ESET SECURITY REPORT

Latinoamérica 2019

CYBERSECURITY
EXPERTS ON YOUR SIDE

Contenido

Introducción

Conocer el estado de la seguridad en las empresas de la región, nos permite tener un panorama más amplio para entender qué es lo que éstas están haciendo en materia de seguridad informática, cuáles son sus preocupaciones y cómo actúan para proteger sus infraestructuras.

En este sentido, dedicaremos la primera parte del informe a entender cuáles son las **preocupaciones** de seguridad que registran las empresas, y analizaremos luego los tipos de **incidentes reconocidos** por ellas para registrar qué **controles** implementan a fin de proteger las redes corporativas. Además, veremos cómo estos datos se relacionan con las preocupaciones que los profesionales de la tecnología dicen tener en torno a la seguridad de sus activos informáticos.

Confiamos en que este análisis proveerá un **diagnóstico certero del estado de la seguridad de la información en empresas de Latinoamérica** y esperamos que sea de utilidad para que los responsables de proteger su entorno e infraestructura puedan **establecer comparaciones y revisar sus propias prácticas.**

Hallazgos claves

Resulta interesante que las empresas de la región dijeran haber sufrido **menos incidentes relacionados con el Ransomware que en años anteriores** (de hecho, el porcentaje disminuyó al menos un 10% en los dos últimos años). Sin embargo, los **casos de Ingeniería Social registraron un incremento,** ubicándose dentro del top 3 de los incidentes que más afectaron a las empresas de Latinoamérica en 2018.

Los casos de ingeniería social registraron un incremento, ubicándose dentro del top 3 en 2018.

01

Metodología y fuentes

Los datos recolectados son producto de encuestas realizadas a lo largo del año en múltiples eventos de seguridad, de los cuales participan representantes de diferentes industrias de la región. Este año, **el análisis está basado en las respuestas de más de 3000 profesionales de la seguridad** de diversas organizaciones a lo largo de Latinoamérica.

Además, el ESET Security Report se compone de datos recolectados de **empresas de diferentes tamaños,** el **30% de más de 1000 empleados** y un **15% de por lo menos 500 empleados,** con una participación del **50% de PyMEs.** En total, figuran representados **más de 10 tipos de industrias.** La mayor cantidad de información corresponde a profesionales de entidades de gobierno (20%), a las que le siguen productos y servicios de tecnología (15%), banca y finanzas (12%), educación (9%) y salud (5%). El informe provee datos de empresas de **13 países de la región**, incluyendo Colombia (18%), Argentina (15%), Guatemala (12%), México (10%) y Chile (10%).

+3000
Participantes

13 Países
de la región

Empresas de diferentes tamaños

+1000 empleados

500 empleados

PyMes

02

Panorama de seguridad durante 2018

La transformación digital que tiene lugar en las empresas conlleva una serie de desafíos, y si bien **algunos significarán una ventaja, existirán otros que pueden representar riesgos para la seguridad.**

Son precisamente estos desafíos los que promueven la adopción de nuevos métodos para aumentar la eficiencia en las operaciones, incluyendo tecnologías que aportan agilidad a los procesos comerciales y operativos de la empresa. Y es esta transformación, muchas veces acelerada, la que puede tener consecuencias negativas para la seguridad, debido a la búsqueda constante de vulnerabilidades en la infraestructura de las organizaciones y la creación de nuevas amenazas por parte de los atacantes.

Incidentes

Del análisis de los datos suministrados por empresas de toda Latinoamérica, pudimos observar que **el 61% de las mismas sufrió por lo menos un incidente de seguridad,** siendo la infección con códigos maliciosos el más recurrente, (2 de cada 5 empresas sufrieron una infección de malware, incluyendo ransomware, en 2018).

2 de cada 5
Empresas de Latinoamérica sufrieron una infección de malware en 2018.

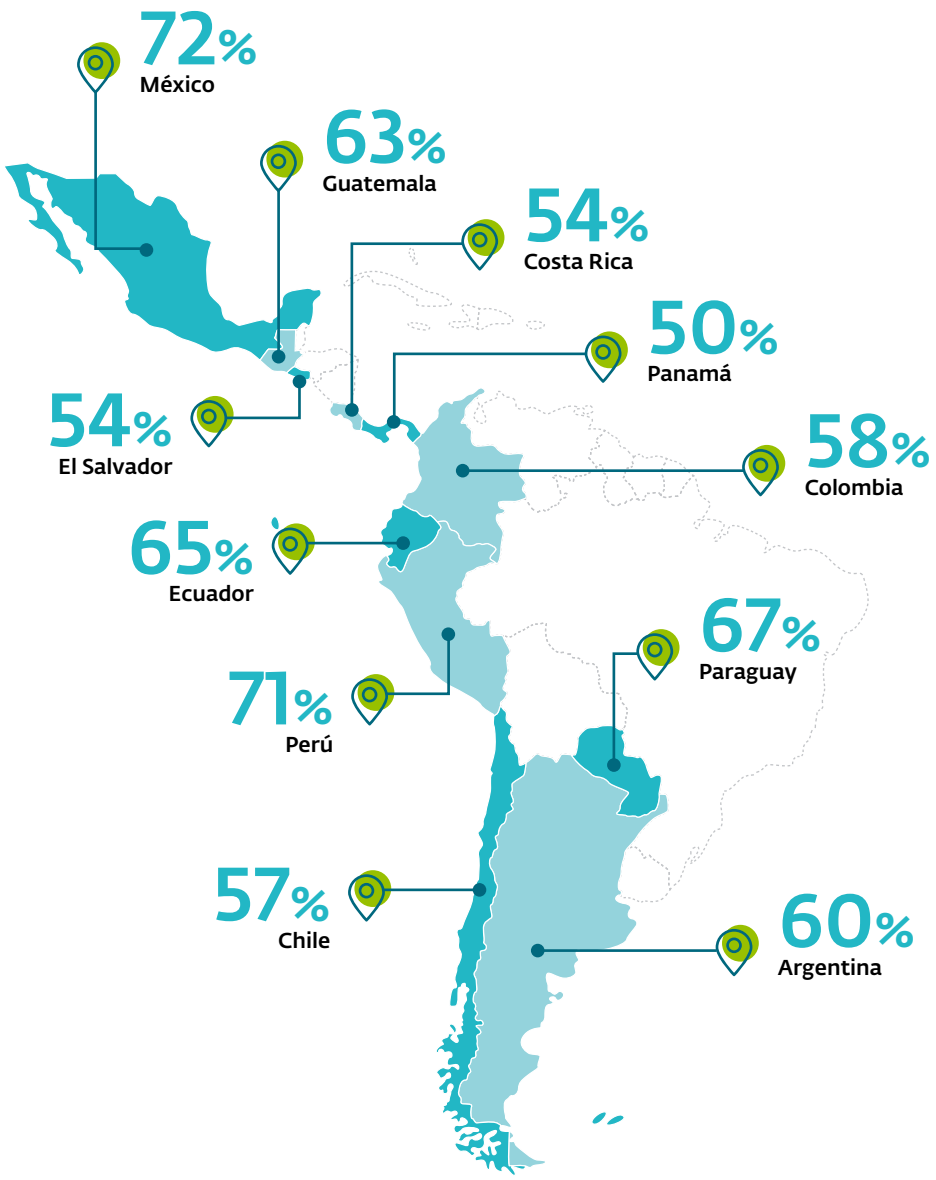
Además, según lo observado, pudo concluirse que **la mitad de estos incidentes está relacionada al ransomware,** es decir que por lo menos 1 de cada 10 empresas encuestadas en toda Latinoamérica sufrió el secuestro de su información.

Sin embargo, en términos generales, **el número de casos de ransomware en las empresas disminuyó en un 10%:** mientras en 2017 la cantidad de empresas víctimas de este código malicioso se acercaba al 18%, 2018 registró un porcentaje total del 8%. Al llevar a cabo un análisis de las detecciones de códigos maliciosos del tipo ransomware de los productos de ESET en países de Latinoamérica, pudo darse cuenta de esta disminución.

10%
Disminuyó la cantidad de casos de ransomware respecto del año anterior.

Sin lugar a dudas, la novedad del ransomware como amenaza predilecta para los cibercriminales ha disminuido. Aún así, dado que su **impacto en la operación de la empresa puede ser muy alto,** debe tenerse en consideración al analizar el riesgo que éste representa para la empresa.

