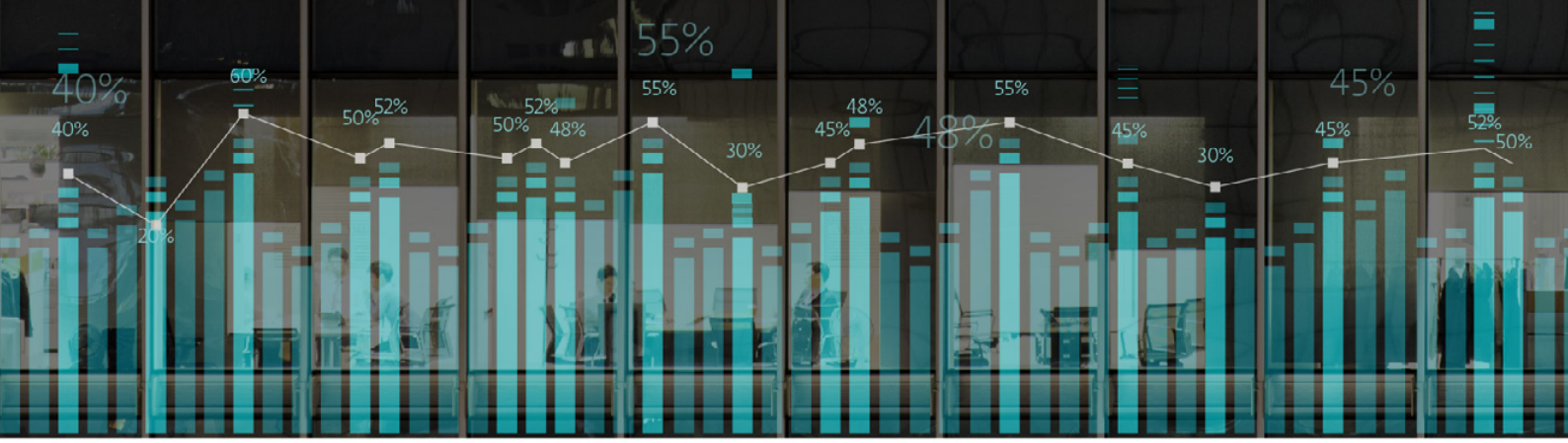
ESET SECURITY REPORT

Latinoamérica 2018



ENJOY SAFER TECHNOLOGY™

Contenido

Introducción

Conocer el estado de la seguridad de la información en las empresas de la región, nos permite tener un panorama general para entender qué prácticas están llevando a cabo, cuáles son sus preocupaciones y cómo trabajan para proteger sus infraestructuras y activos.

Durante 2017, recopilamos información de más de 4500 ejecutivos, técnicos y gerentes que trabajan en más de 2500 empresas de 15 países de la región, divididas en pequeñas (menos de 50 empleados), medianas (entre 50 y 250 empleados), grandes (entre 250 y 1000 empleados) y Enterprise (más de 1000 empleados). A partir de esta información, los especialistas de seguridad del Laboratorio de Investigación de ESET Latinoamérica confeccionamos el **ESET Security Report 2018**, un informe que presenta el estado actual de la seguridad de la información en las empresas en Latinoamérica.

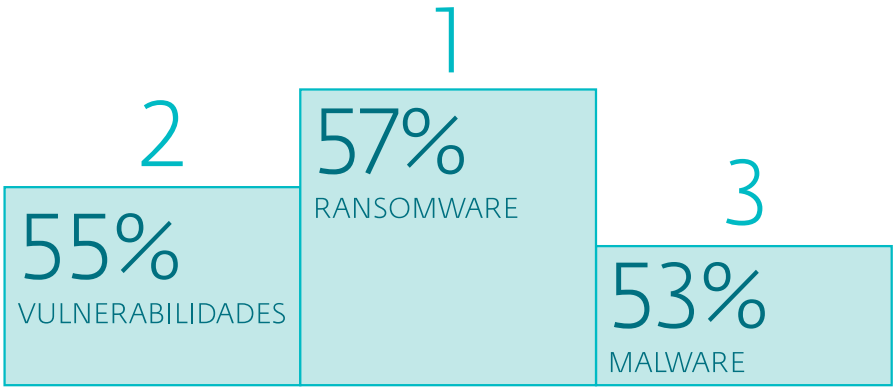
La primera parte del informe estará dedicada a entender las preocupaciones de las empresas en materia de seguridad. Luego, analizaremos los tipos de incidentes reconocidos por dichas empresas para después centrarnos en los controles que se implementan a fin de proteger las redes corporativas, y cómo estos datos se relacionan con las preocupaciones que los profesionales de tecnología dicen tener.

Confiamos en que este análisis proveerá un diagnóstico preciso del estado de la seguridad en empresas de Latinoamérica y esperamos que sea de utilidad para revisar las prácticas de seguridad en su empresa a partir de esta lectura.

