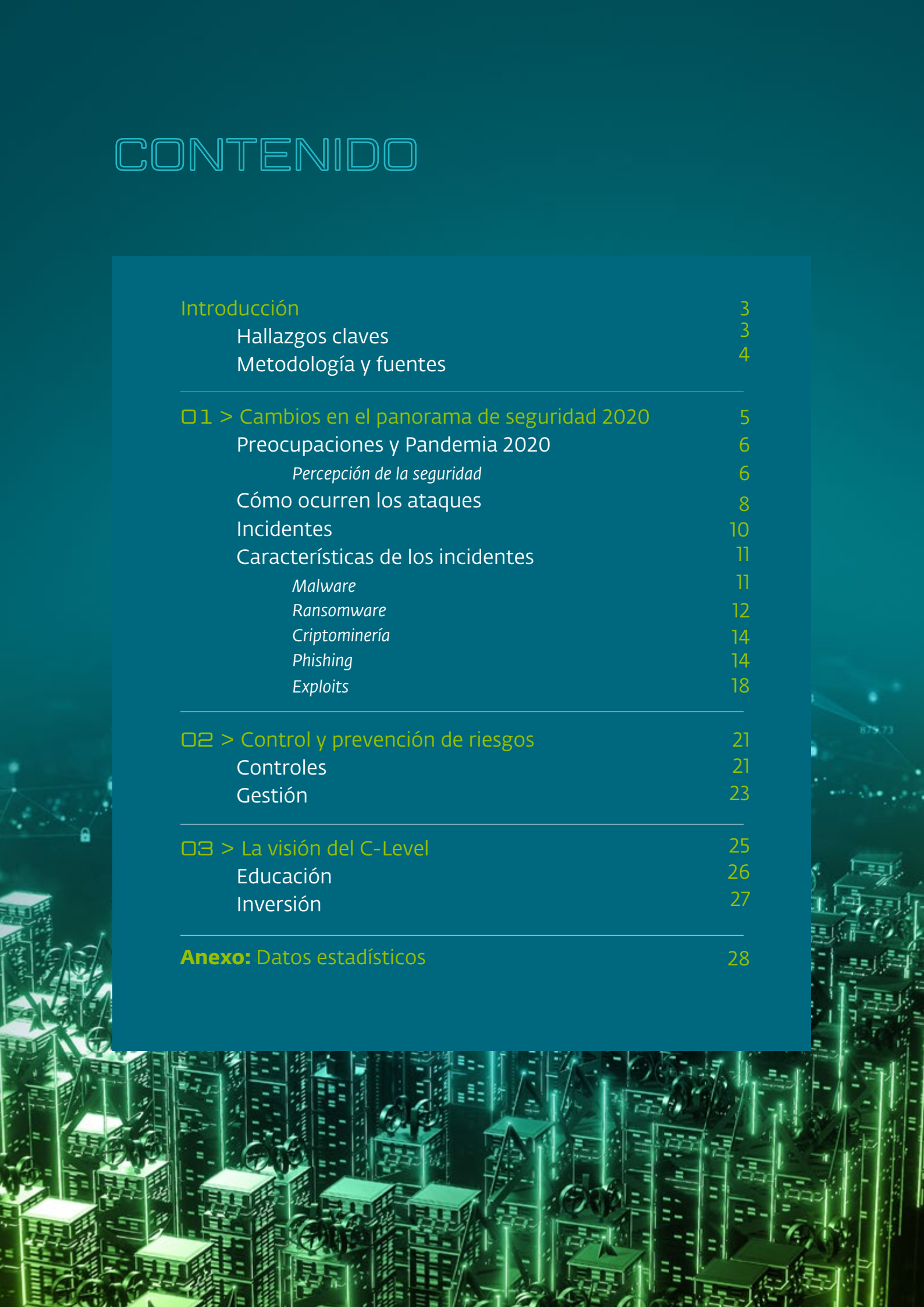
SECURITY REPORT

LATINOAMÉRICA 2020

CONTENIDO



Introducción

Conocer el estado de la información en las empresas de la región nos permite tener un panorama más claro para entender qué están haciendo las empresas en materia de seguridad informática, cuáles son sus preocupaciones y cómo actúan para proteger sus infraestructuras. Es por eso que, desde hace varios años, recolectamos información de toda la región a través de los distintos eventos de seguridad en los que participamos y reunimos las respuestas de casi 4000 empresas de distinta envergadura para elaborar este documento que pretende reflejar en un sentido amplio la situación en la región.

Dedicaremos la primera parte del informe a comprender las preocupaciones que tienen las empresas en materia de seguridad. Observaremos luego los tipos de incidentes más recurrentes y reconocidos por las propias empresas para poder evaluar qué controles se implementan a la hora de proteger las redes corporativas. Por último, analizaremos cómo estos datos se relacionan con las preocupaciones que los profesionales de tecnología dicen tener en torno a la seguridad de sus activos informáticos.

Confiamos en que este análisis refleja el estado de la seguridad de la información en las empresas de Latinoamérica y esperamos que la lectura de este informe sea de utilidad para que los responsables de seguridad de las empresas puedan hacer sus propias comparaciones y revisar sus prácticas.

> Hallazgos claves

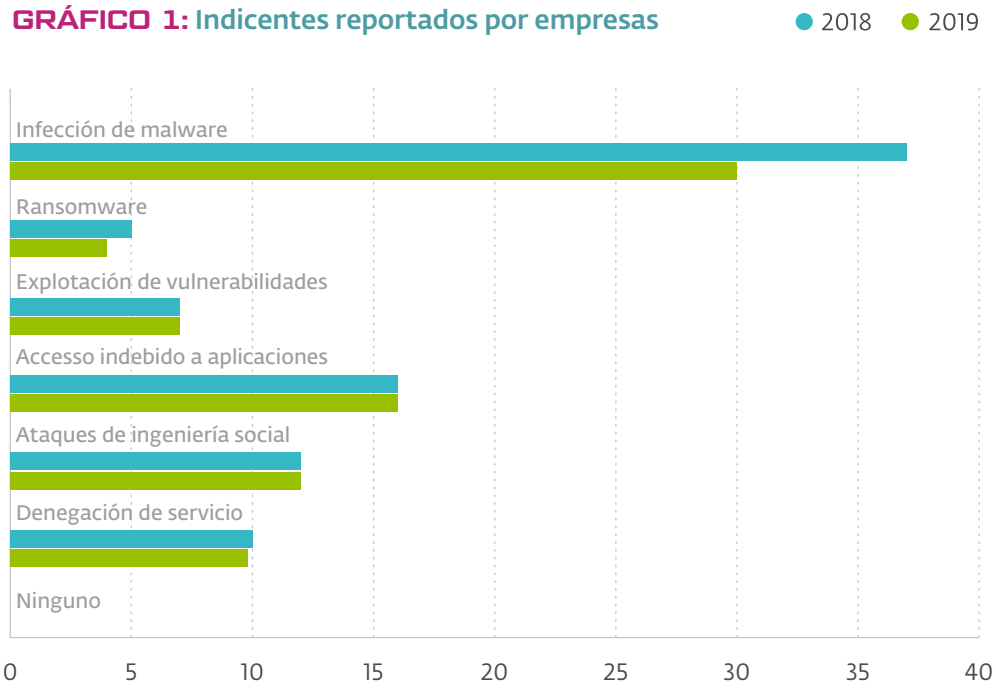
Resulta interesante ver cómo las empresas de la región mantienen, en líneas generales, los mismos niveles de incidencia de seguridad que el año anterior en lo que respecta a Ransomware, ya que, si bien sigue siendo de las amenazas más mediáticas, sufrió una pequeña caída del 2%. El 2019 dejó en evidencia una disminución de los ataques masivos y una transición hacia ataques dirigidos a empresas, cuyo objetivo es, en principio, amplificar la posibilidad de éxito en el cobro de rescates económicos. Por su parte, al comparar períodos, las infecciones de códigos maliciosos sí reflejaron una pronunciada caída del 8%.