GRÁFICO 1 | Incidentes de seguridad por país

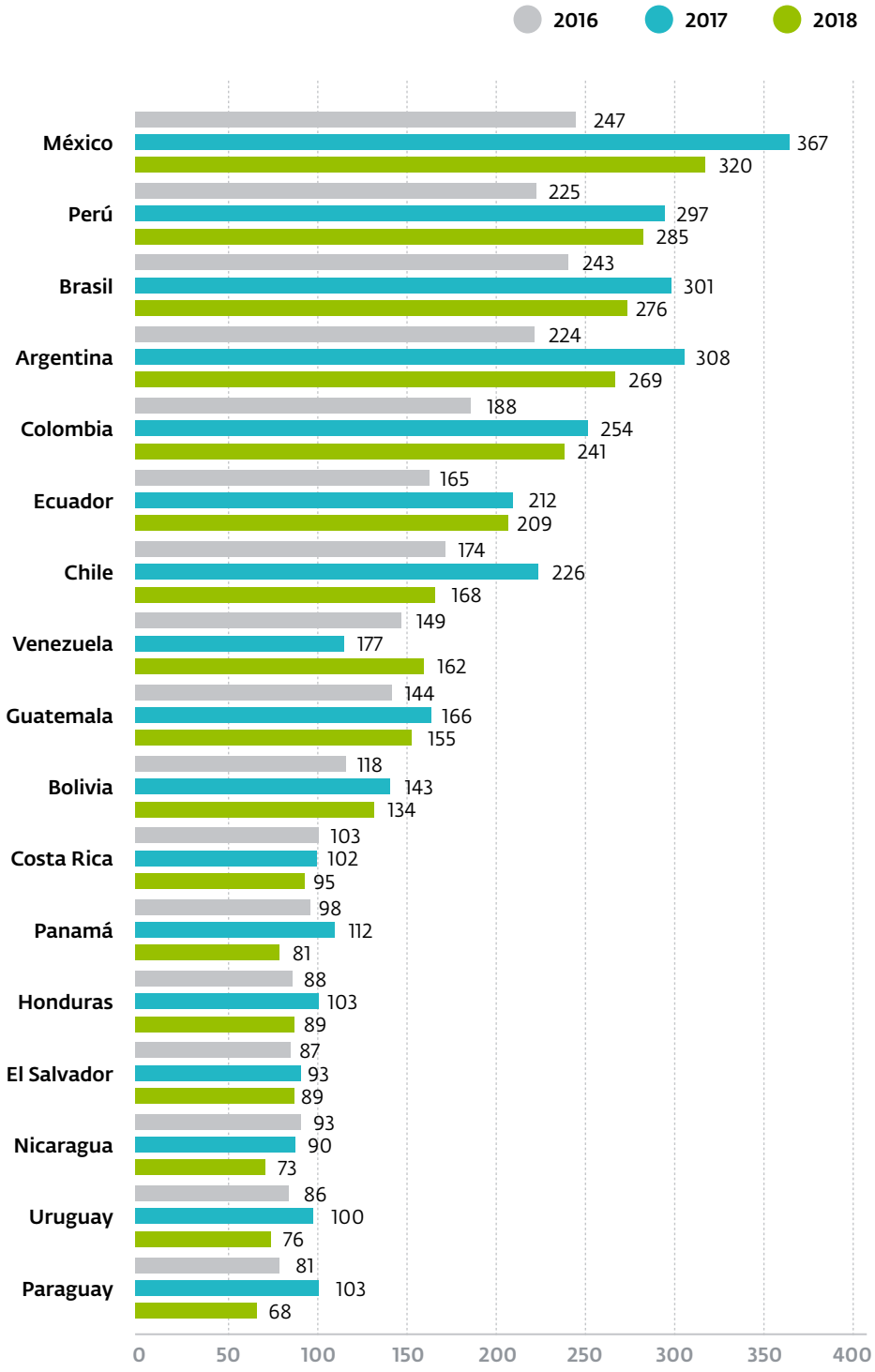


Por último, cabe destacar que, **durante 2017, la actividad de esta amenaza marcó un máximo histórico,** cuando tanto el número de detecciones como la tasa de generación de nuevas variantes registraron un crecimiento exponencial. Aquel año, un tercio de las detecciones se concentró en países de América Latina, siendo Perú (25%) el más afectado de la región.

Este mismo fenómeno se puede observar en la cantidad de variantes diferentes de familias de Ransomware que fueron vistas en países de Latinoamérica. Es importante aclarar que una variante de código malicioso es una versión diferente de un código malicioso conocido, que tiene alguna modificación en su estructura; una

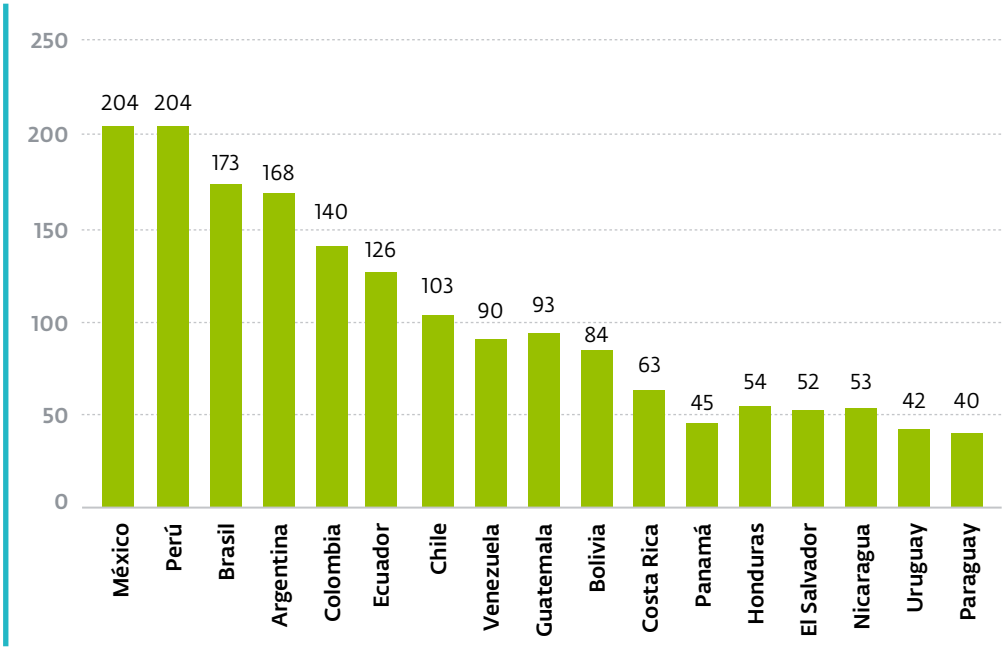
misma variante puede tener asociados archivos o muestras de malware distintas y cada uno de estos archivos propagarse en diferentes tipos de campañas, que tienen el potencial de alcanzar y afectar a miles de usuarios.

GRÁFICO 2 | Cantidad de variantes diferentes de Ransomware vistas en países de Latinoamérica



Ahora bien, si nos enfocamos únicamente en 2019, puede verse una variación en la tendencia en baja de la cantidad de variantes observadas, dado que, durante los primeros meses del año, se observaron valores similares a los registrados en 2018.

GRÁFICO 3 | Cantidad de variantes diferentes de Ransomware vistas en países de Latinoamérica durante 2019



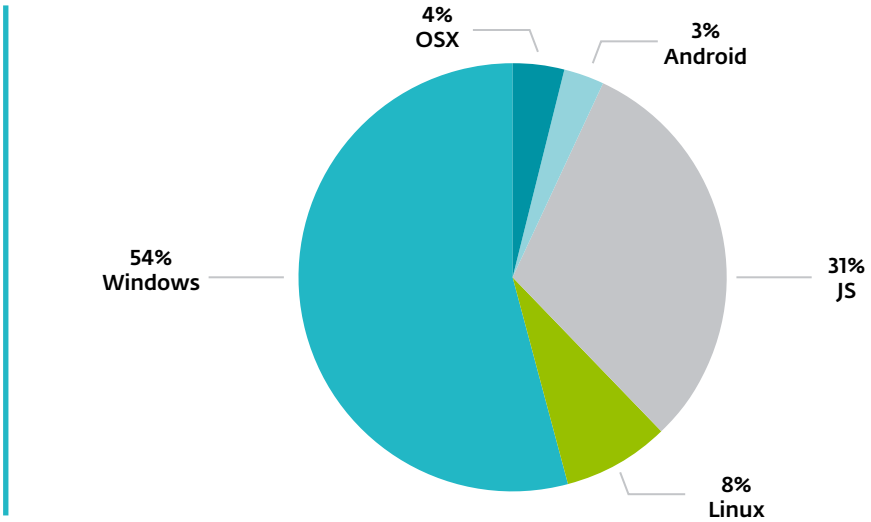
Otro número que pueda dar cuenta de esto es el de la cantidad de variantes nuevas vistas a lo largo de cada período. Durante 2017 se detectaron por lo menos 226 variantes que no se habían visto en años anteriores, esto representó el 39% del total de variantes vistas. **Durante 2018 la relación fue del 26%, con un total de 151 variantes no vistas en años anteriores.** Y si bien durante 2019 la relación se mantiene en un 26%, el total de variantes no vistas en años anteriores es de 106, un valor cercano al del año anterior en poco menos de seis meses.

2018
Se consolidó como medio de infección la minería de criptomonedas.

Pero los incidentes relacionados con Ransomware no fueron los únicos ocurridos durante 2018 en lo que respecta al malware. El último año, **se consolidó como medio de infección la minería de criptomonedas.** Las variantes que corresponden a este comportamiento son identificadas por los productos de ESET como CoinMiner y están disponibles para diferentes arquitecturas[1].

[1] ***Las amenazas informáticas que más afectaron a los países de América Latina.***
www.welivesecurity.com/la-es/2019/01/10/amenazas-informaticas-mas-afectaron-paises-america-latina

GRÁFICO 4 | Distribución de detecciones de Coin Miners por plataforma



El principal riesgo de esta amenaza reside en cómo puede afectar a la reputación de una organización, ya que, si los usuarios notan que los servidores de cualquier empresa que suelen visitar han sido comprometidos, su confianza en ella podría perderse o verse erosionada. Si bien los resultados, en estos casos, no impactan directamente sobre la continuidad del negocio, como sí lo hace el ransomware, las consecuencias pueden ser graves si la cantidad de usuarios afectados es alta.