+4500	2500	15
PARTICIPANTES	EMPRESAS	PAÍSES

01 > Preocupaciones

Tradicionalmente, el podio de preocupaciones de las empresas en la región estuvo liderado por los códigos maliciosos. Sin embargo, este año fue el ransomware (57%) quien se coronó como líder. Si bien se trata de una variante de código malicioso, a raíz del continuo aumento en los niveles de preocupación en las empresas que venimos viendo durante el último tiempo sobre esta amenaza y los ataques recientes (como WannaCryptor), decidimos darle una categoría para sí mismo en función de hacer un seguimiento del tema de manera más detallada.



De aumento en las detecciones de las familias de FileCoder

El crecimiento de esta preocupación se ve respaldado, de cierta manera, si nos remitimos al crecimiento que vimos durante 2017 de las familias de códigos maliciosos de esta amenaza. Tan solo el año pasado, se identificaron 1190 variantes de familias de FileCoder (la detección para el ransomware), que, si se comparan con las 744 de 2016, muestran un **incremento del 60% en no más de un año**[1]. Resulta claro que esta amenaza llegó para quedarse, y las tendencias no son alentadoras: **el ransomware ha venido evolucionando gracias a la rentabilidad que les ofrece a los atacantes**. Por ello, resulta necesario proteger la información y otros activos de los códigos maliciosos de esta naturaleza.

En segundo lugar, encontramos la explotación de vulnerabilidades (55%), algo esperable si consideramos que 2017 fue el año en el que se reportó la mayor can-

[1] *https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/*

tidad de vulnerabilidades. De acuerdo a la información de la Common Vulnerabilities and Exposures[2], **en 2017 se reportaron más de 14700 vulnerabilidades, contra las 6447 de 2016**. Como se ve, los reportes se duplicaron, lo que significa un aumento por encima del 120%; además, vemos que la cantidad de vulnerabilidades reportadas en los primeros meses de 2018 supera las 6000, lo que indica que este año podría seguir la misma línea. A raíz de esto, las empresas deberían estar atentas a cuáles podrían ser las principales fallas dentro de su infraestructura, en función de prevenir incidentes a futuro.

Malware

Ahora bien, si tomamos las dos principales preocupaciones de las empresas y buscamos entre ellas el punto en común, todo nos llevará a mayo de 2017, cuando cierto ataque de ransomware aprovechó una vulnerabilidad de Windows para propagarse de manera masiva y afectar a más 230 mil equipos en 150 países: **hablamos de WannaCryptor**[3]. Este código malicioso usó algunos de los archivos de la NSA filtrados por Shadow Brokers como vectores de infección, especialmente el exploit que permite la ejecución remota de comando y que aprovecha Eternalblue, una vulnerabilidad en el protocolo SMB.

Robo de información

En tercer lugar, aparece el malware (53%), que engloba a la gran mayoría de las amenazas que pueden llegar a comprometer la seguridad de una empresa. No solo la variedad de este tipo de amenazas es muy amplia en cuanto al tipo de acción que pueden realizar, desde botnets hasta ransomware, sino que también es aprovechado en un amplio espectro de plataformas: desde computadoras hasta dispositivos móviles, **sin dejar afuera los dispositivos IoT**.

A lo largo de este año, entre las amenazas que vienen ganando las primeras posiciones en las detecciones de nuestras soluciones se ubican las relacionadas con el criptojacking[4]. El aumento en la cotización de algunas divisas digitales ha generado una especie de "fiebre por las criptomonedas", en la que la minería no solo es llevada a cabo por las personas que intentan ganar dinero de manera legítima. Los cibercriminales aprovechan esta situación **desarrollando amenazas y provocando ataques para apropiarse de las monedas digitales**, o bien, **utilizando los recursos de cómputo de los usuarios** de Internet, que de manera involuntaria contribuyen a la minería para beneficios de terceros.

