las que se ubican en Ecuador con 20,9% de las respuestas afirmativas, seguido de Perú con 16,6% y México en el tercer sitio con el 16,1%. Los resultados completos se observan en el **gráfico 2.2.1** que incluye la información de todos los países que formaron parte de este análisis.

Durante el año pasado, el Laboratorio de Investigación de Malware de ESET Latinoamérica alertó sobre una cantidad importante de campañas de phishing enfo-

GRÁFICO 2.2.1 *Incidentes de phishing por país (2016)*



cadas a usuarios de la región. Por ejemplo, en marzo se identificó una escalada que intentaba imitar el sitio de **Visa** para robar datos de los usuarios. Días después surgió una nueva campaña que involucraba a **MasterCard**; a partir de correos falsos se invitaba a los usuarios a reactivar un supuesto servicio al acceder a un sitio apócrifo. Si el usuario caía en el engaño, toda la información relacionada con su tarjeta de crédito podía ser obtenida por los atacantes.

Sin embargo, las instituciones financieras y bancarias no son las únicas que pueden ser utilizadas como señuelos para afectar a los usuarios, ya que otras organizaciones de renombre también han sido suplantadas. Tal es el caso de **Apple**, **Mercado Libre** e incluso de servicios de redes sociales como **Facebook**, donde los usuarios más afectados fueron de Argentina, México y Colombia.

Por lo tanto, ya sea que se trate de campañas de phishing que tienen como propósito llegar a la mayor cantidad posible de víctimas, como que se trate de spear phishing, donde no se busca tener un alcance masivo sino un ataque dirigido a un grupo u organización específico, sin duda continúan siendo redituables para los atacantes debido a la aplicación efectiva de técnicas de Ingeniería Social y las ganancias económicas que obtienen, ya que la información sustraída se comercializa en el **mercado negro**.

De la misma manera que el malware, el phishing continúa siendo una amenaza que busca atentar contra la información de las empresas y los usuarios en Latinoamérica.

03 // ¿Cómo se protegen las empresas latinoamericanas?

Durante los últimos años, los cibercriminales han encontrado formas aún más efectivas para monetizar sus actividades maliciosas, perfeccionando la industria del crimen digital al incorporar nuevos modelos de fraude.

El auge del ransomware ha sido un claro ejemplo de esta situación, llegando a alarmar a empresas de diferentes países, rubros, industrias y tamaños.

Antivirus

Firewall

Backup

En pasadas secciones hemos visto cómo este escenario se ha reflejado en las preocupaciones manifestadas por las organizaciones encuestadas a lo largo y ancho de América Latina. Ahora, cabe preguntarnos si estas empresas han obrado en consecuencia, adquiriendo la tecnología necesaria para prevenir, detectar y mitigar ataques contra sus activos de información.

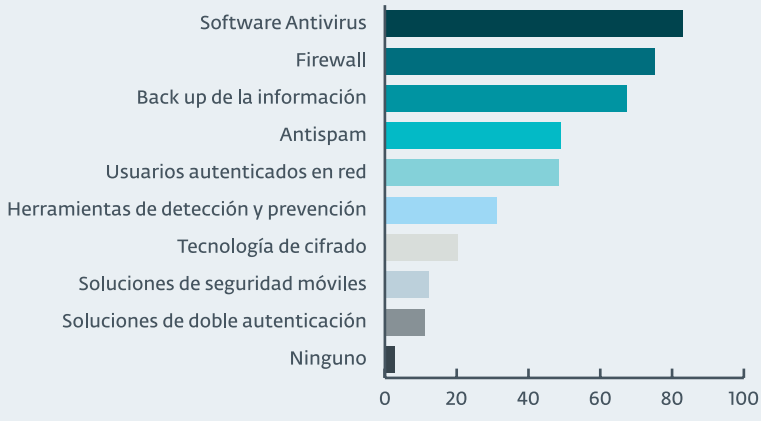
Vale destacar que la inclusión de controles tecnológicos, buenas prácticas de gestión y capacitación constante en seguridad resultan cruciales al momento de salvaguardar la información crítica y, así, asegurar la continuidad del negocio.