A pesar de que el mercado de las criptomonedas es bastante volátil, y en los últimos meses hemos sido testigos de bajas y alzas en sus precios durante períodos muy cortos de tiempo, es habitual que los **cibercriminales usen la capacidad de cómputo de las víctimas para minar criptomonedas.** Muestra de esto es el crecimiento en la cantidad de variantes de códigos maliciosos del tipo minero que se ha visto en los países de la región en los últimos años. De hecho, **los valores registrados durante los primeros meses de 2019 en muchos países iguala, y en algunos casos supera, las cantidades vistas durante 2017.**

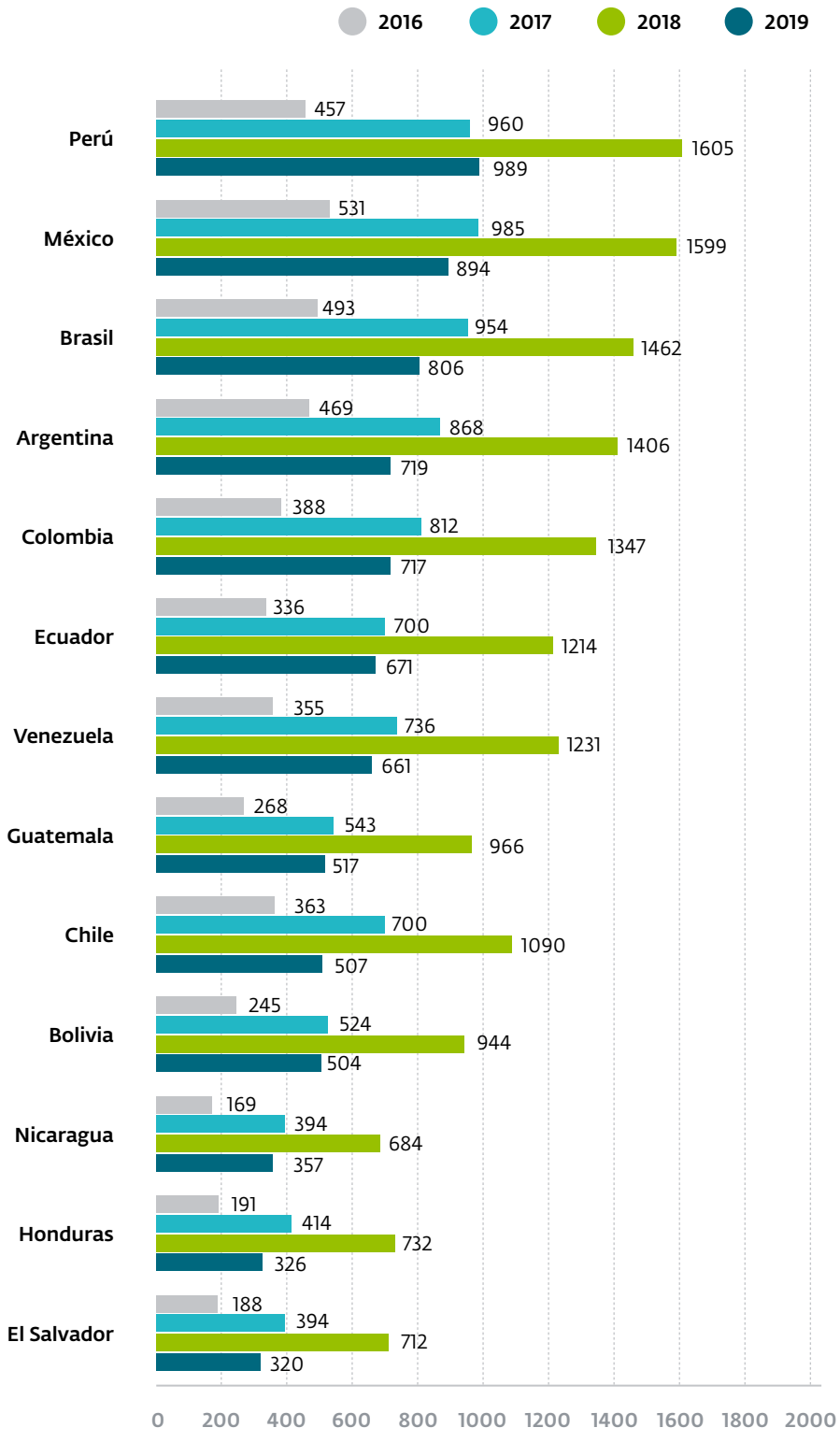
En líneas generales, los códigos maliciosos son un problema que va en aumento para los usuarios en la región. Tal es así que **un análisis sobre la cantidad de archivos maliciosos vistos durante 2018 da cuenta de un crecimiento del 7%,** llegando a más 750 millones solo en países de Latinoamérica. Para mostrar aún más la significancia de este crecimiento, **si comparamos los primeros meses de 2019 con lo que vimos en los primeros meses de 2018, la cantidad de archivos únicos ya fue superada en casi un 30%,** por encima de los 360 millones de archivos maliciosos registrados.

7%
De crecimiento respecto al año anterior, en la cantidad de archivos maliciosos vistos en Latinoamérica durante 2018.

Además de los códigos maliciosos, surgen también como incidentes el **acceso indebido a la información,** con un 20% de las empresas afectadas, seguido por

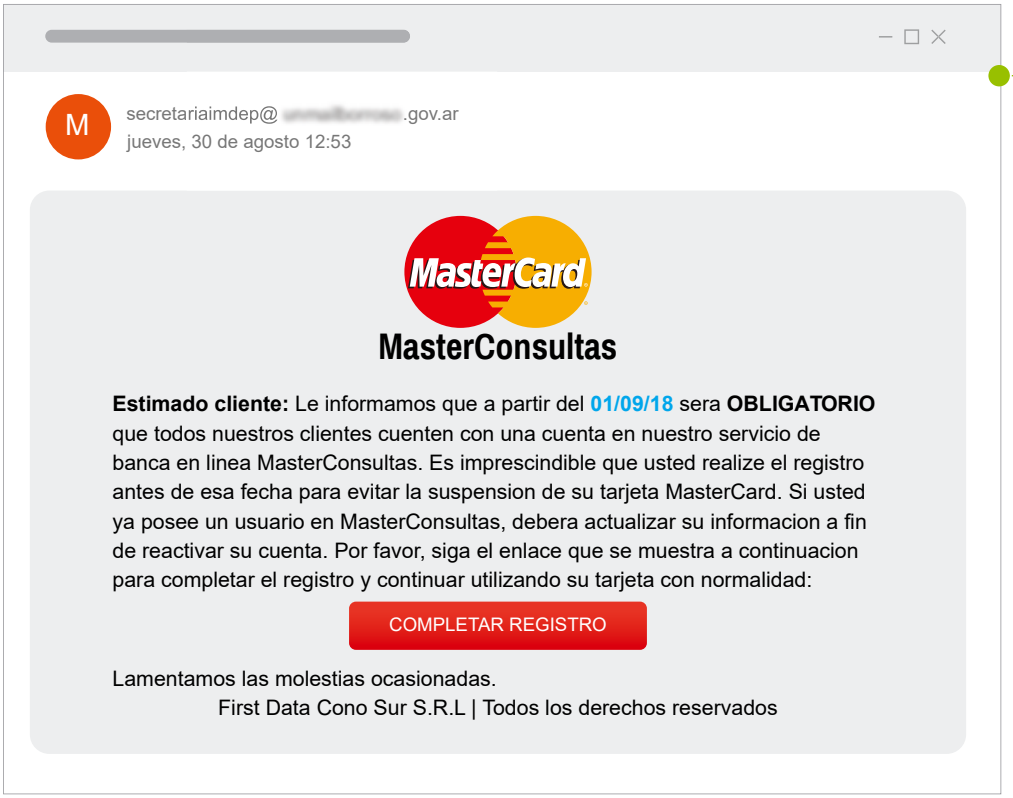
la **Ingeniería Social,** con el 15%, siendo esta última la que mayor crecimiento registró como incidente en los últimos meses.

GRÁFICO 5 | Cantidad de variantes diferentes de Miners vistas en países de Latinoamérica



De hecho, puede asociarse el incremento en el número de incidentes relacionados a la Ingeniería Social con la amplia variedad de campañas de phishing que vimos durante el año pasado, haciendo uso de algunas marcas reconocidas:

Suplantación de Apple

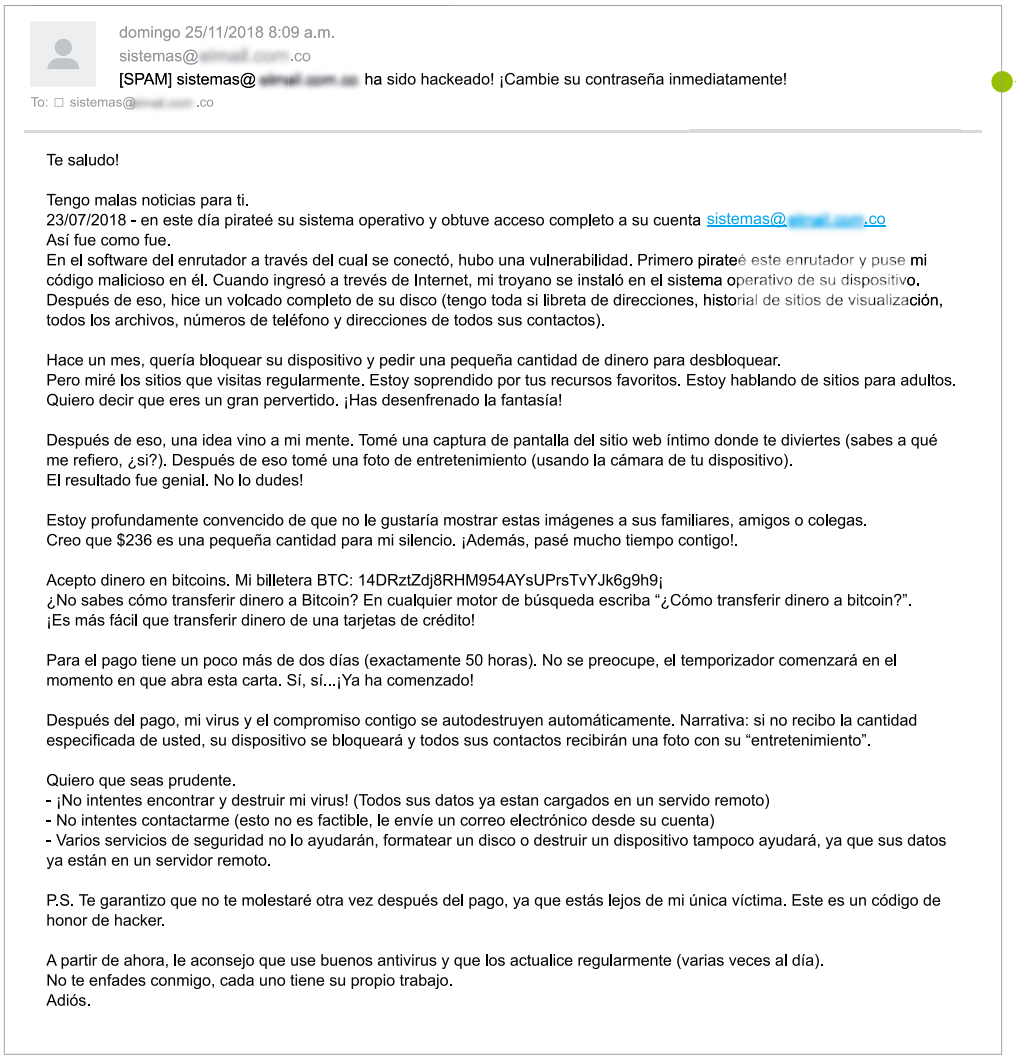


Suplantación de MasterCard

Suplantación de Netflix

Suplantación de Nespresso

Pero no fueron estas campañas las únicas que registraron un incremento durante 2018, sino que **comenzamos a ver otro tipo de engaño, que persiste hasta estos días**[2] , y consiste en el envío de un correo al usuario, con una contraseña utilizada por éste en algún momento, **extorsionándolo a través de supuestas imágenes con contenido sexual capturadas por la cámara web de su dispositivo.** Todos estos engaños nacen precisamente de las masivas fugas de datos relacionadas a servicios que vemos a menudo, y de la posibilidad que tienen los atacantes de usar esta información en contra de las víctimas.



domingo 25/11/2018 8:09 a.m.
sistemas@[redacted].co
[SPAM] sistemas@[redacted] ha sido hackeado! ¡Cambie su contraseña inmediatamente!
To: ☐ sistemas@[redacted].co

Te saludo!

Tengo malas noticias para ti.
23/07/2018 - en este día pirateé su sistema operativo y obtuve acceso completo a su cuenta sistemas@[redacted].co
Así fue como fue.
En el software del enrutador a través del cual se conectó, hubo una vulnerabilidad. Primero pirateé este enrutador y puse mi código malicioso en él. Cuando ingresó a través de Internet, mi troyano se instaló en el sistema operativo de su dispositivo.
Después de eso, hice un volcado completo de su disco (tengo toda si libreta de direcciones, historial de sitios de visualización, todos los archivos, números de teléfono y direcciones de todos sus contactos).

Hace un mes, quería bloquear su dispositivo y pedir una pequeña cantidad de dinero para desbloquear.
Pero miré los sitios que visitas regularmente. Estoy soprendido por tus recursos favoritos. Estoy hablando de sitios para adultos.
Quiero decir que eres un gran pervertido. ¡Has desenfrenado la fantasía!

Después de eso, una idea vino a mi mente. Tomé una captura de pantalla del sitio web íntimo donde te diviertes (sabes a qué me refiero, ¿si?). Después de eso tomé una foto de entretenimiento (usando la cámara de tu dispositivo).
El resultado fue genial. No lo dudes!

Estoy profundamente convencido de que no le gustaría mostrar estas imágenes a sus familiares, amigos o colegas.
Creo que $236 es una pequeña cantidad para mi silencio. ¡Además, pasé mucho tiempo contigo!.

Acepto dinero en bitcoins. Mi billetera BTC: 14DRztZdj8RHM954AYsUPrsTvYJk6g9h9¡
¿No sabes cómo transferir dinero a Bitcoin? En cualquier motor de búsqueda escriba "¿Cómo transferir dinero a bitcoin?".
¡Es más fácil que transferir dinero de una tarjetas de crédito!

Para el pago tiene un poco más de dos días (exactamente 50 horas). No se preocupe, el temporizador comenzará en el momento en que abra esta carta. Sí, sí...¡Ya ha comenzado!

Después del pago, mi virus y el compromiso contigo se autodestruyen automáticamente. Narrativa: si no recibo la cantidad especificada de usted, su dispositivo se bloqueará y todos sus contactos recibirán una foto con su "entretenimiento".

Quiero que seas prudente.
- ¡No intentes encontrar y destruir mi virus! (Todos sus datos ya estan cargados en un servido remoto)
- No intentes contactarme (esto no es factible, le envíe un correo electrónico desde su cuenta)
- Varios servicios de seguridad no lo ayudarán, formatear un disco o destruir un dispositivo tampoco ayudará, ya que sus datos ya están en un servidor remoto.

P.S. Te garantizo que no te molestaré otra vez después del pago, ya que estás lejos de mi única víctima. Este es un código de honor de hacker.

A partir de ahora, le aconsejo que use buenos antivirus y que los actualice regularmente (varias veces al día).
No te enfades conmigo, cada uno tiene su propio trabajo.
Adiós.

Extorsión a través del correo electrónico

Los engaños basados en ingeniería social han evolucionado a lo largo de los años, volviéndose cada vez más efectivos.

Es importante resaltar que **este tipo de engaños, basados en Ingeniería Social, han evolucionado a lo largo de los años, volviéndose cada vez más efectivos.** En el último tiempo, hemos visto una evolución que va desde simples sitios de phishing, pasando por los ataques homográficos, que cada vez toman más relevancia con la suplantación de empresas y marcas reconocidas, hasta sitios con certificados SSL falsos o gratuitos, que explotan el desconocimiento de los usuarios sobre el funcionamiento del protocolo HTTPS.

[2] ***Continúan las campañas de extorsión a través del correo.***
www.welivesecurity.com/la-es/2019/02/11/continuan-las-campanas-de-sextorsion-a-traves-del-correo

Otro de los incidentes con altos niveles de ocurrencia entre las empresas de Latinoamérica fue la **explotación de vulnerabilidades, que afectó a cerca del 10% de las empresas,** y en algunos países como Perú (+7%), México (+3%) y Chile (+3%), se vio incluso un incremento. Quizás una de las cuestiones más preocupantes con este tipo de incidentes en lo que respecta a 2018 es el **aumento en la cantidad de detecciones de exploits, del 117% respecto a 2017 y del 241% respecto a 2016.** De hecho, no se habían registrado tantas detecciones desde el año 2010. Esta realidad se vio reflejada justamente en América Latina, siendo México (21%) y Perú (13%)[3] los países más afectados.

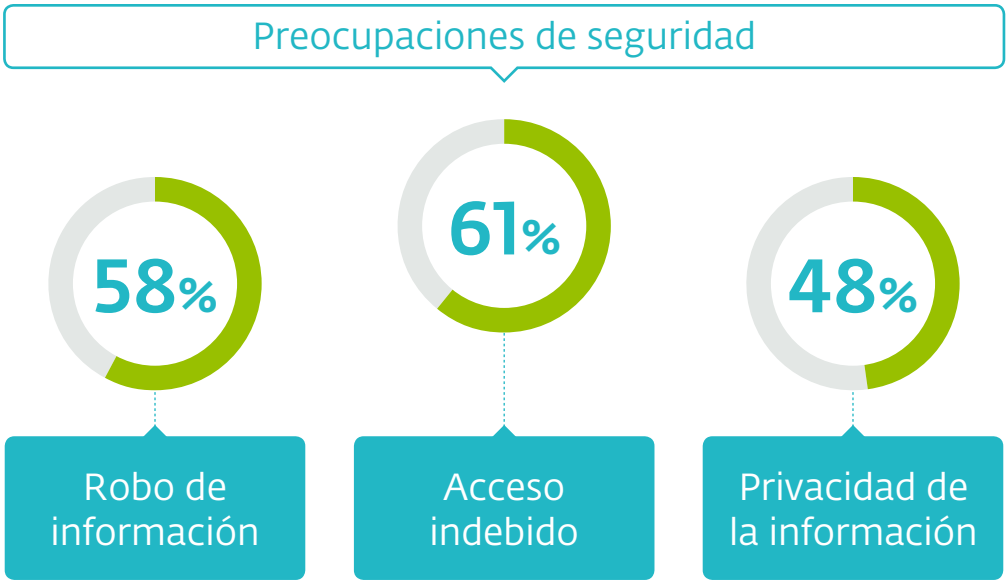
117%
Es el aumento en la cantidad de detecciones de exploits que se registró en 2018.

Percepción de la seguridad

Todo este panorama de incidentes y amenazas trae aparejado el interés de las empresas por la seguridad de su información. **El 61% de las empresas en Latinoamérica manifestó que su mayor preocupación respecto a la seguridad, es el acceso indebido.** Sin embargo, esta no es su única inquietud y el podio lo completan el **robo de información (58%) y la privacidad de la información (48%).**

61%
De las empresas en Latinoamérica manifestó que su mayor preocupación respecto a la seguridad, es el acceso indebido.

Era de esperar que estas preocupaciones fueran las más relevantes para las empresas ya que, durante el año pasado, los casos de fuga de información fueron noticia recurrente. De hecho, 2018 quedará en la historia como el año en el que la protección de datos y la privacidad tomaron un rumbo diferente e histórico, luego de que haya **entrado en efecto el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés)** dentro de la Unión Europea, logrando un alcance global.