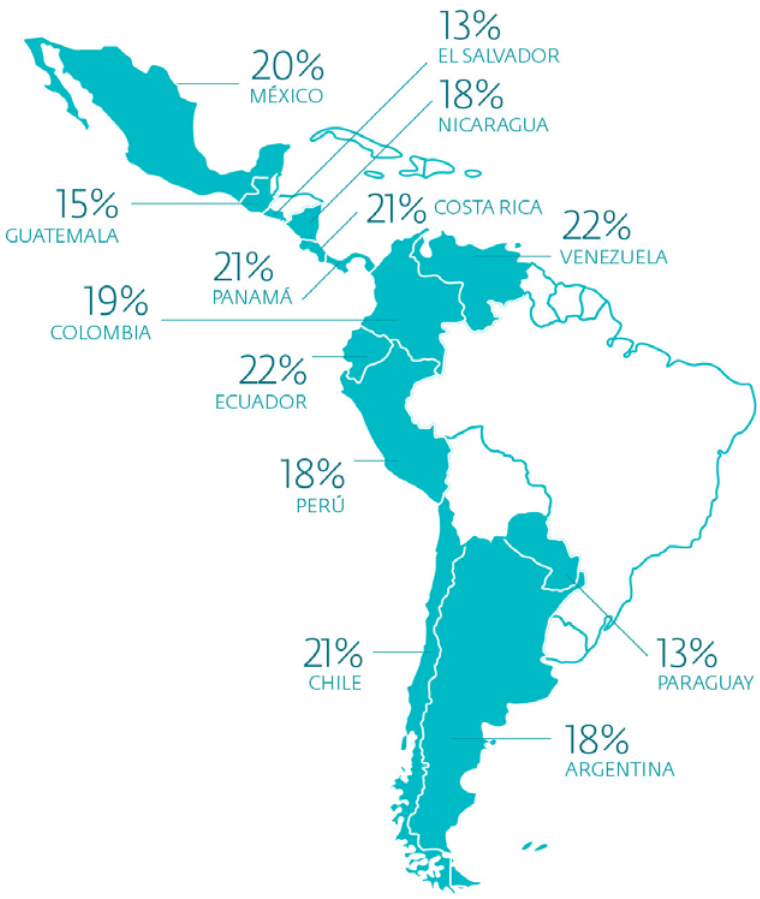
El robo de información (51%) no alcanzó a estar en este podio de preocupaciones, pero, aun así, los números muestran que **más de la mitad de las empresas encuestadas se preocupan por este incidente**. Y dada la amplia variedad de amenazas que pueden emplearse para robar información valiosa, desde ataques externos hasta fraudes, esta actividad se posiciona como una preocupación que vale la pena destacar.

[2] *https://cve.mitre.org/*
[3] *https://www.welivesecurity.com/la-es/2017/05/15/wannacryptor-todos-hablaron-de-seguridad/*
[4] *https://www.welivesecurity.com/la-es/2018/01/17/criptomoneda-campo-minado-trampas-ciberseguridad/*

02 > Incidentes

Tras revisar la información recolectada, se hace evidente que al menos tres de cada cinco empresas en la región sufrieron por lo menos un incidente de seguridad, estando en el top la infección con **códigos maliciosos (45%)**. La mitad de ellos aparecen relacionados al ransomware, es decir que al menos una de cada cinco empresas encuestadas en toda Latinoamérica fueron víctimas del secuestro de información. De hecho, en el siguiente gráfico puede verse que no existe una gran diferencia entre las empresas encuestadas en cada país, siendo **Ecuador el que tiene un mayor índice de infecciones de ransomware** y El Salvador el que tiene el menor.

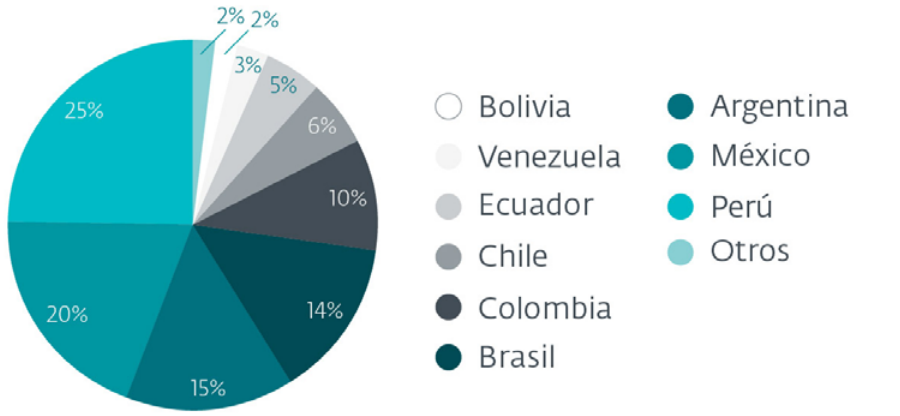
Gráfico 1 > Infecciones de malware por país



Fue el índice de infecciones por malware de Venezuela y Ecuador, los dos países que más sufrieron este incidente

Analizando las detecciones de códigos maliciosos de la familia FileCoder, encontramos que **la mayor cantidad de detecciones durante 2017 estuvo en Perú, con un 25% del total** en los países latinoamericanos. El segundo lugar lo ocupa México, con el 20% de las detecciones, seguido de Argentina (15%), Brasil (14%) y Colombia (10%).

Gráfico 2 > Detecciones de Filecoder en países de LATAM durante 2017



Pero los incidentes relacionados al ransomware no fueron los únicos que se registraron durante 2017 en lo que respecta a malware. Si bien familias como TeslaCrypt, CryptoWall, Cerber, Crysis y Locky fueron las más propagadas en la región, sin olvidar al **infame WannaCry**, las empresas de Latinoamérica también fueron víctimas de otro tipo de códigos maliciosos. Entre las familias con más altos niveles de propagación, se encuentra la llamada Win32/HoudRat, cuyos primeros registros se hicieron presentes durante 2016, y que valiéndose de un lenguaje de scripting como AutoIt, estaba diseñado en sus inicios para tomar capturas de pantalla. Hoy, esta amenaza evolucionó y ya cuenta con funcionalidades de keylogger, robo de información de sitios de comercio electrónico y contraseñas almacenadas en los buscadores y, más recientemente, la **capacidad de minar criptomonedas**.