3.1. Controles de seguridad

Los datos arrojados por las encuestas demuestran que los controles de seguridad más implementados en Latinoamérica son el antivirus (83%), el firewall (75%) y el backup de la información (67%). Históricamente, de acuerdo con información del ESET Security Report, estas tres herramientas han eclipsado los primeros lugares en el ranking de tecnologías de seguridad más utilizados.

Si un número tan elevado de empresas posee al menos estas tres tecnologías de seguridad, ¿cómo puede ser que el porcentaje de incidencias de seguridad sea tan alto? En primer lugar, el hecho de que un 83% cuente con un antivirus instalado implica que un 17% no lo hace; ese porcentaje se traduce en casi 800 empresas desprotegidas –un número más que considerable– dentro de las más de 4500 encuestadas. Además, la efectividad de estas herramientas dependerá también de su correcta configuración, actualización y uso.

GRÁFICO 3.1.1 *Controles de seguridad más implementados en Latinoamérica durante 2016*



A/-BF5G!\
LPF6G23

21%
Cifrado

*****

11%
Doble factor de autenticación

12%
Soluciones para dispositivos móviles

En los últimos años, debido al desarrollo de nuevas plataformas tecnológicas y la siempre cambiante interacción con ellas, la superficie de exposición de las empresas ha aumentado de manera drástica. Esto implica que existe un mayor número de vectores de ataque que pueden ser utilizados para comprometer la seguridad de los datos.

Como respuesta a este fenómeno, resulta vital incorporar múltiples herramientas para crear una arquitectura de seguridad óptima frente a las amenazas latentes. En este sentido, el uso de tecnologías como el cifrado (21%), sistemas IPS e IDS (31%) y soluciones de doble factor de autenticación (11%) se vuelve cada vez más crítico. De igual manera, las soluciones de seguridad móviles aún no reciben la atención que deberían.

Los resultados de nuestro ESET Security Report reflejan que solo el 12% de las empresas latinoamericanas encuestadas utilizan algún tipo de solución para sus equipos móviles. Si contrastamos este dato con el crecimiento sostenido del malware móvil, el resultado no puede ser más desalentador.

Empresas que implementan soluciones móviles	
2013	11%
2014	10%
2015	10%
2016	12%

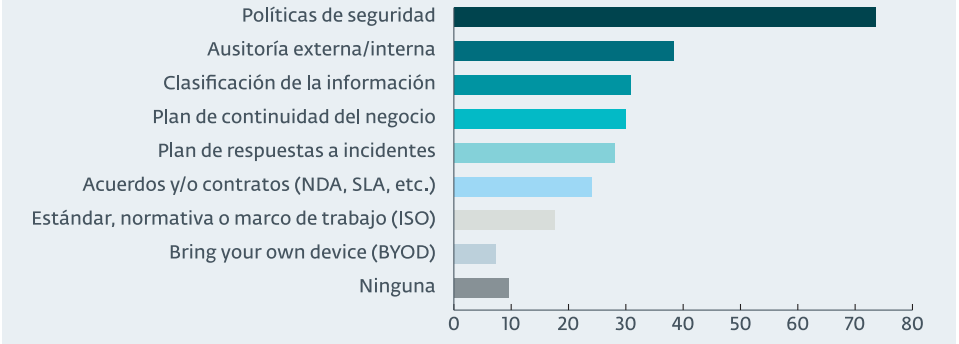
Especialmente en pequeñas y medianas empresas, los empleados muchas veces se ven forzados a utilizar sus propios teléfonos celulares para manejar los datos de la organización. De hecho, Gartner estima que para este año, el **50% de los empleadores** requerirá que sus equipos entreguen sus dispositivos personales para manipular datos corporativos.

En otras palabras, aunque han pasado ya muchos años desde la creación del concepto BYOD, el verdadero impacto de esta modalidad en los procedimientos de seguridad aún está por verse.