[3] ***Las amenazas informáticas que más afectaron a los países de América Latina.***
www.welivesecurity.com/la-es/2019/01/10/amenazas-informaticas-mas-afectaron-paises-america-latina

Si bien a futuro se puede imaginar un escenario más optimista, hay que tener en cuenta que a los múltiples casos de brechas de seguridad y exposición de datos de usuarios ocurridos durante 2018 **ya se le han sumado varios en lo que va de 2019.** Por ejemplo, el denominado *Collection #1*, en el que cerca de 773 millones de direcciones de correo únicas y más de 21.2 millones de contraseñas únicas, utilizadas para acceder a sitios de terceros (en texto plano), fueron filtradas de forma masiva.

Además de las ya mencionadas, **los códigos maliciosos siguen estando dentro de las mayores preocupaciones de las empresas de la región con un 57%.** De hecho, lo problemático es que la gran mayoría de los ataques que pueden llegar a comprometer la seguridad de una empresa están asociados con alguna variante de malware. La gran variedad de acciones maliciosas que este tipo de amenazas puede realizar (desde botnets hasta ransomware), sumado al amplio espectro de plataformas en las que se pueden utilizar (computadoras, dispositivos móviles, dispositivos IoT, etc.) convierten al malware en **una de las técnicas más usadas por los atacantes.**

Particularmente en 2019, ya hemos visto cómo los cibercriminales utilizan técnicas variadas para propagar sus amenazas. Un ejemplo claro fue el uso de la vulnerabilidad de WinRAR, publicada en los primeros meses del año. Un par de días después de descubierta la falla, ya se conocían exploits y campañas maliciosas que buscaban aprovecharla para propagar algunas familias de ransomware.

Códigos maliciosos
Sigue siendo una de las mayores preocupaciones de las empresas

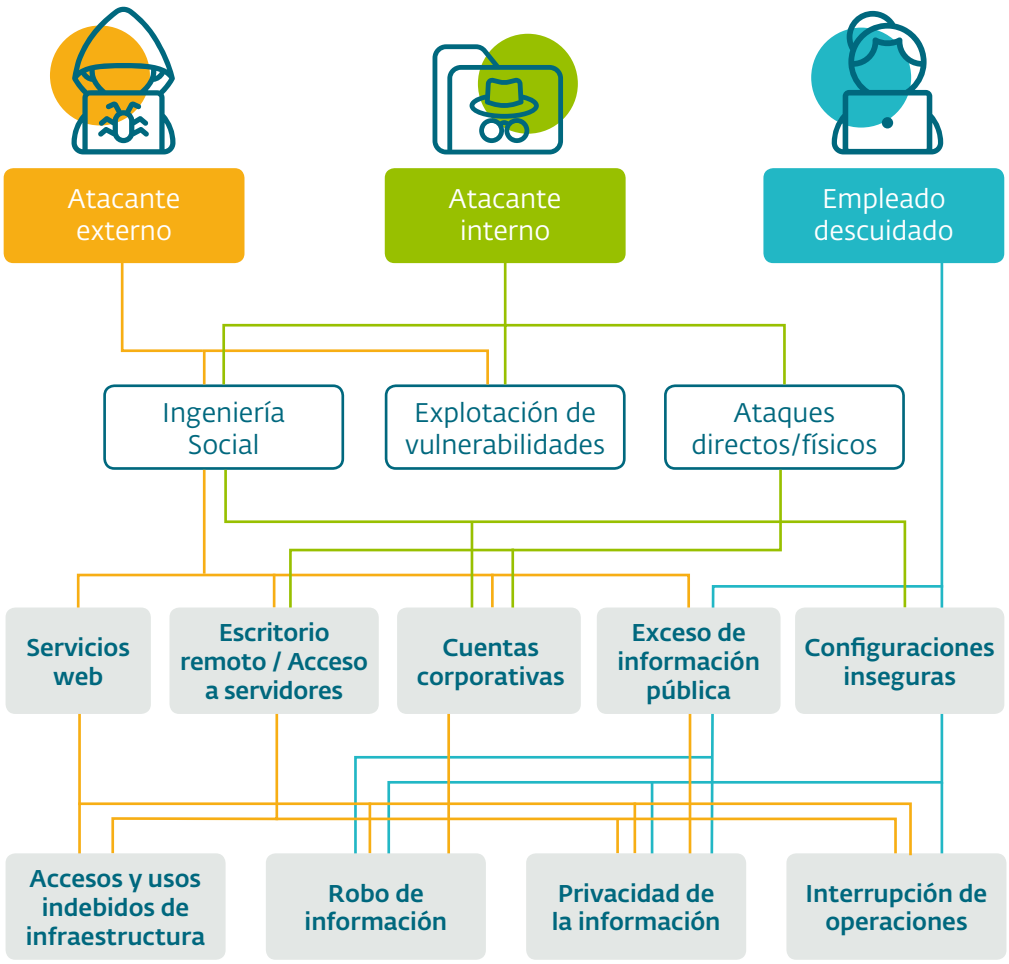
Cómo ocurren los ataques

Considerando la amplia variedad de amenazas que pueden llegar a afectar a las empresas y las principales preocupaciones en materia de seguridad, es importante identificar las diferentes vías por las cuales puede llegar un ataque. De esta forma, se podrán tomar las medidas de control más adecuadas.

Desde el Laboratorio de Investigación de ESET, empleamos datos obtenidos por medio de nuestras soluciones de seguridad para elaborar un diagrama con **las vías más utilizadas en los ataques.** Las mismas **fueron identificadas en nuestros clientes de la región.** Es importante destacar que, si bien muchas veces los ataques llegan desde el exterior de la organización, también pueden darse desde el interior de la empresa, ya sea por descuidos o malas prácticas de seguridad.

La Ingeniería Social y la explotación de vulnerabilidades siguen siendo los principales vectores que puede aprovechar un atacante para comprometer los servicios de una empresa.

En cualquier caso, **la Ingeniería Social y la explotación de vulnerabilidades siguen siendo los principales vectores** que puede aprovechar un atacante para comprometer los diferentes servicios que una empresa utiliza. A estos se suman las acciones maliciosas que pueden darse cuando alguien, de manera malintencionada, busca hacer algún daño a la información aprovechando los accesos físicos que puede tener. Es fundamental tener en cuenta que, independientemente del camino o el actor que esté detrás del incidente de seguridad, la continuidad del negocio siempre puede verse afectada.



03

Control y prevención de riesgos

Ante el panorama anterior, y entendiendo que son múltiples las vías por las cuales un atacante puede llegar a comprometer la seguridad de una organización, es necesario conocer **cómo se protegen las empresas en la región y dónde pueden estar las opciones de mejora** para incrementar los niveles de seguridad.

Es importante mencionar que **la seguridad de la información debe abordarse desde un enfoque por capas,** las cuales no deben estar basadas exclusivamente en el uso de tecnología. Cuando se habla de controles de seguridad quizás lo primero en lo que se piensa es en contar con tecnologías de protección, lo cual es evidentemente necesario, pero probablemente pocos tengan en cuenta **la importancia de contar con políticas y planes para gestionar la seguridad de la información.**

Lo anterior se ve reflejado precisamente en que más del 99% de las empresas de la región tienen algún control basado en tecnología, que puede ir desde una solución de seguridad hasta un DLP, mientras que **2 de cada 5 empresas todavía no cuentan con Políticas de seguridad,** y apenas un 28% clasifica su información.

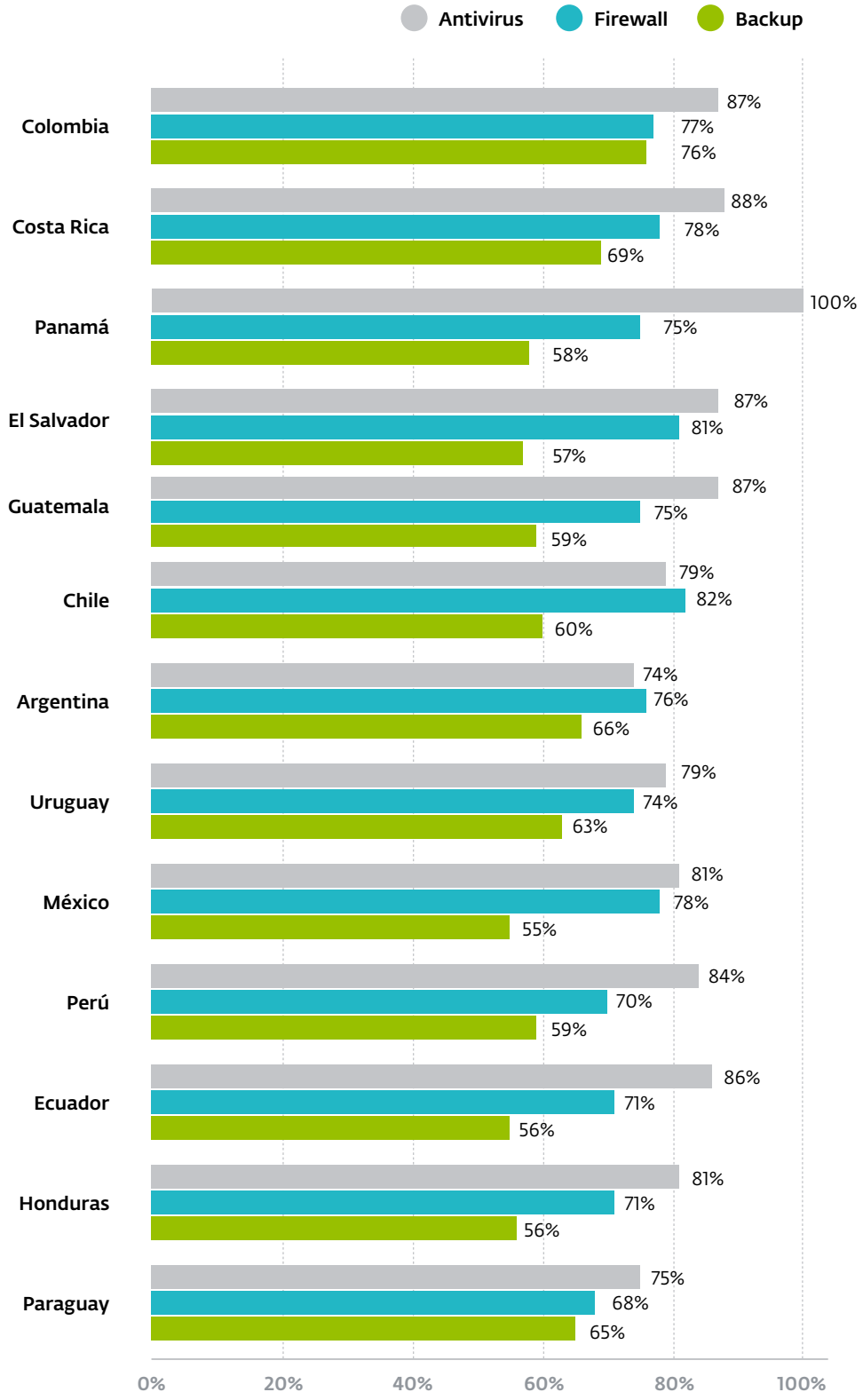
2 de cada 5
Empresas todavía no cuentan con Políticas de seguridad.