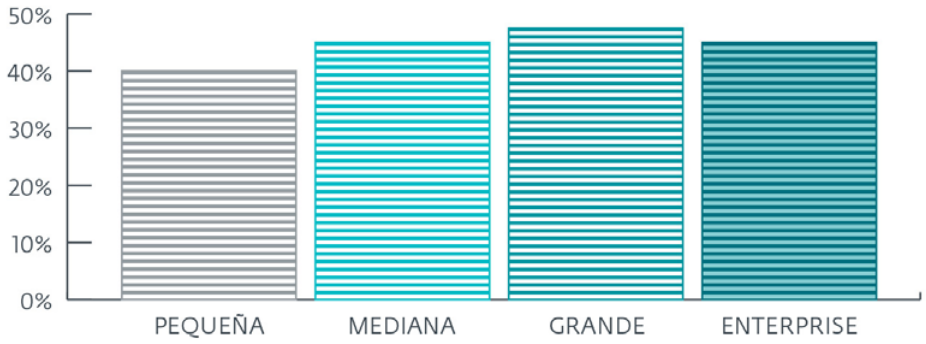
Del total de las detecciones de Bondat se concentran en Perú, México, Ecuador y Colombia

Otro viejo conocido que sigue recorriendo Latinoamérica es Bondat. Esta botnet, que tiene mayor presencia en países como Perú, México, Ecuador y Colombia, donde se concentra más del 85% de las detecciones de la región, sigue robando información de usuarios, y las últimas variantes registradas tienen también módulos de minado de criptomonedas. Al menos la mitad de las familias están relacionadas al cryptojacking, y recién desde agosto del año pasado empezamos a ver detecciones de diferentes **familias de JS/CoinMiner**. Particularmente en estos casos, nos encontramos con que la forma de operar de este tipo de amenazas se inicia comprometiendo un servicio web, y a partir de ello **utiliza los recursos de los usuarios que ingresan al sitio para minar criptomonedas**. El riesgo de esta amenaza está en su capacidad de afectar la reputación de la organización, ya que, si los

usuarios notan que los servidores de una empresa que suelen visitar han sido comprometidos, **su confianza en la institución se verá afectada**. Si bien el efecto no repercute de manera directa en la continuidad del negocio, como sí puede hacerlo el ransomware, el impacto puede ser alto si la cantidad de usuarios afectados es también elevada.

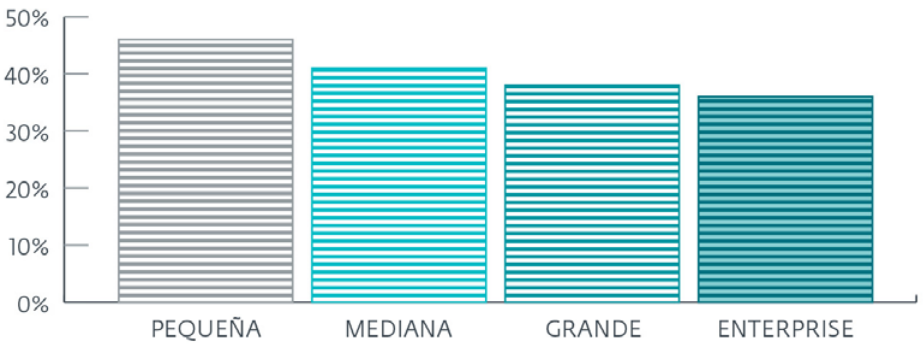
Un análisis interesante de los datos recopilados, evidencia las pequeñas diferencias en cuanto a la incidencia de infecciones con códigos maliciosos en las empresas según su tamaño. Este tipo de amenaza afecta a las empresas de manera muy similar, y **sorprende que en las de mayor tamaño el porcentaje se eleve**, aunque la explicación pueda hallarse probablemente en su capacidad para reconocer más fácilmente un incidente de este tipo, lo cual les deja margen para corregirlo.

Gráfico 3 > Porcentaje de empresas con incidentes de códigos maliciosos por tamaño de empresa



No obstante, al analizar la cantidad de empresas que dijeron no haber tenido incidentes de seguridad, separándolas por tamaño de empresa, los resultados muestran que las pequeñas tuvieron menos incidentes, mientras que las más grandes registraron más. Tal como mencionamos antes, esto nos lleva a pensar que **es muy probable que las empresas más grandes estén mejor preparadas** no solo para detectar incidentes de seguridad, sino también para poder corregirlos.