3.2. Gestión de la seguridad

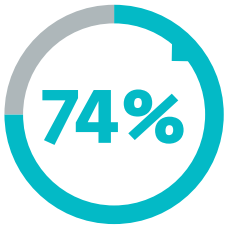
En cuanto a la gestión de la seguridad de la información, los resultados obtenidos no varían mucho respecto a la **edición pasada** de nuestro reporte. Las prácticas más

GRÁFICO 3.2.1 *Prácticas de gestión de la seguridad más implementadas en 2016 en Latinoamérica*



utilizadas resultaron ser el mantenimiento de políticas de seguridad (74%), la realización de auditorías internas y/o externas (38%) y la clasificación de la información (31%).

Si bien existe un leve incremento del 5% con respecto a 2015 en la cantidad de empresas latinoamericanas que utilizan políticas de seguridad, algunos indicadores despiertan dudas en relación a qué tan bien diseñadas se encuentran. Por ejemplo, ¿cuán efectivas pueden ser aquellas políticas que no están basadas en la clasificación de los activos de información según su criticidad?



Políticas de seguridad

Auditorías internas/ externas

Realiza actividades de concientización de manera periódica

Cuando consideramos el tamaño de la empresa junto a las gestiones implementadas, vemos que el 17% de las pequeñas organizaciones, el 10% de las medianas y el 6% de las grandes no siguen ninguna de estas prácticas. Esto es muy preocupante, sobre todo cuando tenemos en cuenta las consecuencias que puede conllevar para la protección del negocio. No obstante, estas cifras han disminuido en los últimos años, planteando un panorama esperanzador para el futuro.

También resulta interesante que, mientras que se redujo el porcentaje de grandes y medianas organizaciones que implementan políticas BYOD, las pequeñas empresas parecen haber tomado esta preocupación más en serio, incrementando su implementación desde un 5% en 2015 a un 8% en 2016. Claro que, aun así, el porcentaje que adopta gestiones para mitigar este riesgo es muy bajo.

3.3. Educación y concientización

En ocasiones, resulta difícil para los empleados asumir que también son parte del sistema en una compañía y que sus acciones pueden derivar en posibles incidentes. En este sentido, suelen delegar la seguridad únicamente a los componentes informáticos; desestiman su propio valor o el de la información que manejan. Por ello es tan importante capacitar a los diferentes estratos de la organización respecto a las amenazas informáticas que buscan atacar el factor humano mediante las técnicas de Ingeniería Social.

Según los resultados de las encuestas, el 35,3% de las empresas realiza periódicamente actividades de concientización, el 39,3% lo hace ocasionalmente, el 13,4% directamente no posee programas de capacitación y el 12% restante actualmente no cuenta con planes de capacitación, pero planea incorporarlos en el corto plazo.

Como vemos en la **tabla 3.3.1**, aunque el porcentaje de empresas que promueve actividades de concientización periódicamente sigue siendo menor que en 2014, una mayor cantidad de organizaciones lo hace ocasionalmente o planea hacerlo, lo cual proyecta un mejor escenario para este año.

TABLA 3.3.1 *Comparativa de realización de actividad de concientización en seguridad de la información*

2014	2015	2016	
40,7%	33,2%	35,3%	Sí, periódicamente
38,1%	37,0%	39,3%	Sí, ocasionalmente
11,9%	13,6%	13,4%	No
9,3%	16,2%	12,0%	No, pero planean hacerlo a corto plazo

Además de realizar actividades de concientización y orientar los procesos de seguridad hacia la usabilidad, se debe prestar atención a que tales actividades educativas resulten efectivas. Muchas organizaciones ostentan un único programa de capacitación en seguridad de la información, cuando existe un universo de usuarios con diferentes aptitudes técnicas. En consecuencia, el principal problema en la capacitación suele ser la falta de motivación de los usuarios.

Es importante, entonces, diseñar planes para audiencias específicas, construirlos sobre los resultados esperados y pensarlos para ganar la atención de su público buscando mantener a los distintos actores interesados en aprender. Además, es necesario estipular mecanismos para mantenerlos al tanto de los cambios que sufre la política de la organización, puesto que estas se deben actualizar y modificar periódicamente.

12%

de las empresas tiene un área dedicada exclusivamente a la seguridad de la información

Finalmente, el abordaje práctico de este tema requerirá un conocimiento extenso de la organización, una estrategia estructural, las herramientas correctas y mucha paciencia.