28%
De las empresas de la región, clasifica su información.

Controles

Una de las cuestiones que más sorprende es que las medidas más básicas de control que uno esperaría ver en todas las empresas, a saber: una solución de seguridad (Antivirus), un backup y una solución de Firewall, no están implementadas en todas las compañías encuestadas, de hecho, solo un **50% cumple con estas medidas elementales.**

GRÁFICO 6 | Niveles de implementación de controles básicos de seguridad por país



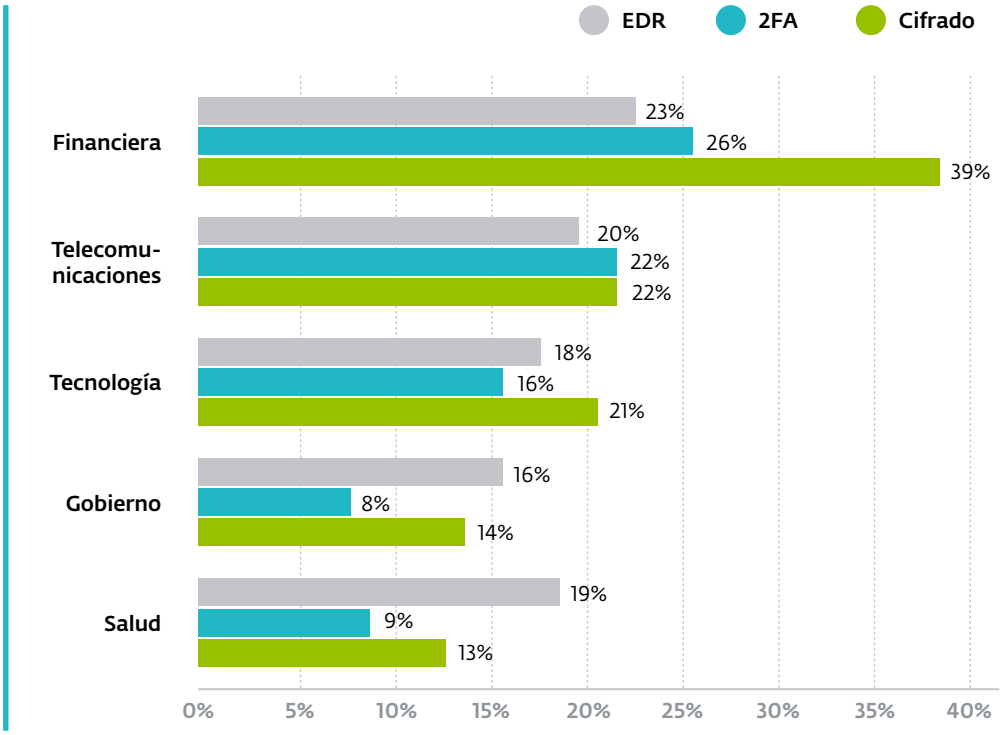
El **control más utilizado sigue siendo el antivirus (83%)** lo que lo pone al frente como la primera línea de defensa contra los atacantes.

Dado el amplio abanico de posibilidades que tienen los atacantes para comprometer la seguridad de una empresa, en los últimos años han ido apareciendo nuevas tecnologías para complementar la protección. Sin embargo, notamos que su adopción aún es bastante baja. Por ejemplo, un **segundo factor de autenticación es considerado como una opción por apenas el 13% de las empresas encuestadas, valor apenas superado por un 16% de las empresas que cuentan con un EDR o el 18% de las empresas que cifran su información.**

13%
De las empresas encuestadas considera utilizar Segundo Factor de Autenticación para complementar la protección.

Según los datos recolectados, **la industria Financiera es la que marca la tendencia en la adopción de las tecnologías de protección,** seguido por las empresas de Telecomunicaciones y las de Tecnología. En la retaguardia se encuentran los sectores de Salud y de Gobierno.

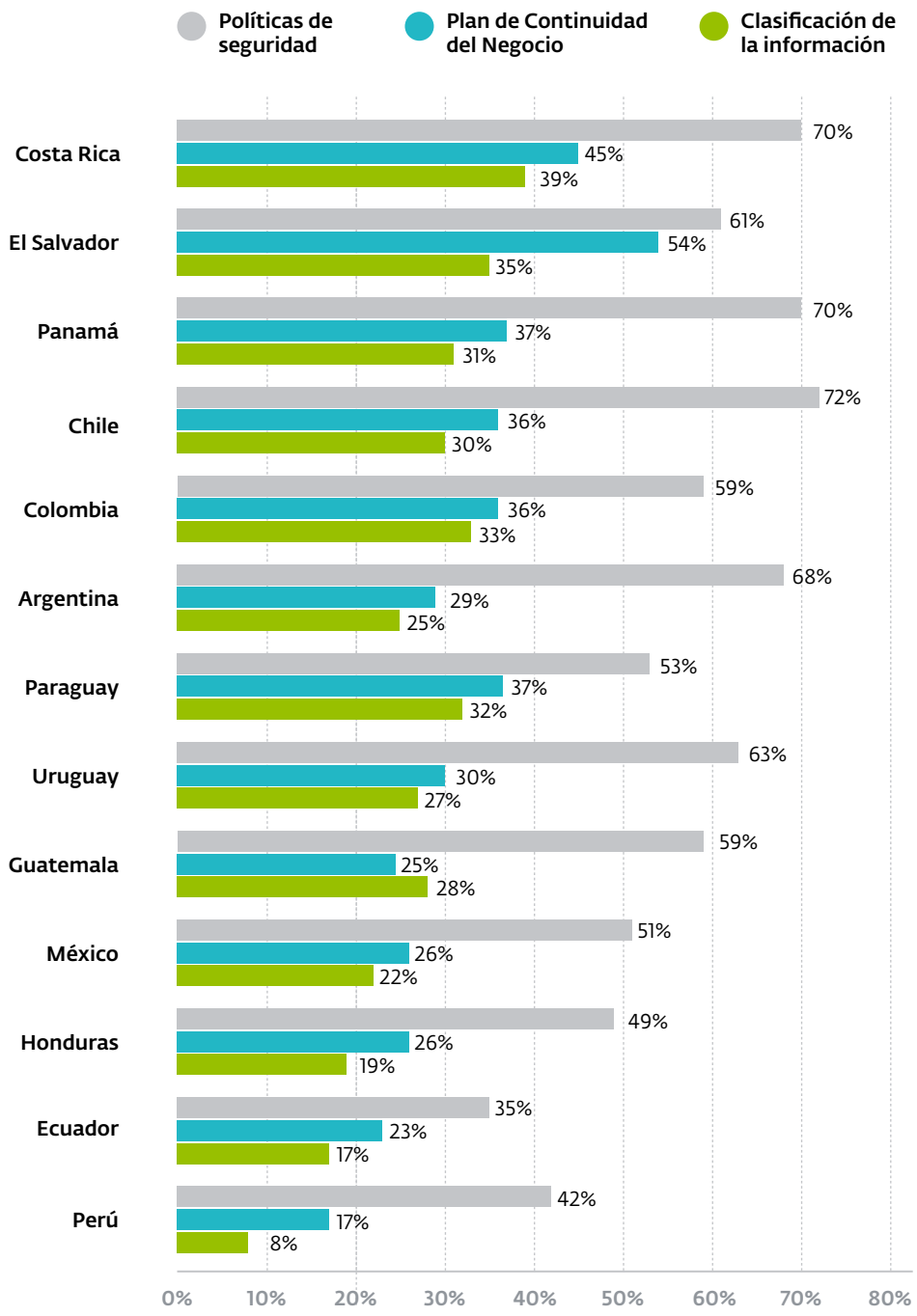
GRÁFICO 7 | Implementación de controles por Industria



Gestión

Como mencionamos, la tecnología no lo es todo en el campo de la seguridad de la información y es necesario complementarla con una adecuada gestión. Si bien la implementación de Políticas de seguridad es una de las prácticas más utilizadas en este campo, aún **los niveles de adopción no son los óptimos.** Esto se evidencia sobre todo en países como Ecuador (35%) y Perú (42%) en los que **menos de la mitad de las empresas encuestadas afirmaron contar con este tipo de gestiones.**

GRÁFICO 8 | Niveles de implementación de prácticas de gestión para la seguridad por país



Al analizar los datos relevados en la región, resulta preocupante ver que, **si tomamos a todas las empresas encuestadas, apenas una tercera parte cuenta con un Plan de continuidad del negocio.** Es crucial que las empresas sepan cómo responder en el caso de que ocurra un incidente que pueda poner en riesgo las operaciones de la compañía. Esto es clave no solo para tener una respuesta rápida y eficiente para la recuperación del incidente, sino también como medida de protección para identificar las fallas y evitar que incidentes de este tipo vuelvan a presentarse.