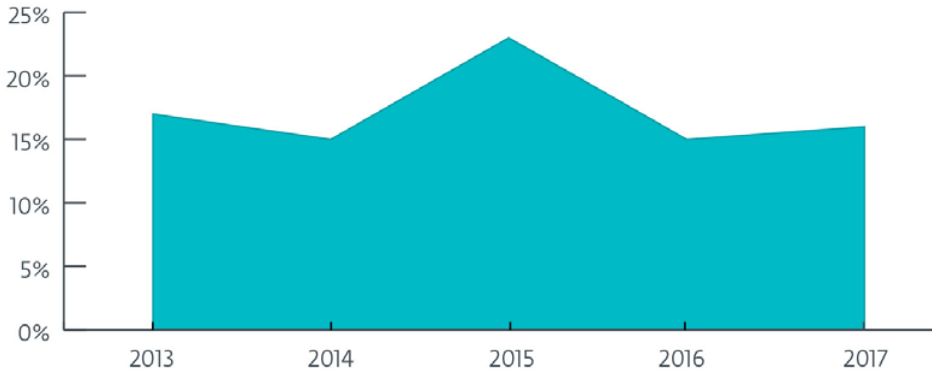
Gráfico 4 > Porcentaje de empresas que dijeron no tener incidentes de seguridad durante los últimos 12 meses por tamaño de empresa.



Pero no todo son códigos maliciosos a la hora de hablar de incidentes de seguridad en las empresas. Detrás de estos, encontramos que por lo menos una de cada diez empresas encuestadas dijo haber sido víctima de incidentes que afectaron la disponibilidad de servicios críticos (10%) o de un acceso indebido a aplicaciones o bases datos (11%). Además, en los últimos años, los porcentajes de empresas que dijeron ser víctimas de ataques de ingeniería social **se han mantenido estables**, con pequeñas diferencias a lo largo de 2017.

Dijo haber sido víctima de incidentes que afectaron la disponibilidad de servicios críticos

Gráfico 5 > Incidentes de seguridad relacionados con ataques de ingeniería social



Es importante resaltar que, los engaños basados en ingeniería social, han evolucionado a lo largo de los años, logrando en muchos casos hacerse más efectivos. En el último tiempo los vimos mutar desde simples sitios de phishing, **hasta webs con certificados SSL falsos o gratuitos** que explotan el desconocimiento del usuario de cara al funcionamiento del protocolo HTTPS, pasando por los ataques homográficos, que cada vez toman más relevancia suplantando empresas y marcas reconocidas.

03 > Implementación de controles

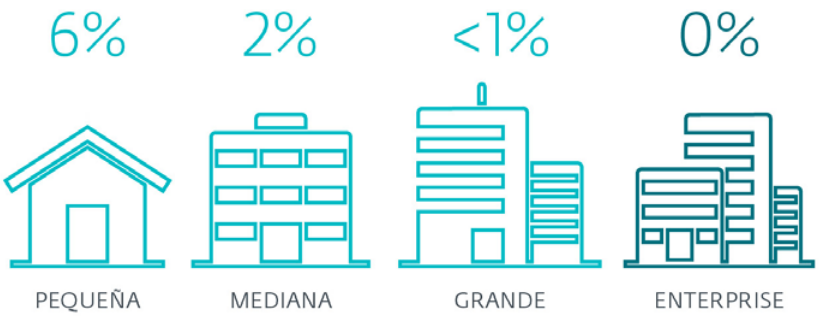
Al hablar de controles de seguridad, probablemente sean muchos los que piensen en contar con alguna solución de seguridad o tecnología de protección, pero pocos se plantearán la **opción de incluir políticas y planes para gestionar la seguridad de la información**.

Esto último se ve reflejado, por ejemplo, en que poco más del 1% de las empresas encuestadas no cuenta con ninguna tecnología de seguridad, mientras que al menos el 25% no posee una política para asegurar su protección.

Estas diferencias están en directa relación con el tamaño de la organización; es decir, el porcentaje de pequeñas empresas que no cuentan con tecnologías de protección es más elevado que el que registran las empresas más grandes.

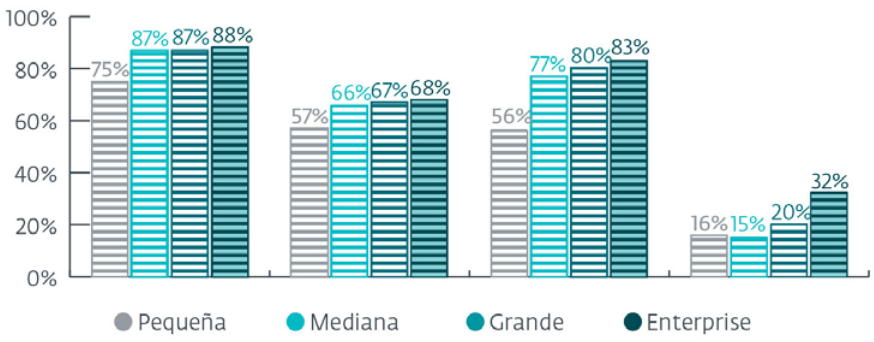
De las empresas no cuenta con una política de seguridad

Gráfico 6 > Porcentaje de empresas que no tienen ningún control de seguridad



Dado que las pequeñas empresas tienen menos dinero para invertir en su seguridad, no todas cuentan con las variadas tecnologías de protección disponibles, y, de acuerdo al análisis de riesgos que hagan de sus entornos, adoptarán diferentes tipos de controles.