2019 DEJÓ EN EVIDENCIA UNA DISMINUCIÓN DE LOS ATAQUES MASIVOS Y UNA TRANSICIÓN HACIA ATAQUES DIRIGIDOS A EMPRESAS.

A lo largo del informe veremos cuáles son las principales características de estos

cambios y cómo influyen en la gestión de la seguridad de las empresas. Por otro lado, resulta interesante el hecho de que únicamente el 33% de las empresas que participaron en el *ESET Security Report 2020* contara con un plan de continuidad del negocio. Si bien es poco probable que una organización tuviera un plan de respuesta ante una pandemia, la transición hacia modos de operación diferentes, como los que debieron adoptarse a poco de finalizar el primer trimestre del año, resultará siempre más sencilla de llevar adelante para aquellas empresas que cuenten con planes de continuidad operativos y probados.

GRÁFICO 1: Indicentes reportados por empresas



> Metodología y fuentes

Los datos fueron recolectados de encuestas realizadas a lo largo del año en diferentes eventos de seguridad de los que participan representantes de diversas industrias de la región. Este nuevo reporte basa su análisis en las respuestas de más de 3900 profesionales de la seguridad de organizaciones alrededor de Latinoamérica.

Además, el reporte se compone de datos suministrados por empresas de diferentes tamaños: este año, un 30% lo conforman empresas de más de 1000 empleados; un 11% empresas grandes de por lo menos 500 empleados; y un 57% lo integran PyMEs, entre las que se incluyen más de diez tipos de industrias. Además, cabe destacar que una cuarta parte del informe corresponde a información aportada por ejecutivos C-Level, pudiéndose segmentar a este último grupo en CISO (21%), CTO (40%) y CEO (37%).

El informe recopila información de empresas ubicadas en 14 países diferentes de la región, incluyendo Argentina, Brasil, México, Colombia, Chile y Guatemala.

01

Cambios en el panorama de seguridad 2020

Durante 2019 se hizo evidente el aumento en la adopción de tecnologías prometedoras en un contexto en el que los artículos cotidianos se vuelven cada vez más inteligentes y conectados. En este sentido, las empresas están incorporando estas tecnologías a los edificios para aumentar su eficiencia operativa y ahorrar grandes sumas de dinero. Las ciudades incluso compiten por implementar soluciones inteligentes que les permitan lucir con orgullo las credenciales de ciudad inteligente. Sin embargo, esto plantea nuevos desafíos al momento de mitigar ataques y evitar responsabilidades mayores en cuanto al manejo de los datos personales (de empleados, ciudadanos, etc.). Si bien la idea de revolución digital en las empresas se ha planteado e instalado hace años, entre los principales desafíos que enfrentan hoy las corporaciones para seguir la línea de la Transformación Digital destaca el de considerar a la ciberseguridad como aspecto integral de cada uno de sus procesos. De no hacerlo, será cada vez más común ver problemas asociados a bases de datos mal configuradas (por ejemplo, filtraciones de información masivas por una mala configuración de servidores), y que la adopción de nuevas tecnologías que buscan brindar mayor seguridad genere más problemas que soluciones (cámaras, controles de acceso biométricos, entre otros).

El aprendizaje automático, también conocido como Machine Learning (ML), gana cada vez más terreno, y gracias a esta tecnología muchas de las tareas se han simplificado. Desde el análisis de grandes cantidades de datos hasta la evasión de tareas repetitivas con las que lidiar, el aprendizaje automático permite a los sistemas mejorar la forma en que abordan los problemas. Sin embargo, tal como mencionamos en nuestro reporte Tendencias 2020, en 2019 el ML ganó notoriedad debido a otro asunto preocupante: el aumento de las deepfakes. Esta tecnología, que hace que el dicho popular "ver para creer" pierda todo sentido, podría ser aprovechada para dañar la reputación de figuras públicas o incluso influir en la opinión pública. Tal es así que en 2019 se reportó un caso de un engaño en el que los atacantes utilizaron un software basado en Inteligencia Artificial para imitar la voz del CEO de una compañía y convencer a la víctima para que realice una transferencia monetaria a cuentas bancarias de los estafadores.

La tecnología ML ha sido también aplicada en un contexto menos siniestro, como es el caso de FaceApp, la app que permite envejecer y rejuvenecer rostros. Sin

embargo, la aplicación mostró problemas vinculados a la privacidad de los datos de los usuarios y generó preocupación; sobre todo de cara a futuras implementaciones que hagan uso de esta tecnología de una forma similar, como podría ser, por ejemplo, la tecnología de reconocimiento facial como mecanismo de autenticación.

> Preocupaciones en materia de seguridad

Percepción de la seguridad a comienzos de año

El panorama de incidentes y amenazas que hemos introducido trae como consecuencia la preocupación de las empresas por la seguridad de su información. Si tuviéramos que conformar un orden, un 60% de las organizaciones encuestadas afirma que su principal preocupación es el **acceso indebido a la información**. El podio lo completan el **robo de información** (55%) y la **infección con códigos maliciosos** (53%). Aun así, y tal como analizaremos más adelante, sorprende la baja implementación de controles de identificación, como herramientas de múltiple factor de autenticación, para evitar accesos indebidos.

60% DE LAS ORGANIZACIONES ENCUESTADAS AFIRMA QUE SU PRINCIPAL PREOCUPACIÓN ES EL ACCESO INDEBIDO A LA INFORMACIÓN.

Era de esperarse que estas fueran las principales preocupaciones para las empresas, ya que, si nos remitimos a lo ocurrido durante 2019, los casos de fuga de información se convirtieron en noticia recurrente. De hecho, aun habiendo entrado en efecto el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) dentro de la Unión Europea, cuyo alcance es global, el pasado año se registraron casos de fugas de información y de datos personales cada vez más grandes con el pasar de los meses. Se trata de un problema que no solo afecta a empresas privadas, sino también a entes gubernamentales; tal es el caso del Gobierno de Ecuador, que en septiembre de 2019 comenzó a investigar la posible filtración de millones de datos de sus ciudadanos. Asimismo, pueden mencionarse los errores de configuración de base de datos que expusieron información de más de dos millones de habitantes en Colombia y que contenían datos sensibles que aluden a relaciones personales, situación financiera, salarios e incluso puestos de trabajo.

No está de más destacar que, por fuera de las preocupaciones mencionadas, la privacidad de la información (46%) se acerca al último puesto del podio como preocupación central para las empresas de la región.

En lo que respecta a ese tercer puesto, la infección con códigos maliciosos acarrea consigo lo problemático de este tipo de amenazas: la gran mayoría de los ataques que pueden comprometer la seguridad de una empresa suele estar asociada a alguna variante de malware. La amplia variedad de acciones maliciosas que este tipo de amenazas puede realizar, desde botnets a ransomware, es igualmente

aprovechada en un amplio espectro de plataformas: desde computadoras hasta dispositivos móviles sin dejar afuera los dispositivos IoT, lo que hace que la infección mediante malware sea uno de los métodos más usados por los atacantes.

Ya hemos visto cómo los cibercriminales utilizan técnicas variadas para propagar sus amenazas. A modo de ejemplo, apenas comenzaba 2019 se hizo pública una vulnerabilidad en WinRAR, y pocos días después comenzaron a surgir exploits y campañas maliciosas que buscaban aprovechar la vulnerabilidad para propagar determinadas familias de ransomware. Lo mismo ocurrió con la vulnerabilidad de WhatsApp revelada a mediados de año que permitía el acceso al dispositivo con una simple llamada a través de esa plataforma, poniendo en riesgo, una vez más, datos sensibles y personales de las víctimas y/o las empresas para las que trabajaban.