3.4. Distribución de las responsabilidades en seguridad

La asignación de responsabilidades referidas a las tareas de ciberseguridad es un asunto más delicado de lo que parece. Las mejores prácticas establecen que los roles en este ámbito deben ser independientes para brindar objetividad e imparcialidad; de lo contrario, el reporte de incidentes puede ser alterado o pasado por alto.

Desafortunadamente, un gran porcentaje de empresas no cuentan con los recursos para seguir estos lineamientos. En 2016 más del 50% de los encuestados afirmó que el área de Seguridad de la Información de sus empresas depende de la gerencia de TI, mientras que solo el 12% ha establecido un área dedicada exclusivamente a tareas de seguridad informática.

2016	
Gerencia de TI	54%
Gerencia de Operaciones	5%
Gerencia General	13%
Gerencia de Seguridad	12%
No hay ningún área conformada	9%
Otra	7%

La cantidad de empresas que no poseen ningún área dedicada a dichas tareas ha decrecido un 1% con respecto a 2015, llegando al 9% en 2016. Esto nos indica que la mayoría de las organizaciones latinoamericanas se preocupan por la seguridad de sus activos, al punto de reflejarlo en su estructura organizacional.

3.5. Presupuesto para seguridad

La concesión de recursos para la protección de los datos suele generar conflictos entre técnicos y gerentes ya que, a diferencia de inversiones en instalaciones o ma-

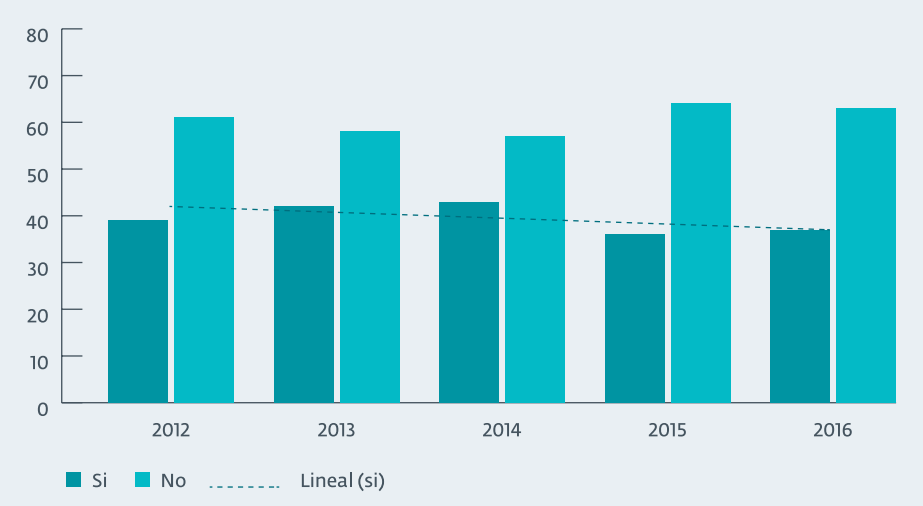
quinaria, el beneficio es más difícil de percibir: las herramientas de seguridad no buscan aumentar las ganancias, sino disminuir posibles pérdidas.

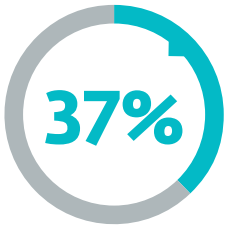
Es por esto que, a pesar de la abrumadora evidencia respecto a la evolución de amenazas informáticas, el número de empresas que no cuenta con un presupuesto para la seguridad supera año tras año a aquellas que sí lo hacen, como puede verse en el gráfico 3.5.1. En 2016, solo el 37% de las empresas latinoamericanas destinó parte de sus ganancias a incorporar herramientas de control, lo cual supone un aumento del 1% respecto a 2015.

El concepto de "potencial pérdida" es, quizá, lo que desalienta a los administradores de empresas a invertir en minimizar el riesgo de ver sus activos digitales comprometidos. No obstante, deben entender que los ataques informáticos no pertenecen al campo del azar, sino al de la probabilidad; y hoy son casi una certeza.