Gráfico 7 > Distribución de tecnologías de protección por tamaño de empresa



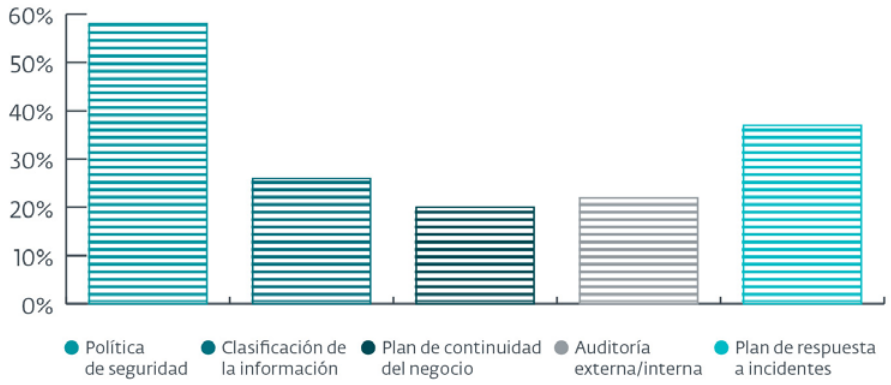
Sin embargo, la tecnología no lo es todo a la hora de hablar de seguridad, sino que **deberá complementarse con una adecuada gestión**; y es en este punto donde hallamos las mayores diferencias y los principales riesgos. Apenas un 58% de las empresas más pequeñas cuentan con una política de seguridad, en contraposición a casi la totalidad de empresas grandes (78%) y Enterprise (84%) que sí cuentan con este tipo de controles. En el caso de las empresas medianas, tres cuartas partes de las encuestadas cuentan con políticas de seguridad.

Quizá uno de los puntos más débiles en cuanto a tecnologías de seguridad está relacionado con los dispositivos móviles. Resulta preocupante que, de todas las empresas encuestadas, apenas el 11% cuente con soluciones de seguridad para este tipo de equipos.

Otro punto que también resulta preocupante y que cabe destacar, es la baja adopción (34%) de tecnologías como las que permiten hacer administración de parches y actualizaciones de software. Habiendo mencionado que 2017 fue histórico en cuanto a la cantidad de vulnerabilidades reportadas, surge como un aspecto esencial para la protección **tener las herramientas que permitan mantener los parches y las actualizaciones al día**. El elevado número de vulnerabilidades reportadas se encuentra acompañado del crecimiento en la cantidad de dispositivos IoT, que debido a su capacidad de procesamiento pueden ser utilizados para realizar algún tipo de ataque o acceder a las redes a las que están conectados.

Además, un incidente bastante recurrente durante los últimos meses ha sido la **fuga de información**. Basta con mirar casos como los de SONY, HBO o Equifax para tomar dimensión del alcance de éstos. Aun así, apenas una de cada diez empresas encuestadas cuenta con una solución de DLP (*Data Loss Prevention*).

Gráfico 8 > Adopción de controles basados en gestión



Los niveles de implementación vistos aquí exponen que los principales cambios no deben realizarse sobre la implementación de controles basados en tecnología, sino en la adopción de políticas, la implementación de planes de gestión, la adopción de estándares o mejores prácticas y la realización de auditorías periódicas del estado de la seguridad.

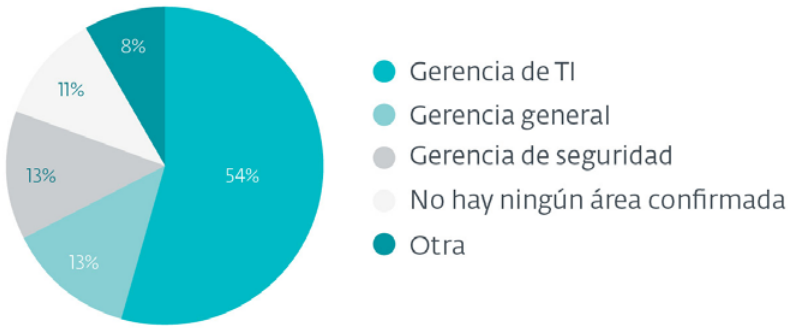
Tiene soluciones de seguridad para moviles

De las empresas cuenta con una solución de DLP

04 > Panorama de la seguridad en LATAM

Dado que la gestión de la seguridad es un proceso integral, nuestro análisis no puede limitarse únicamente a la tecnología y a los controles que se implementen. Debe entenderse, en primera instancia, **cómo está conformada el área de seguridad** de las empresas en la región. A grandes rasgos, observamos que al menos un 10% de las empresas no tiene constituida un área a cargo de la seguridad, exclusivamente.