Nuevos retos para la seguridad

Pero este panorama de la seguridad se vio alterado por la situación extraordinaria que han debido enfrentar las empresas como consecuencia del COVID-19, y lo que ello ha implicado al momento de garantizar la continuidad de las operaciones. Según datos relevados a partir de encuestas realizadas durante los últimos meses en la región, casi el 45% de los usuarios recibió intentos de Phishing relacionados a la pandemia, y más del 50% aseguró que la organización para la que trabajan no brindó las herramientas de seguridad necesarias para migrar hacia el teletrabajo en estas condiciones.

CASI EL **45%** DE LOS USUARIOS RECIBIÓ INTENTOS DE PHISHING RELACIONADOS A LA PANDEMIA, Y MÁS DEL **50%** ASEGURÓ QUE LA ORGANIZACIÓN PARA LA QUE TRABAJAN NO BRINDÓ LAS HERRAMIENTAS DE SEGURIDAD NECESARIAS PARA MIGRAR HACIA EL TELETRABAJO.

El nuevo escenario que trajo la pandemia sumó retos y preocupaciones a las empresas, dado que el perímetro a proteger se ha extendido considerablemente. A continuación, presentamos algunos de los desafíos que aceleró este fenómeno sanitario.

Aceleración de los procesos de transformación digital

Es evidente que el proceso de transformación digital para muchas empresas había comenzado hace ya algunos años, pero la pandemia expuso la necesidad de contar con medios alternativos para poder realizar las actividades cotidianas, como el teletrabajo.

En este sentido, si bien en el ámbito corporativo hay quienes ya habían adoptado estos mecanismos como una opción para realizar sus funciones, lo que ayudó a que el impacto de la crisis provocada por el COVID-19 fuera menor a la hora de continuar con sus operaciones, las organizaciones que ignoraron o postergaron la decisión de llevar adelante esta transición digital se vieron afectadas por la falta de disponibilidad, integridad o confidencialidad de su información.

La seguridad debe estar en todos lados, no tiene límites físicos

El distanciamiento social reafirmó una premisa de la que hemos hablado con anterioridad: la seguridad debe acompañarnos a cada lugar y en todo momento. Si bien las empresas invierten recursos de toda índole para proteger su información e infraestructura tecnológica, en ocasiones se piensa únicamente en un espacio físico (por ejemplo, una oficina).

Las nuevas condiciones de trabajo exponen la necesidad de contar con mecanismos de protección (entre ellos, soluciones de seguridad y la aplicación de buenas prácticas), en todos los puntos desde donde se procesen, almacenen o transmitan datos.

LAS NUEVAS CONDICIONES DE TRABAJO EXPONEN LA NECESIDAD DE CONTAR CON MECANISMOS DE PROTECCIÓN EN TODOS LOS PUNTOS DESDE DONDE SE PROCESEN, ALMACENEN O TRANSMITAN DATOS.

Se ponen a prueba los planes de contingencia

La pandemia también mostró la necesidad de implementar, revisar, probar, mejorar, y actualizar herramientas como las de Análisis de Impacto al Negocio (BIA); Evaluaciones de Riesgos; Planes de Continuidad del Negocio (BCP); o Planes de Recuperación (DRP). Al mismo tiempo, dejó en claro la importancia de considerar al personal, los lugares de trabajo, las tecnologías y los servicios críticos.

Aunque un escenario de esta naturaleza era muy difícil de predecir, su llegada hizo evidente el alto impacto para los negocios. De hecho, que nuevamente una tercera parte de las empresas que participaron del informe este año tuviera un plan de continuidad del negocio, refleja lo poco preparadas que en general siguen estando las organizaciones a la hora de responder ante incidentes que comprometan la operatividad del negocio.

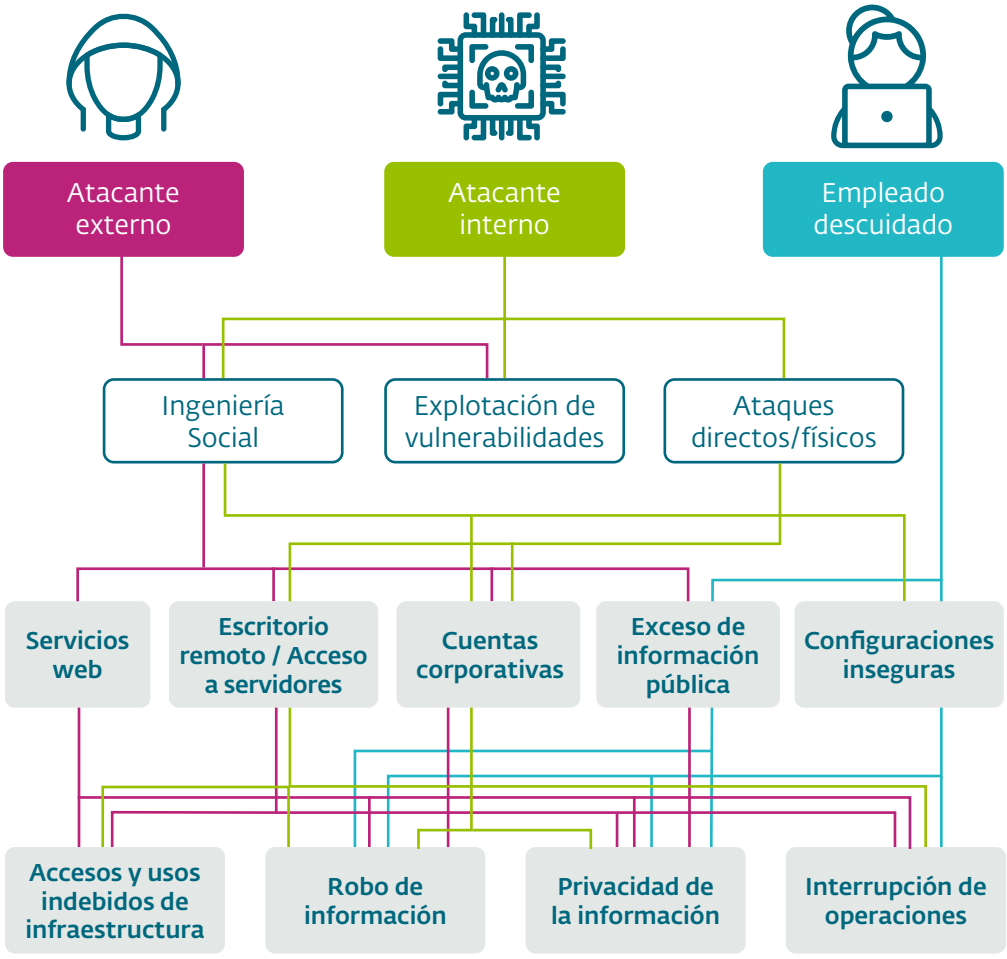
Por ello, el foco de las organizaciones está ahora puesto en contar con medidas y planes de respuesta que permitan garantizar la continuidad de los procesos comerciales.

Junto con estas condiciones, las preocupaciones de las empresas comienzan a mutar, y se dirigen también hacia la toma de medidas para garantizar mayores niveles de seguridad al momento de conectarse desde redes Wi-Fi hogareñas o al utilizar diferentes herramientas de comunicación. Esto conlleva retos, y las empresas deben ahora implementar nuevas dinámicas de capacitación y/o concientización para que sus colaboradores asuman la importancia de proteger los datos sensibles, tanto personales como corporativos.

> Cómo ocurren los ataques

Dada la amplia variedad de amenazas que puede afectar a las empresas, y habiendo conocido sus principales preocupaciones en materia de seguridad, es impor-

tante identificar cuáles son los diferentes vectores por los cuales puede llegar un ataque para luego tomar las medidas de control más adecuadas.
Desde el Laboratorio de Investigación de ESET elaboramos un diagrama con las vías más utilizadas en la ejecución de los ataques, según han identificado nuestras soluciones de seguridad en intentos dirigidos a nuestros clientes alrededor de Latinoamérica. Se ha tenido en consideración que, si bien muchas veces los ataques llegan desde fuera de la organización, es posible que ocurran dentro de la empresa, incluso por descuidos o malas prácticas de seguridad.