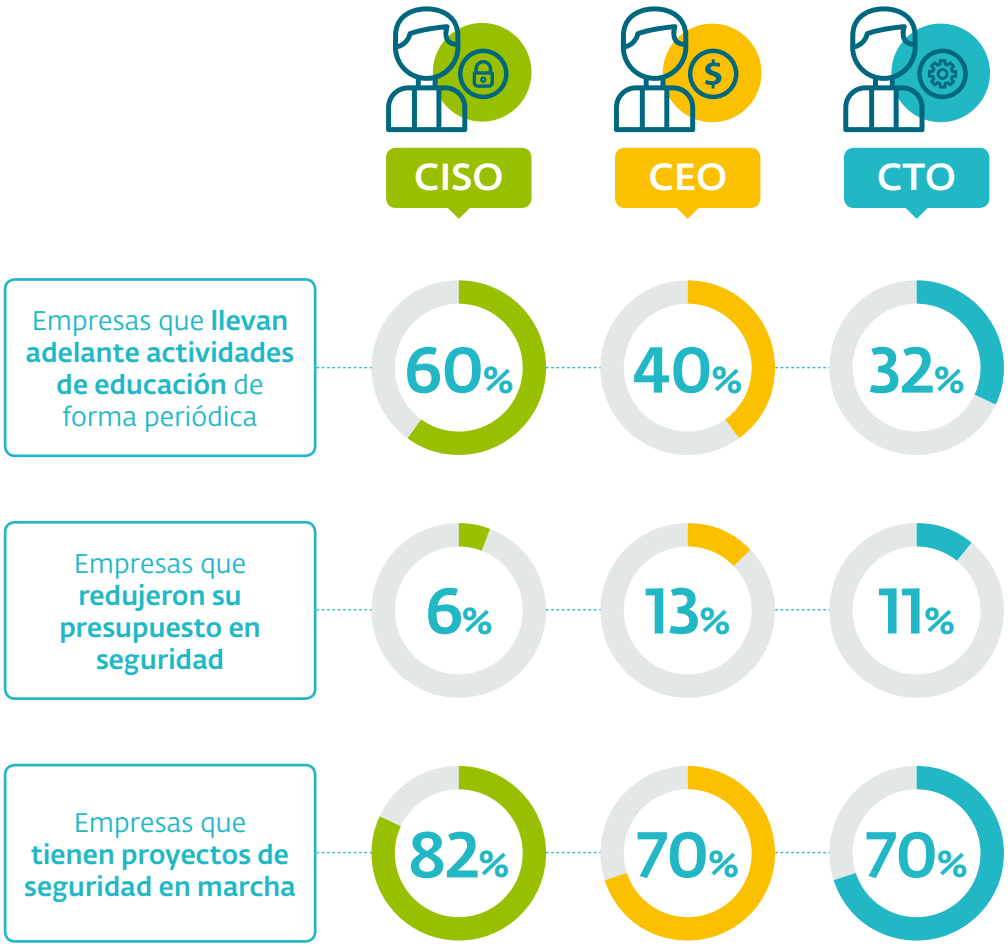
Apenas una tercera parte del total de empresas encuestadas cuenta con un Plan de continuidad del negocio.

04

La visión del C-Level

Ante este panorama de incidentes y preocupaciones, resulta interesante entender cómo están organizadas las empresas para afrontar los retos relacionados con la gestión de la seguridad de la información. En este sentido, además de los controles de seguridad implementados, entran en juego nuevas dimensiones que amplían el alcance de la gestión.

Entre las encuestas respondidas para el C-Level, obtuvimos información respecto de las **actividades de educación que llevan a cabo las organizaciones, las variaciones de presupuesto y el desarrollo de proyectos de seguridad.**



Como podemos ver, **aquellas empresas que cuentan con un CISO a cargo de las actividades de seguridad parecen tener un escenario más apto para el desarrollo de una estrategia de seguridad integral,** independientemente del uso de tecnologías de seguridad. Por ejemplo, la **implementación de actividades periódicas de educación en aquellas empresas donde hay un CISO (60%), es mayor que en aquellas donde no existe esta figura.**

El presupuesto para desarrollar este tipo de actividades resulta un factor fundamental, y si bien el porcentaje de empresas que redujeron su presupuesto de seguridad es menor al 15%, son aún menos las organizaciones en las que, habiendo un CISO, se registró esta disminución.

Educación

Sin lugar a dudas, la figura de un responsable de seguridad genera un movimiento positivo de las actividades y los proyectos relacionados con la seguridad dentro de la empresa. ¿Pero qué impacto tiene la realización de estas actividades?

El porcentaje de empresas que lleva a cabo actividades de educación de forma periódica y sufrió incidentes de seguridad, es menor que el de aquellas en las que no se realizan este tipo de actividades. Por ejemplo, el **18% de las empresas que llevaron adelante actividades de educación registró incidentes de ingeniería social, pero ese porcentaje aumentó al 40% en aquellas que no implementan actividades educativas.** Este mismo comportamiento se observa al analizar otros incidentes, como la infección con códigos maliciosos y los accesos indebidos a información sensible.

40%
De las empresas en las que NO se implementan actividades educativas sufrió incidentes de ingeniería social.

Y si bien no hay forma de medir directamente la incidencia de este tipo de actividades, podemos ver el **rol fundamental que juega aquí la educación de los usuarios,** como factor diferencial para garantizar la seguridad de la información. Dado que la gestión de la seguridad es un proceso integral, no podemos limitar nuestro análisis únicamente a la tecnología y a los controles que se implementen.

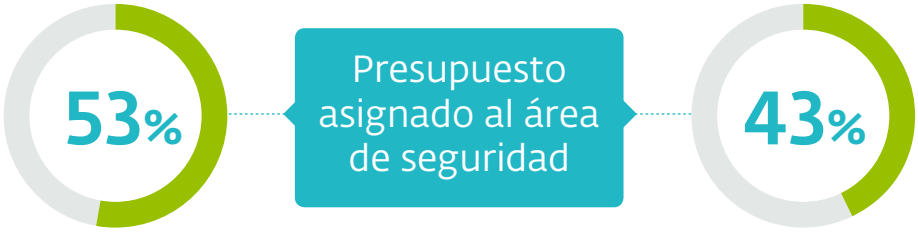
Inversión

Quizá una de las quejas más recurrentes en muchas empresas sea la falta de presupuesto destinado al área de seguridad; de hecho, en los últimos años se ha mantenido en **64% la proporción de empresas que considera que el presupuesto destinado a seguridad es insuficiente.**

64%
De las empresas considera que el presupuesto destinado a seguridad es insuficiente.

A su vez, el presupuesto asignado a los proyectos de seguridad cambia de acuerdo al tamaño de la empresa. Al menos un **43% de las empresas Enterprise aumentó el presupuesto** destinado al área de seguridad en relación a 2017, mientras que, en el **53% de las pequeñas y medianas empresas el presupuesto sufrió una reducción** con respecto al año anterior.

Estas cifras reflejan la necesidad de que las empresas busquen alternativas para desarrollar sus proyectos de seguridad. Si bien en lo que respecta a los encargados de seguridad parece haber mejorías, quizás se necesite una mayor inversión de tiempo y recursos para lograr los resultados más óptimos.



Pequeñas y medianas empresas **redujeron su presupuesto**

Empresas enterprise **aumentaron su presupuesto**

Conclusión

Uno de los principales datos que podemos recoger de esta edición del ESET Security Report es que **2 de cada 3 empresas sufrieron un incidente de seguridad durante 2018,** y el **40% sufrió una infección con códigos maliciosos,** siendo el incidente más recurrente. Más allá de esto, se evidencia una **caída en las infecciones de ransomware.** Esto podría significar que los cibercriminales no están aprovechando tanto esta herramienta o bien que las empresas se han sabido preparar mejor frente a esta amenaza dada su prevalencia en los últimos años, aunque **solo la mitad de las empresas encuestadas cuenta con 3 de los controles más básicos, antivirus, firewall y backup.** De todos modos, el impacto del ransomware continúa siendo alto para las empresas en caso de ocurrir una infección y no debe minimizarse a pesar de estar observando una menor cantidad de nuevas variantes para este tipo de código malicioso

En cuanto a las mayores preocupaciones, podemos observar que giran en torno a los principios de seguridad de la información, con el **acceso indebido (61%), el robo de información (58%) y la privacidad (48%)** obteniendo altas cifras y ubicándose en lo más alto del ranking. Esto se combina con la preocupación por los **códigos maliciosos (57%),** que son las principales herramientas de los cibercriminales para poder hacerse de la información de las empresas. En este sentido, es muy importante que las organizaciones tomen con la importancia necesaria la **capacitación de sus recursos humanos y la gestión de las herramientas de seguridad** para evitar dos de las **vías de propagación más populares: la Ingeniería Social y la explotación de vulnerabilidades.**

2 de cada 3
Empresas tuvo un incidente de seguridad durante 2018

40%
Sufrió una infección con códigos maliciosos

En cuanto a los controles, continuamos viendo una **baja implementación de soluciones de seguridad** por fuera de los 3 anteriormente mencionados. Tan solo la implementación de parches y actualizaciones de software supera la mitad de las empresas (51%), mientras que las **herramientas de detecciones de intrusiones apenas alcanzan a un tercio (29%) de las empresas,** a pesar de que la principal preocupación ha sido el acceso indebido. Controles útiles y relevantes para la época en la que vivimos, en la que los ataques se complejizan y la información se vuelve cada vez más vital, como las soluciones de doble factor de autenticación, el cifrado de información y las soluciones de seguridad para dispositivos móviles **no alcanzan ni el 20% de adopción.**

Algo similar ocurre con la gestión ya que, en promedio, la mayoría cuenta con una Política de seguridad en la empresa, pero **son bastante menores los casos que tienen un Plan de continuidad del negocio en caso de sufrir un incidente de seguridad.** Aún peor es la implementación de la Clasificación de la información, que es clave a la hora de implementar una política de backup en una organización.