Estos indicadores demuestran la importancia de una correcta capacitación en seguridad de la información que se extienda incluso hacia los altos mandos de la jerarquía organizacional.

GRÁFICO 3.5.1 *Comparativa de empresas con presupuesto para seguridad*





Considera que tiene suficiente presupuesto para seguridad

04 // La apuesta a la seguridad por capas

Quizá una de las cuestiones en las que más se insiste cuando hablamos de gestionar la seguridad de la información en una empresa es en la necesidad de contar con distintas alternativas para los diferentes tipos de incidentes que podrían llegar a ocurrir.

Algunas veces se habla de seguridad holística o en otros casos de tener diferentes capas de seguridad. Independiente de cómo se denomine el enfoque, todos apuntan a lo mismo: contar con múltiples medidas de seguridad que ayuden a controlar los diferentes vectores de ataque, o inclusive tener la capacidad de reaccionar de la mejor manera si algún incidente se llegara a materializar.

Cuenta con antivirus, backup y firewall

De las secciones anteriores, vemos niveles altos en la implementación de controles como un software antivirus o un firewall. Si bien estos indicadores o los de otros controles no son los óptimos, pues esperaríamos que estuvieran más cerca del 100%, sí alcanzan a cubrir una mayoría por lo menos importante.

Pero si comparamos estos datos con la cantidad de empresas que tuvieron algún incidente de seguridad (un porcentaje cercano al 70%) hay algo que pareciera no estar bien. Ya que si los niveles de implementación de controles de seguridad y políticas de seguridad sobrepasan por lo menos las tres cuartas partes de empresas encuestadas, no sería de esperar que casi el mismo porcentaje tenga algún incidente de seguridad.

La respuesta a esta paradoja, la podemos encontrar en el análisis de los mismos datos. Si observamos a las empresas que tienen implementadas medidas de seguridad como el software antivirus, el backup de la información y un firewall concluimos que el porcentaje apenas alcanza un 52%. Es decir que apenas la mitad de las empresas cuenta con los controles más básicos de seguridad, tanto para prevenir incidentes como es caso del antivirus y el firewall, como para recuperarse de un incidente, como lo es con el backup.

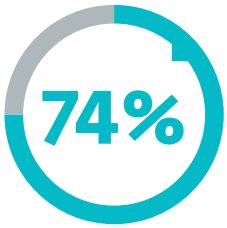
Estamos ante un panorama por demás complicado ya que las empresas no tienen implementadas las diferentes medidas de seguridad que puedan evitar que la información corporativa se vea comprometida por un incidente de seguridad.

Entonces surge el interrogante respecto si la situación sería diferente si las empresas implementaran diferentes medidas de seguridad. Una aproximación indirecta a esta respuesta, la podemos encontrar luego de analizar más profundamente los datos recolectados.

Si tomamos el total de empresas encuestadas y analizamos cuántas de las empresas que sufrieron algún incidente de seguridad tenían implementados controles de seguridad como el software AV, el Firewall y autenticación de usuarios para ingresar a los sistemas, se puede observar que el porcentaje antes mencionado se reduce a la mitad. Es decir que apenas un 20% de las empresas que tenían implementados estos tres controles de seguridad sufrió un incidente de seguridad.

Desde ESET siempre hemos insistido que no basta con tener medidas de control de tipo tecnológico para gestionar la seguridad de forma adecuada. Se deben tener, además, políticas de seguridad y actividades de educación para los empleados. De hecho, al considerar a las empresas que sufrieron al menos un incidente de seguridad que además de las medidas tecnológicas también contaban políticas de seguridad y hacían actividades de capacitación a toda la empresa, el porcentaje de empresas afectadas se reduce únicamente a un 10%. Si bien no es un cero (el número que quisiéramos encontrar) sí se reduce considerablemente la cantidad de empresas que sufrieron algún incidente de seguridad. Estos datos refuerzan el enfoque que planteábamos sobre la necesidad de contar con una protección en capas para proteger la información corporativa y a continuación veremos más datos que profundizan esta relación.