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. Una vez que logran el acceso, pueden llevar adelante distinto tipo de **acciones maliciosas**.

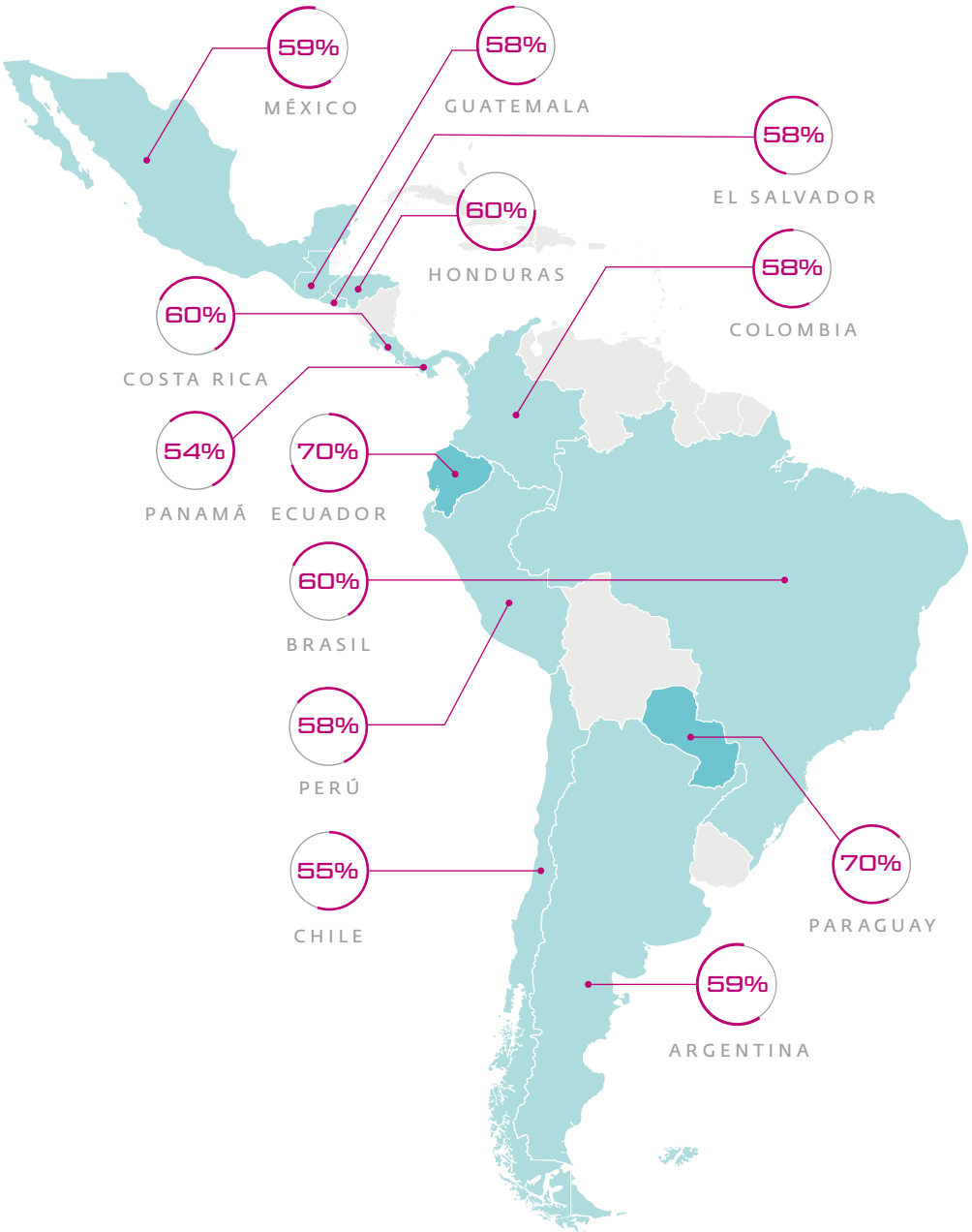
Independientemente del camino o del actor que esté detrás del incidente de seguridad, tanto la continuidad del negocio, como la reputación de la empresa, pueden verse afectadas.

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.

> Incidentes de seguridad

De las preocupaciones pasamos a los incidentes. Es importante para ello entender el nivel de los incidentes que se presentan, y es precisamente del análisis de los datos suministrados por organizaciones de toda Latinoamérica que podemos afirmar que un 60% de las empresas sufrió al menos un incidente de seguridad, número que se mantiene respecto del año anterior. La infección con códigos maliciosos también conserva su lugar, siendo el incidente más recurrente: 1 de cada 3 empresas sufrió una infección con algún código malicioso, incluyendo ransomware.

GRÁFICO 2: Empresas con incidentes de seguridad



EL **60%** DE LAS EMPRESAS SUFRIÓ AL MENOS UN INCIDENTE DE SEGURIDAD EN 2019.

Algo que surge de la revisión de la información recolectada es que dentro de los incidentes relacionados a la infección con códigos maliciosos (32%), solo el 18% está relacionado al ransomware, lo que indica una incidencia del 6% sobre el total de las empresas. Esto se traduce en una caída respecto del 2019, año en el que el ransomware había registrado una incidencia del 8%.

> Características de los incidentes

Más allá de conocer cuáles fueron los incidentes con mayor presencia en los diferentes países de la región, resulta también interesante conocer qué tipo de amenazas estuvo detrás de cada uno de ellos. Haremos un recorrido por las principales familias de malware visto en la región, detallando sus características, y elaborando un apartado especial para el ransomware y la criptominería; dos amenazas muy presentes en Latinoamérica junto con el phishing y los exploits.

Malware

Entre los códigos maliciosos detectados en la región, los más relevantes resultaron:

- </> Ramnit
- </> ProxyChanger
- </> Emotet
- </> Bondat
- </> Exploit.CVE-2012-0143.A

< Win32/Ramnit > Código malicioso utilizado principalmente para robar datos confidenciales relacionados a servicios bancarios de los usuarios. Se propaga a través de dispositivos extraíbles y una de sus principales características es la capacidad de infectar el Master Boot Record (MBR) para mantener su persistencia en el sistema operativo.

< JS/ProxyChanger > Se trata de un malware del tipo troyano escrito en JavaScript. Tiene como función impedir al usuario acceder a sitios web para redirigir el tráfico hacia sitios de atacantes.

< Win32/Emotet > Este código malicioso se ocupa principalmente de la distribución de otras familias de troyanos bancarios. Es conocido por su arquitectura modular, sus métodos de persistencia y su capacidad de autopropagación, así como por sus características polimórficas que intentan evadir la detección basada en firmas.

< JS/Bondat > Gusano informático escrito en JavaScript que tiene como función

principal infectar sistemas Windows para unirlos a una botnet. Funciona como un vector de infección inicial, ya que también descarga nuevos archivos capaces de realizar otras acciones maliciosas. Su vía de propagación son los medios extraíbles, utilizando archivos LNK.

< Exploit.CVE-2012-0143 > Es una vulnerabilidad que data del 2012 y que permite un atacante externo ejecutar código de manera arbitraria a partir de un error en el manejo de la memoria de Microsoft Excel 2003 SP3 y Office 2008 para Mac.

Merecen una mención especial los troyanos bancarios. Estos códigos maliciosos que se utilizan para robar información financiera de los usuarios tienen un accionar muy alto en Latinoamérica, donde existen familias de troyanos específicos que presentan características comunes entre sí. En este sentido, la mayoría de los troyanos bancarios presentes en América Latina que se analizaron durante 2019, y que venimos siguiendo en 2020, convierten al dispositivo de la víctima en un equipo zombie, de manera tal que se conectan al servidor de C&C y permanecen allí a la espera de recibir cualquier comando que envíe el servidor. Una vez que reciben un comando, lo ejecutan y esperan la llegada de uno nuevo. Algunas familias representativas de este tipo de amenazas presentes en la región son Amavaldo, Casbaneiro, Mispadu, Guildma o Grandoreiro.