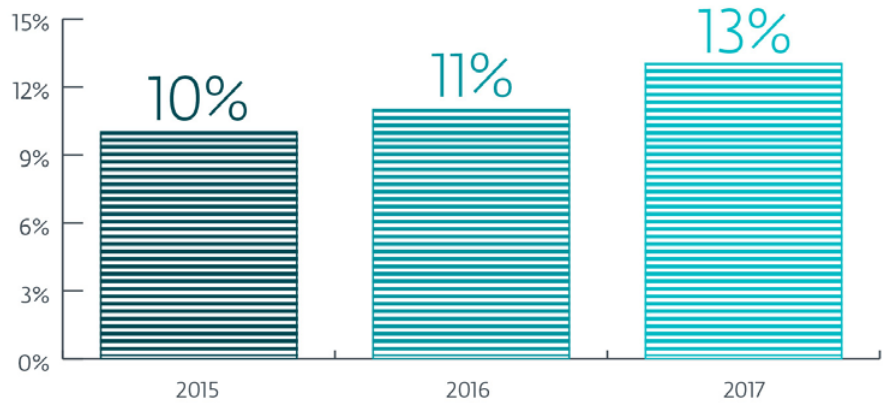
Gráfico 9 > Área encargada de la gestión de la seguridad



Sin embargo, cerca de la mitad de las empresas en Latinoamérica gestiona la seguridad desde su equipo de TI. Si bien esto surge como opción, **las mejores prácticas sugieren la conformación de un área independiente**, con autonomía propia para revisar todas las implementaciones relacionadas a la gestión de la seguridad.

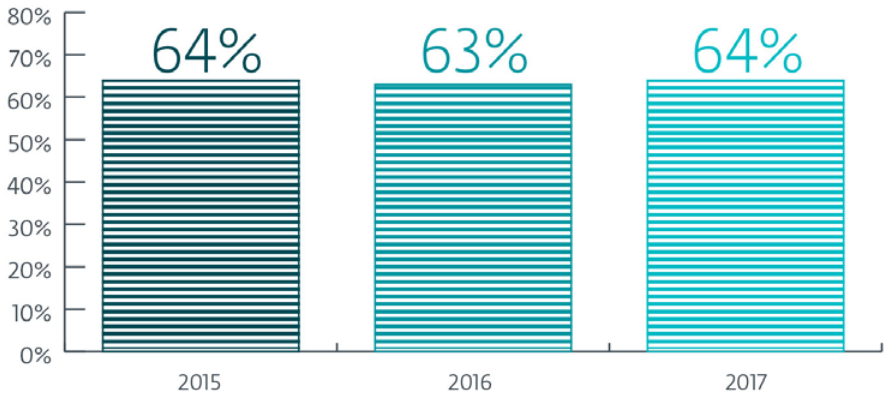
Ahora bien, aun si los porcentajes se mantienen bajos, al analizar los últimos tres años podemos ver que el número de empresas que cuentan con un área independiente para la gestión de su seguridad se ha mantenido estable, **incluso registrando un ligero incremento**.

Gráfico 10 > Evolución en la cantidad de empresas que cuentan con un área dedicada a la gestión de seguridad



Quizá una de las quejas recurrentes en muchas empresas es la **falta de presupuesto** para el área de seguridad, y es esta una cuestión que registró números similares con el paso del tiempo.

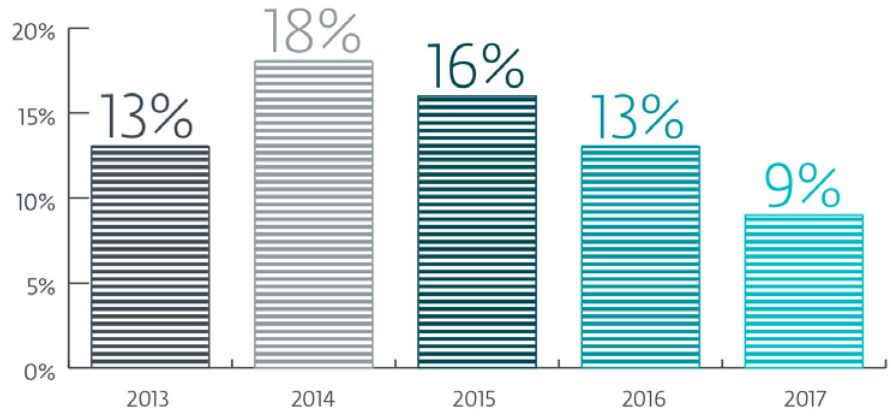
Gráfico 11 > Porcentaje de empresas que consideran que el presupuesto destinado a seguridad no es suficiente



Aun así, pudimos ver que al menos el 46% de las empresas aumentó la cantidad de presupuesto destinado a estas áreas, con respecto al año anterior, e incluso que fue 2017 el año en el que menos empresas (9%) redujeron el presupuesto invertido en seguridad, lo que **representó el porcentaje más bajo en los últimos cinco años**.