De las empresas que tenían una solución de seguridad como el único control de seguridad, encontramos que el 73% sufrió algún incidente relacionado con infección con códigos maliciosos. ¿Quiere decir esto que las soluciones de seguridad no sirven para detener los incidentes relacionados con las infecciones de malware? No realmente, lo cierto es que tener solamente este control no alcanza para garantizar que la empresa no tenga casos de infecciones con códigos maliciosos.



de las víctimas de ransomware tenía un respaldo de su información

Si la organización cuenta además con políticas de seguridad, las cuales incluyen en muchos casos cómo configurar las soluciones de seguridad, el porcentaje de incidentes se reduce a un 57%; más aún, el indicador se disminuye a un 31% de empresas afectadas por incidentes relacionados con malware en aquellos casos en los que la empresa cuenta con planes de seguridad para todos los empleados.

4.1 El caso del Ransomware

Mucho se ha venido hablando en el último año del ransomware y de lo nefasto que ha sido para las empresas en el mundo. De aquellas que durante 2016 tuvieron un incidente con este malware, solamente el 10% tenía una solución de seguridad, doble factor de autenticación y políticas de seguridad. Es un porcentaje bastante bajo y que nuevamente demuestra que contar con diferentes medidas de seguridad reduce las posibilidades de ser víctima de un incidente de este tipo.

Por otra parte, vale la pena revisar cuántas de las empresas que fueron víctimas de una infección con ransomware estaban preparadas para responder ante este incidente. Del análisis de los datos, encontramos que apenas un 74% tenía respaldada su información con copias de seguridad. Si bien no podemos determinar cuántos de los infectados pagaron el rescate, sí podemos afirmar que existe un porcentaje muy grande que seguramente no pudo recuperar su información ya que se hace muy complicado romper el cifrado de estas amenazas.

Algo adicional y por demás preocupante que pudimos obtener a partir de los datos, y que podría ampliar la cantidad de víctimas que no pudieron recuperar su información luego de una infección con ransomware, está relacionado con la cantidad de empresas que habiendo sufrido una infección de este tipo y teniendo respaldos, realmente contaban con un plan de recuperación de incidentes. Encontramos que apenas una cuarta parte de las empresas tenía estos planes implementados, lo que nos deja con tres cuartas partes que si bien tenían backup no tenían un plan para re-

cuperarse del incidente, lo cual podría implicar incluso que las copias de seguridad no funcionaran o no estuvieran completas.

4.2 La diferencia de las pequeñas implementaciones

Como ya vimos, el tema del presupuesto destinado a seguridad sigue siendo una complicación para muchas empresas en la región. Esto puede plantear una encrucijada para muchas compañías que ven que los incidentes se siguen presentando pero no cuentan con los recursos económicos para enfrentarlos.

Este panorama que parece tan adverso, nos enfrenta a retos que debemos afrontar y que obligan a buscar medidas diferentes no solamente basadas en la adquisición de tecnología para mejorar los niveles de seguridad.

Es verdad que contar con más medidas de control va a mejorar nuestro esquema de seguridad. De hecho, la estrategia de defensa en capas está muy relacionado con el hecho de contar con diferentes medidas y controles que permitan evitar diferentes tipos de amenazas. Pero no es lo único por lo que las empresas deberían preocuparse ya que hay otras alternativas como las políticas de gestión, las de seguridad o la educación de los usuarios que no requieren una inversión directa de dinero, pero que pueden marcar diferencias en la forma en que se gestiona la seguridad.

que realiza actividades de concientización no tuvo incidentes de seguridad

De hecho, si consideramos las empresas que dijeron no tener incidentes de seguridad, el 80% realizó actividades de concientización a toda la empresa, lo cual nos deja ver que esta medida es primordial dentro de los casos en donde se minimizó la cantidad de incidentes.

Si bien el reto no es sencillo, podemos lograr grandes cambios en la gestión de seguridad con la implementación de pequeñas medidas como la educación a todos los empleados de la empresa. La respuesta para mejorar nuestros niveles de seguridad está en ver la gestión de la seguridad como un sistema, el cual abarca desde los empleados de todos los niveles y jerarquías, hasta la implementación de tecnología y procesos de gestión.

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/latam**

/ESETLA /@ESETLA /company/eset-latinoamerica

ENJOY SAFER TECHNOLOGY™