Ransomware

En términos generales, el número de casos de ransomware muestra una tendencia decreciente por tercer año consecutivo. En 2017, la cantidad de empresas afectadas por esta variante de malware fue del 18%, mientras que en 2018 el porcentaje cayó al 8% y en 2019 registró apenas un 6%.

De hecho, un análisis de las detecciones de códigos maliciosos del tipo ransomware de los productos de ESET en países de Latinoamérica da cuenta de esta disminución. Sin lugar a dudas, la novedad del ransomware como amenaza predilecta para los cibercriminales ha disminuido en importancia, pero no así su uso en ataques más dirigidos. Es común encontrarnos con amenazas que generan la interrupción de las operaciones de negocio, exponen información sensible y exigen pagos de rescate mayores. Por este motivo, dado el alto impacto que puede tener en la operación de la empresa, el ransomware no debe desestimarse al momento de realizar los análisis de riesgo de la empresa y tomar medidas de control, tanto preventivas como correctivas. En los últimos meses hemos sido testigos de casos importantes como el ataque a la petrolera PEMEX en México. No solo se trató de un ataque de secuestro de información, sino que mutó luego a una extorsión de filtrado de información sensible, en caso de no pagarse el rescate.

En 2017 la actividad de esta amenaza marcó un máximo histórico, cuando tanto la cantidad 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. Sin embargo, si se analiza la cantidad de detecciones de este tipo de amenazas en la región a lo largo de 2019, puede verse una tendencia a la baja durante el 90% del periodo.

GRÁFICO 3: Detecciones mensuales en LATAM

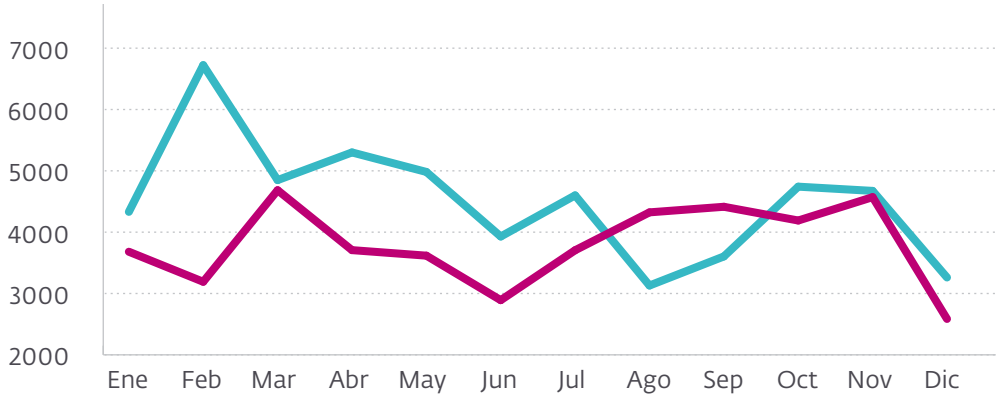
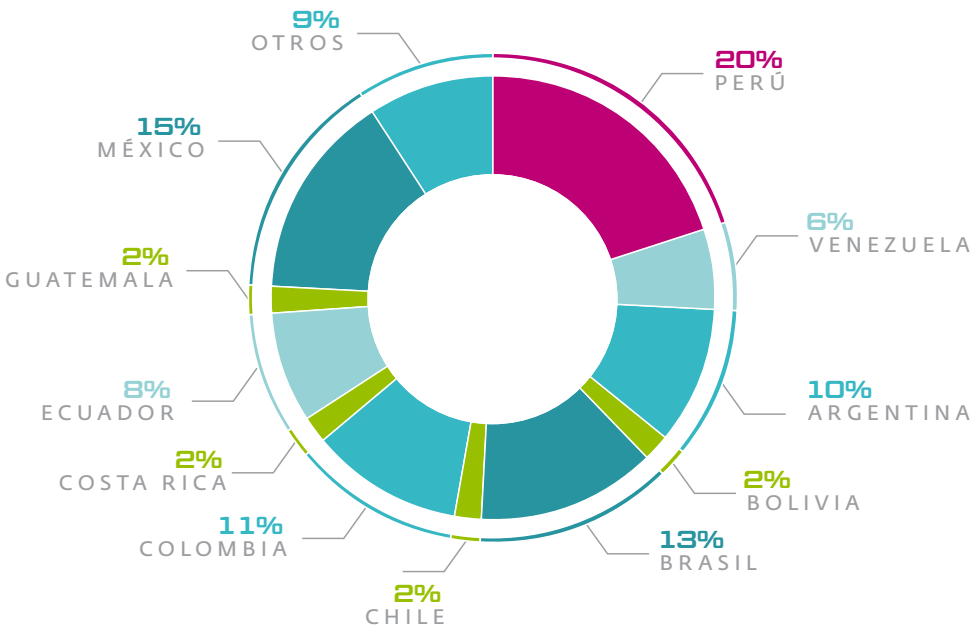


GRÁFICO 4: Detecciones de Ranswomware por país

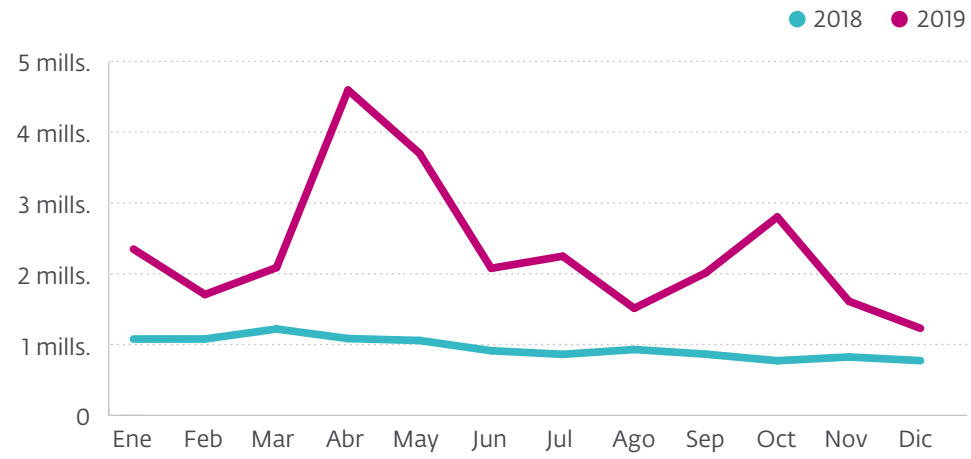


Criptominería

Otra variante de código malicioso cuya evolución vale la pena mencionar corresponde a los mineros de criptomonedas. Si bien el mercado de la criptominería sigue en crecimiento, y las estadísticas muestran que una parte es realizada a partir de ataques de criptojacking que utilizan los recursos de las víctimas en favor de los cibercriminales, durante 2019 se registró un descenso en su actividad en comparación con 2018. Esto indica que, al igual que con el Ransomware, si bien el registro de ataques disminuyó, es su modo de ejecución lo que ha sido modificado. Es decir, se trata de acciones dirigidas que buscan atacar infraestructuras más preparadas para la tarea, dado que, al tener posiblemente servidores con mayor capacidad de procesamiento, funcionamiento continuo y mayor ancho de banda, entre otras características, se convierten en un blanco más atractivo para minar criptomonedas. Esto se debe a que se necesitará entonces una menor cantidad de equipos infectados para tener una capacidad de procesamiento atractiva para el minado, especialmente si se la compara con el alto número de dispositivos necesario para afectar a usuarios domésticos.

SI BIEN EL REGISTRO DE ATAQUES DE CRIPTOMINERÍA DISMINUYÓ, ES SU MODO DE EJECUCIÓN LO QUE HA SIDO MODIFICADO.