De las empresas aumentó el presupuesto para áreas encargadas de la seguridad IT

Gráfico 12 > Porcentaje de empresas que redujeron su presupuesto de seguridad



Realiza actividades periódicas de seguridad

En cierta manera, esto muestra una mayor intención de las empresas de invertir en temas relacionados con su seguridad. Quizá, falte aún una mayor dedicación de tiempo y recursos en pos de lograr los resultados más óptimos, pero sí parece registrarse un esfuerzo en vistas a tomar un mayor control de su entorno a la hora de protegerse.

Finalmente, debemos mencionar el **rol fundamental que cumplen los usuarios y su educación**, como factor diferencial para garantizar la seguridad de la información. Si bien, como mencionamos, queda camino por recorrer en cuanto a la implementación de controles de seguridad, se presenta un panorama positivo a futuro en cuanto a la concientización en la materia, donde más del 75% de las empresas realiza actividades periódicas de seguridad, y al menos un 11% planea implementarlas.

Conclusión

Luego de ver este reporte y analizar los datos que nos brindaron más de 4500 ejecutivos de empresas de la región, lo primero que se destaca es que el **malware perdió el liderazgo en las preocupaciones ante el ransomware**. Y si bien esto puede ser un poco sesgado, dado que el ransomware es un malware en sí mismo, demuestra que nuestra idea de separarlo para darle mayor análisis fue correcta.

Más aún, que este malware que secuestra la información para luego pedir un rescate se haya quedado con el primer escaño del ranking demuestra lo intenso que fue 2017 con el brote de WannaCryptor, que logró algo histórico: **que todo el mundo comenzara a hablar de seguridad informática**. Pero el ransomware no solo se quedó ahí, ya que solo dos meses después apareció el brote de Diskcoder; y hoy en día seguimos viendo cómo los cibercriminales **siguen haciendo uso del exploit EternalBlue** para comprometer a empresas y usuarios de todo el mundo.

Seguidamente, destacamos un **leve descenso de las empresas que se infectaron con códigos maliciosos** entre 2017 (45%) y 2016 (49%). No obstante, de nuevo el ransomware nos obligó a poner el ojo en sus detecciones, lo que nos llevó a ver que sus números son estables entre todos los países de la región, pero que oscilan en porcentajes relevantes, como el 13% y el 22%, por lo que es una amenaza que los encargados de seguridad de las empresas no pueden dejar de atender.

Asimismo, no podemos dejar de mencionar el **crecimiento el cryptojacking**, otra de las amenazas que estuvo bajo el reflector en 2017 y que también evidencia cómo los cibercriminales están muy al día y atentos a las tendencias en Internet, aquí particularmente al boom de las criptomonedas en la economía digital.

Finalmente, una buena noticia es que cada vez son menos las empresas que no cuentan con al menos un control básico de seguridad, como una solución antivirus. Sin embargo, seguimos viendo que **la gestión de la seguridad sigue sin estar demasiado atendida**, lo que representa un problema serio. Como siempre decimos, una óptima seguridad no se logra solo teniendo muchos controles tecnológicos, sino también con una buena gestión de los mismos y de cómo se interrelacionan.

Confiamos en que el panorama aquí presentado será efectivo a la hora de revisar los procesos de seguridad en todas las empresas de la región, y que estos ejemplos sirvan para dar nuevas ideas y desencadenar acciones que permitan aprovechar la tecnología y aumentar la seguridad de forma general.

Durante 30 años, ESET ha desarrollado software y servicios de seguridad de TI líderes en la industria para empresas y consumidores en todo el mundo. Con soluciones que van desde la seguridad para endpoints, equipos hogareños y móviles hasta el cifrado y la doble autenticación, los productos fáciles de usar y de alto rendimiento de ESET brindan tranquilidad a los usuarios y empresas para que disfruten de todo el potencial de la tecnología.

ESET protege y monitorea discretamente las 24 horas del día, los 7 días de la semana, actualizando las defensas en tiempo real para mantener a los usuarios seguros y las empresas funcionando sin interrupción. Las amenazas en evolución requieren de todo un equipo de seguridad que también esté en movimiento y actualización. Respaldada por centros de Investigación y Desarrollo en todo el mundo, ESET se convirtió en la primera compañía de seguridad informática en ganar 100 premios VB100, del laboratorio Virus Bulletin, identificando todas las muestras de malware in-the-wild sin interrupción desde 2003.

Asimismo, desde 2004 ESET opera para la región de América Latina en Buenos Aires, 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 en la región.

Para estar actualizado sobre todas las noticias relacionadas con la seguridad informática visite:
www.welivesecurity.com/latam

ENJOY SAFER TECHNOLOGY™