En definitiva, seguimos observando algunas falencias en las empresas a la hora de resguardar y proteger su información. La falta de información y la baja adopción de algunas tecnologías de sencilla implementación son algunos de los puntos más preocupantes del panorama actual de las empresas. Y en la medida que el ecosistema de amenazas continúe evolucionando y complejizándose, las falencias de hoy serán aún más graves el día de mañana.

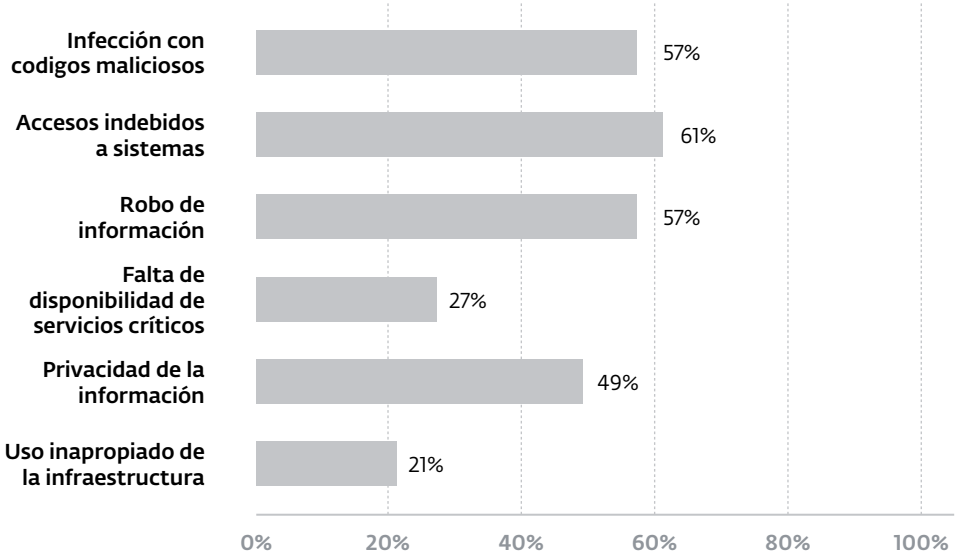
Baja implementación de soluciones de seguridad

Implementa parches y actualizaciones de software

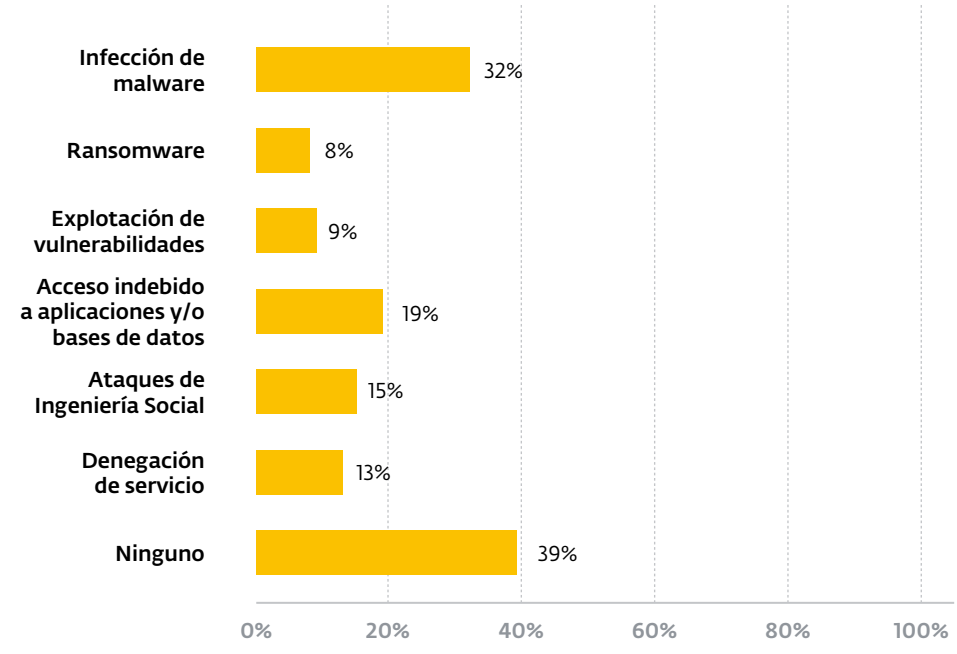
Emplea herramientas de detecciones de intrusiones

ANEXO
Datos estadísticos

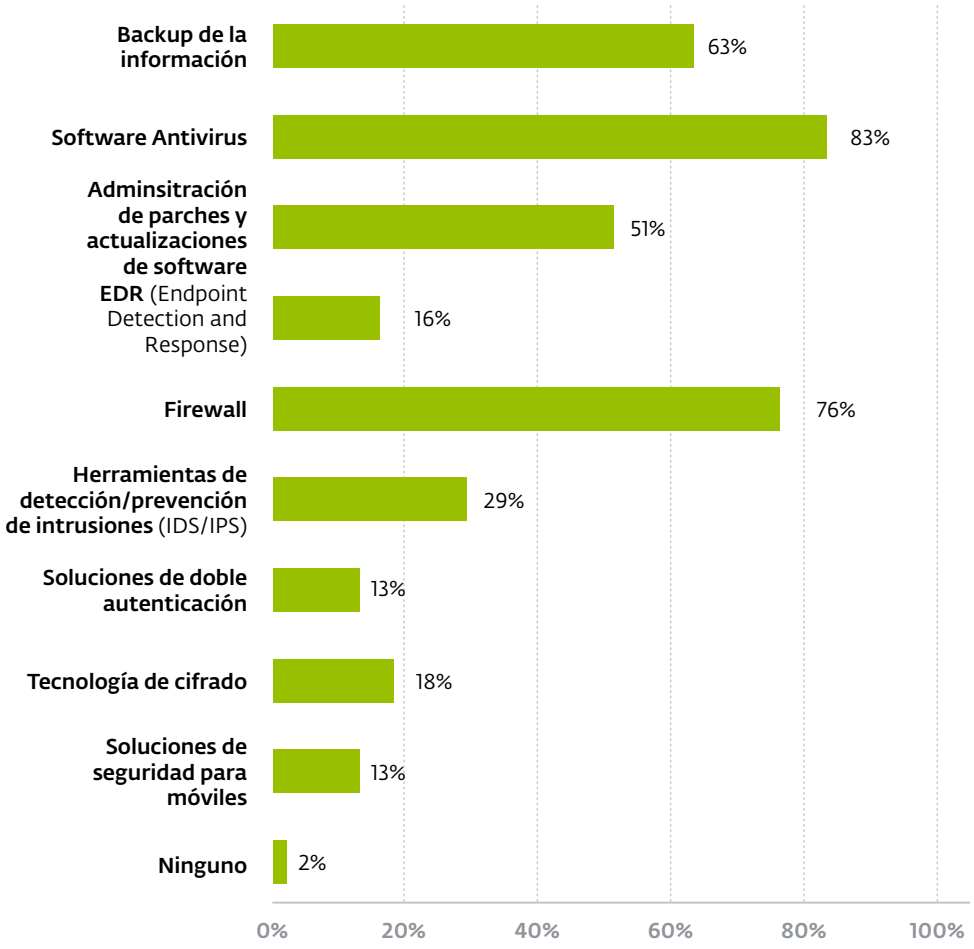
PREOCUPACIONES



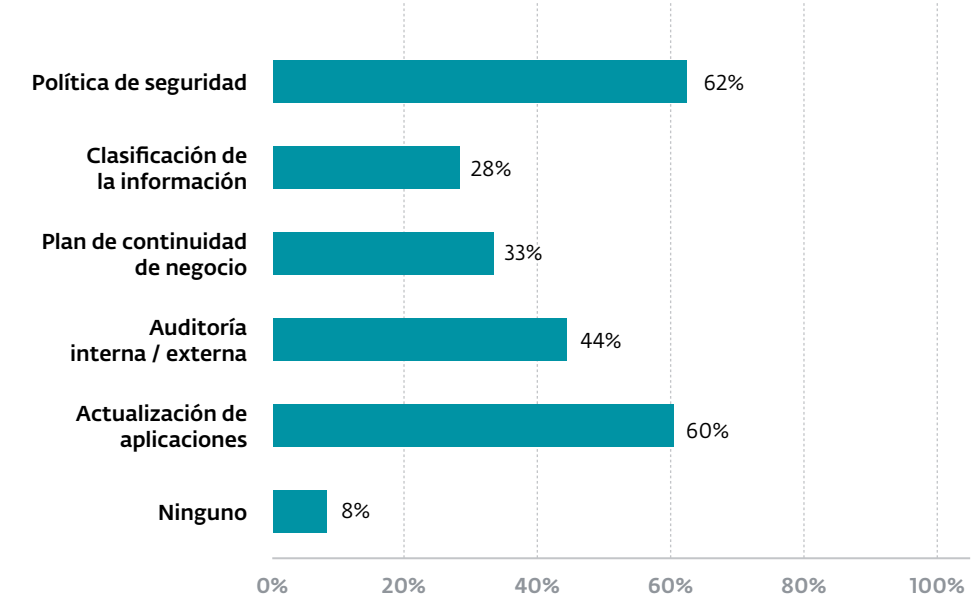
INCIDENTES



CONTROLES



GESTIÓN



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

CYBERSECURITY
EXPERTS ON YOUR SIDE