GRÁFICO 5: Detecciones de Mineros a lo largo del año



Dejando de lado los códigos maliciosos, un 18% de las empresas aseguró haber sufrido accesos indebidos a la información, mientras que un 15% dijo haber sido víctima de técnicas de ingeniería social, siendo este el incidente con mayor crecimiento de los últimos meses.

LA INGENIERÍA SOCIAL FUE EL INCIDENTE CON MAYOR CRECIMIENTO EN LOS ÚLTIMOS MESES DE 2019.

Phishing

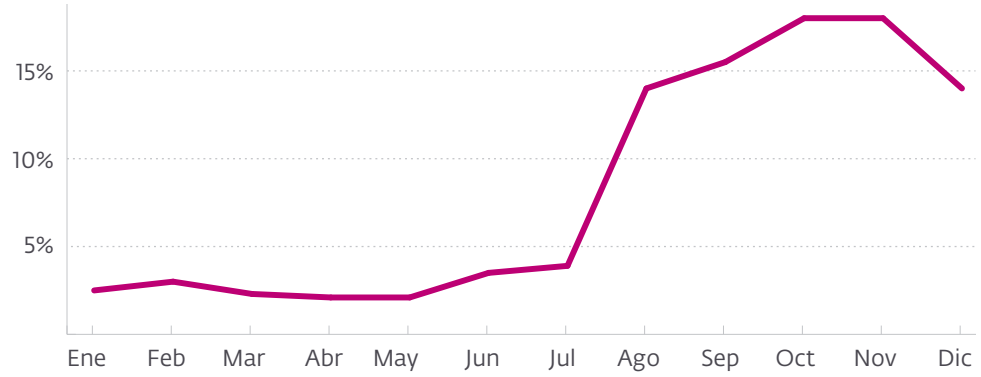
Es posible que el incremento en el número de incidentes asociados a la ingeniería social esté ligado a la amplia variedad de campañas que vimos durante 2018. Diversas marcas reconocidas fueron utilizadas como anzuelo y nuevos vectores de ataque se sumaron a la lista. El correo electrónico dejó de ser la única vía para lanzar mensajes de phishing, y otras herramientas de mensajería como WhatsApp

y los SMS han sido muy utilizadas para estos fines. Una vez más, resulta llamativa la poca protección en dispositivos móviles que utilizan las empresas, dado que apenas un 12% aseguró implementar soluciones de seguridad para dispositivos móviles. Aún más preocupante resulta esto si se tiene en cuenta que a través de los dispositivos móviles se manipula y se comparte cada vez más información sensible del negocio.

Es importante entender que, si bien muchos ataques de ingeniería social solo buscan robar credenciales de usuarios finales (de servicios de streaming, correo electrónico, redes sociales, entre otros), no es extraño que dichos usuarios utilicen las mismas contraseñas en sus cuentas personales y en entornos corporativos. Por otro lado, es preciso mencionar la existencia de ataques que traen asociados troyanos bancarios, como Emotet, o amenazas de tipo Spyware que conservan su persistencia en los dispositivos afectados esperando la llegada de nueva información útil para sus propósitos.

En lo que respecta a detecciones de phishing, es evidente un notable aumento durante la segunda mitad de 2019, particularmente al ver los picos registrados en el último trimestre.

GRÁFICO 6: Detecciones de Phishing durante el 2019



A lo largo de 2019 también fuimos testigos de grandes fugas de información a nivel global. Más allá de los casos anteriormente mencionados en Ecuador y Colombia, vale la pena destacar otras importantes filtraciones; entre ellas: el caso de la mundialmente conocida plataforma de diseño Canva, que sufrió un incidente de seguridad en el que los atacantes robaron datos privados de 139 millones de usuarios; o el caso de la banco estadounidense Capital One, que fue víctima de una de las fugas de información financiera más grandes de la historia con más de 100 millones de usuarios afectados. Es importante tener en cuenta que al hacerse públicos todos estos datos, se vuelve más sencillo para los atacantes crear campañas de phishing más dirigidas y efectivas al aprovechar esta información. A modo de ejemplo, vemos a continuación uno de los correos más recurrentes y frecuentemente utilizados, que suplantan la identidad de servicios o marcas reconocidas.

Suplantación de Netflix

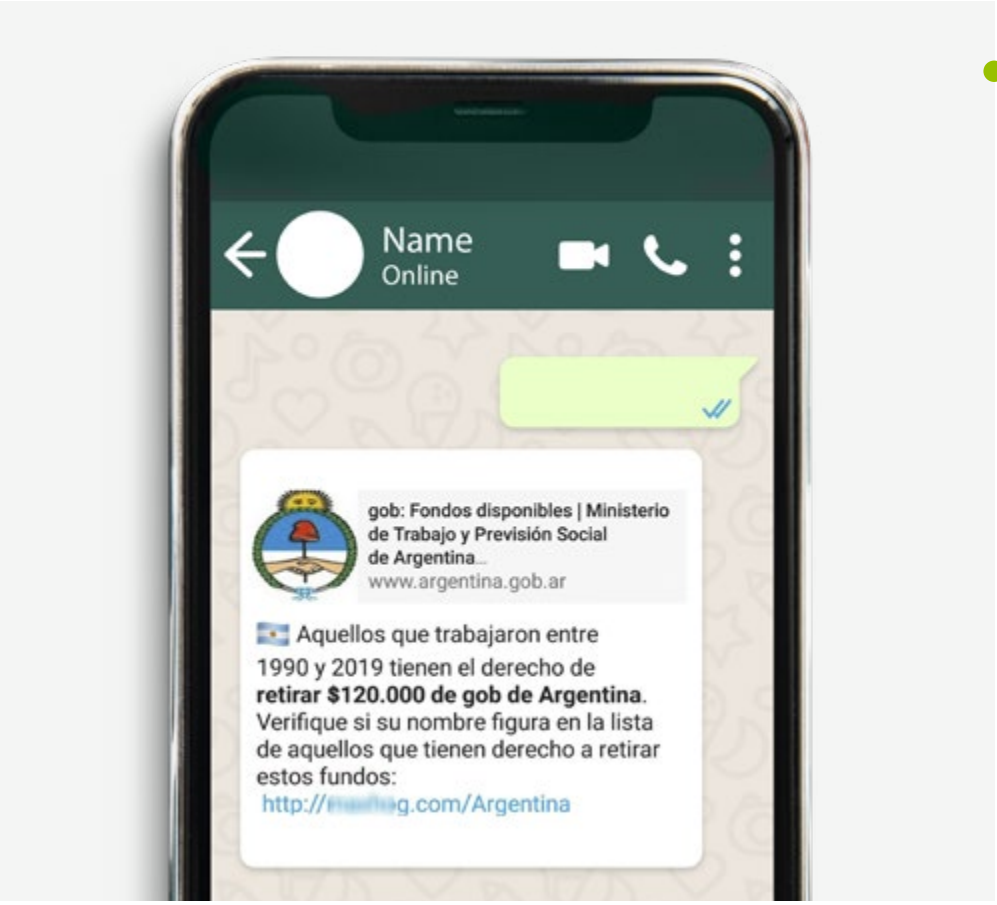
Acción requerida

Equipo de Netflix <contact@getticket.solutions>
Responder a: contact@getticket.solutions
Para: Martín Perez

7 de abril de 2019, 2.56

El aumento en la frecuencia con la que vemos circular este tipo de campañas no debe pensarse únicamente como una consecuencia directa de la exposición de información personal del usuario. Como mencionamos anteriormente, es la suma de todos los pequeños datos y detalles lo que puede aprovechar un atacante al momento de lanzar ataques más dirigidos. De aquí se desprende el hecho de que fueran solo este tipo de campañas las que registraron una alta actividad durante 2019. La circulación de campañas falsas a través de diferentes aplicaciones de mensajería (principalmente WhatsApp) en las que se prometen cupones o promociones por aniversarios, buscan desplegar publicidad, pero en muchos casos también obtener información personal de quienes reciben los mensajes, y es éste otro factor clave en el incremento de fugas de datos. De estos engaños surge

precisamente la posibilidad de utilizar información personal contra personas desprevenidas en ataques más sofisticados y dirigidos. A comienzos de 2019 se conocía la filtración de más de 2.200 millones de contraseñas, direcciones de correo y nombres de usuario con la publicación de cinco carpetas (Collection#1 a #5) que recopilaban esta información proveniente de distintas brechas. Fue este evento el que marcó a 2019 como el año de los datos personales y la privacidad.



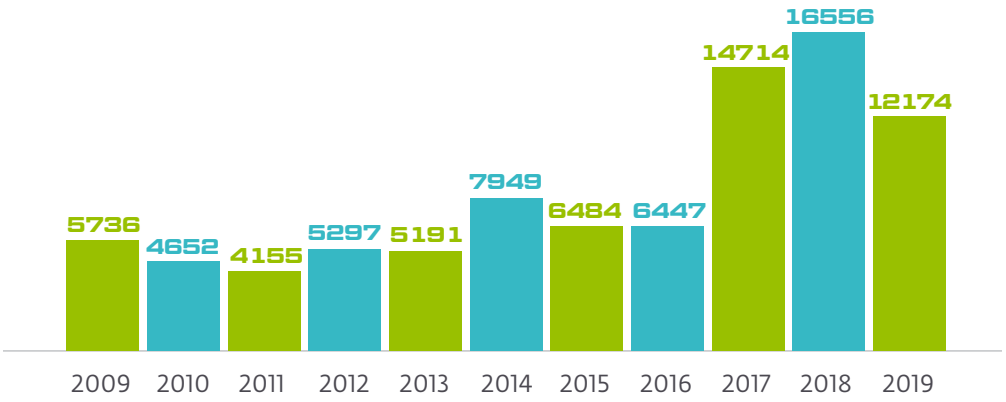
Suplantación Ministerio de Trabajo vía WhatsApp

Si bien aquella brecha fue la más grande, no fue la única. A lo largo del año se conocieron nuevos casos que las empresas se vieron obligadas a reportar al estar involucrados los datos de sus usuarios, bajo el deber de cumplir con las nuevas regulaciones, principalmente GDPR.

Es importante resaltar que los engaños basados en ingeniería social han ido evolucionando y lograron en muchos casos aumentar su efectividad. En este sentido, los cibercriminales han pasado de utilizar simples sitios de phishing a incorporar certificados SSL falsos o gratuitos con el objetivo de aprovecharse del desconocimiento del usuario de cara al funcionamiento del protocolo HTTPS, pasando por los ataques homográficos que tomaron más relevancia al suplantar la identidad de empresas y marcas reconocidas.

Otro de los incidentes con altos niveles de ocurrencia entre las empresas de Latinoamérica fue la explotación de vulnerabilidades, sufrido por el 8% de las encuestadas. Quizá una de las cuestiones más interesantes al abordar este tipo de incidentes es el hecho de que la cantidad de detecciones de vulnerabilidades informadas durante 2019 registró un descenso significativo respecto a 2018 y 2017,

GRÁFICO 7: Cantidad de detecciones de vulnerabilidades informadas



De todas formas, los números siguen siendo preocupantes si observamos la incidencia en las empresas y consideramos la cantidad de tecnología que debe mantenerse constantemente actualizada para evitar ser víctima de este tipo de explotaciones.

Exploits

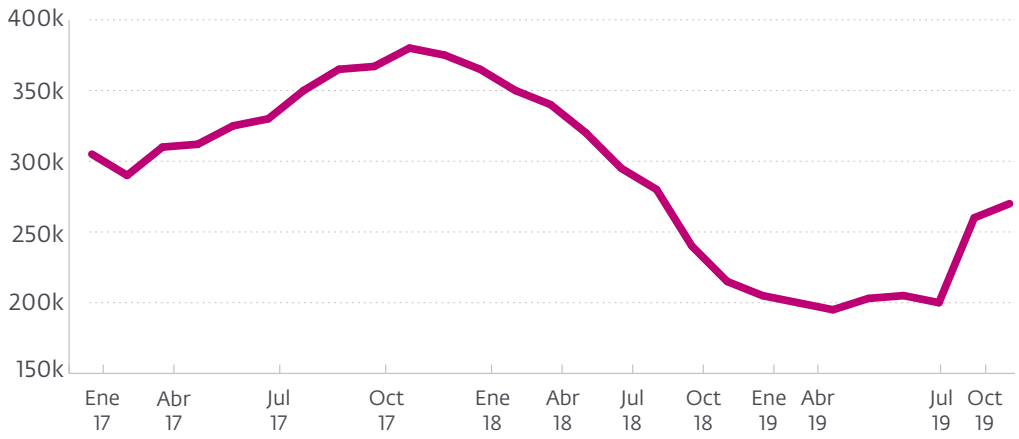
El otro elemento de esta combinación son los exploits. ¿Qué son? Se trata de códigos que, además de mostrar la existencia de una falla, exponen también la presencia de una vulnerabilidad. Es decir, que puede ser aprovechada por un atacante para comprometer la confidencialidad, integridad y disponibilidad de la información.

A lo largo de los últimos tres años se ha detectado un comportamiento decreciente en la cantidad de variantes detectadas y asociadas a exploits, pero lejos está esto de poder asociarse a la disminución del riesgo para las empresas. Un análisis detallado de la telemetría de ESET en estos últimos años demuestra que, desde la aparición del infame Wannacry, los cibercriminales están atentos al descubrimiento de nuevas vulnerabilidades para intentar aprovecharlas en sus últimas campañas.

GRÁFICO 8: Cantidad de variantes detectadas y asociadas a exploits

En el siguiente gráfico se aprecia el promedio móvil de la cantidad de hashes únicos detectados por mes en los últimos tres años asociados a detecciones de exploits en Latinoamérica. Durante 2017, es evidente el comportamiento creciente en la cantidad de nuevos hashes detectados, llegando a su máximo en octubre, mes en el que cambia la tendencia. Este crecimiento encuentra su explicación en el uso intensivo de los cibercriminales de EternalBlue, la familia de exploits que aprovechaba las vulnerabilidades de SMB, utilizado en diferentes tipos de códigos maliciosos más allá de Wannacry.

GRÁFICO 9: Promedio móvil de cantidad de hashes únicos detectados por mes asociados a detecciones de exploits en Latinoamérica

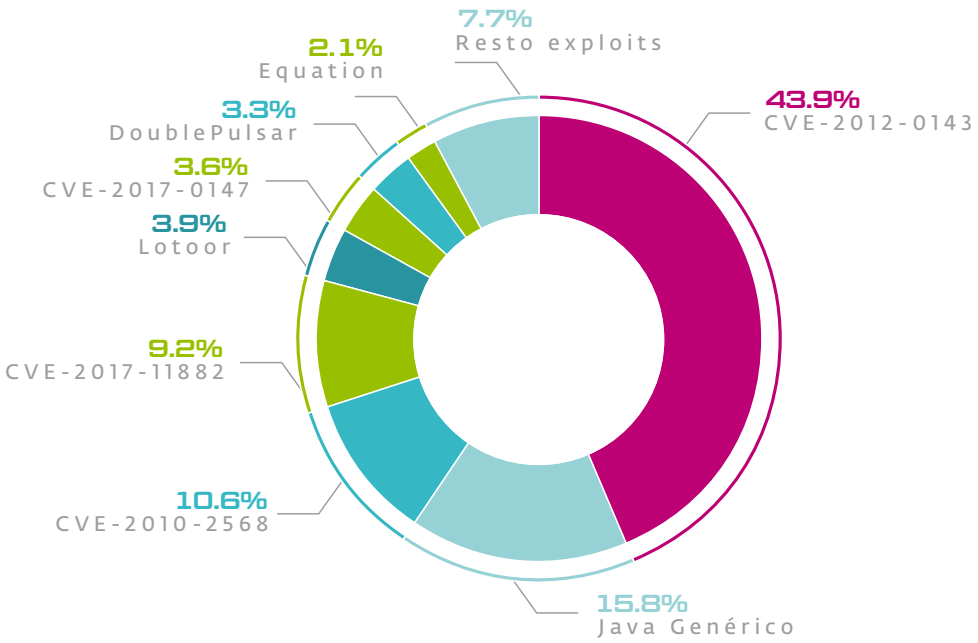


A lo largo de 2018 no se han registrado grandes variaciones en la aparición de nuevos hashes asociados con exploits, a pesar del máximo histórico en la cantidad de vulnerabilidades reportadas y del registro de vulnerabilidades importantes como Spectre, Meltdown y PowerPool, aunque no fueron utilizadas de forma masiva en campañas maliciosas. Ya entrados en 2019 vemos un nuevo punto de inflexión en la tendencia, cerca del mes de junio, cuando se dio a conocer la vulnerabilidad BlueKeep que, en noviembre de 2019, derivó en un nuevo máximo en la cantidad de detecciones. Hacia 2020 se ha registrado un comportamiento con tendencia decreciente, algo que probablemente se mantenga hasta la aparición de una nueva vulnerabilidad que tenga las características adecuadas para ser usada en campañas maliciosas.

Distribución de exploits en América Latina durante 2019

El siguiente gráfico muestra cómo ha sido la distribución de los exploits con mayores registros durante 2019 en Latinoamérica:

GRÁFICO 10: Mayores índices de exploits regitrados en LATAM durante 2019



En lo que respecta a la distribución por país, el 50% de las detecciones de la región estuvo concentrado en México (20,8%), Perú (18,4%) y Colombia (11,1%); seguidas por Brasil (10,3%), Argentina (7,4%) y Guatemala (7,1%).

Estos análisis dejan en evidencia el riesgo asociado a la explotación de vulnerabilidades, un problema latente para las empresas, ya sea que se utilicen en ataques masivos o dirigidos.

EL **50%** DE LAS DETECCIONES DE EXPLOITS EN LATINOAMÉRICA SE CONCENTRÓ EN MÉXICO, PERÚ Y COLOMBIA.

02

Control y prevención de riesgos

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

La seguridad de la información debe abordarse desde un enfoque por capas que no deben estar únicamente basadas en tecnología. Quizás, cuando se habla de controles de seguridad, lo primero que venga a la cabeza de muchos sea contar con tecnologías de protección. Si bien esto es absolutamente necesario, también lo es contar con políticas y planes para gestionar la seguridad de la información, así como también con planes continuos de capacitación a los colaboradores.

Esto último se ve reflejado precisamente en que casi el 98% de las empresas en la región cuenta con algún control basado en tecnología, que puede incluir desde una solución de seguridad hasta un DLP. Sin embargo, aún el 39% de las empresas no cuenta con políticas de seguridad y apenas un 28% clasifica su información.

EL **39%** DE LAS EMPRESAS NO CUENTA CON POLÍTICAS DE SEGURIDAD, Y APENAS UN 28% CLASIFICA SU INFORMACIÓN.

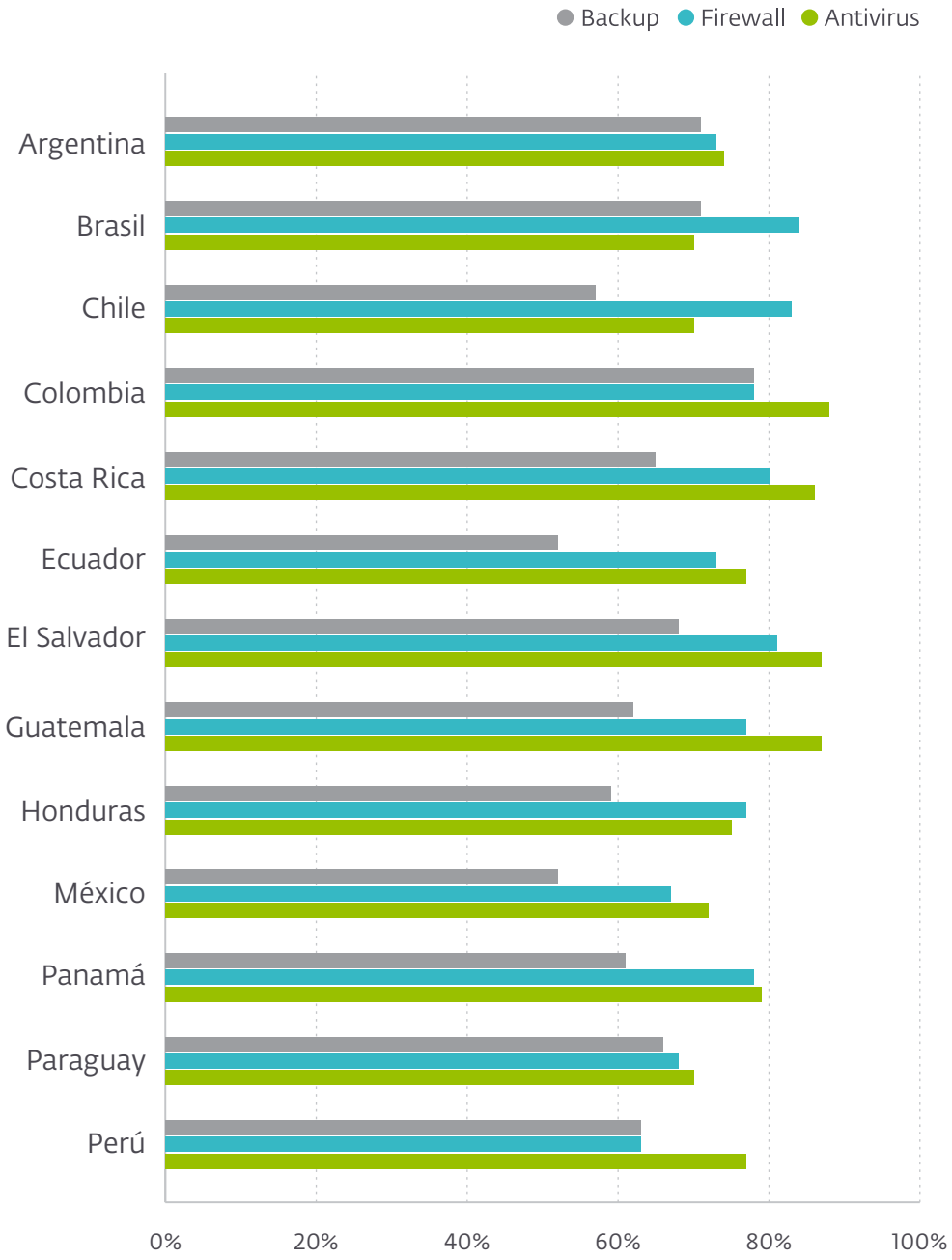
> Controles

Una de las cuestiones más sorprendentes es que las medidas más básicas de control, aquellas que podría esperarse ver en todas las empresas como una solución de seguridad antivirus, un backup (como gestión y no copias aisladas) o una solución de Firewall, no están realmente implementadas en la totalidad de las empresas encuestadas. De hecho, este número apenas alcanza el 48% en las organizaciones abordadas.

SOLO EL **48%** DE LAS EMPRESAS DE LA REGIÓN CUENTA CON LAS TRES MEDIDAS BÁSICAS DE PROTECCIÓN: SOLUCIÓN ANTIVIRUS, BACKUP Y FIREWALL.

El antivirus sigue siendo la herramienta de control más utilizada (78%), lo que lo ubica como la primera línea de defensa contra los atacantes. No obstante, si bien se trata de una tecnología fundamental que debe estar implementada, existe todavía un 22% de empresas que no cuenta con una solución antivirus entre sus barreras de protección.

GRÁFICO 11: Niveles de implementación de controles básicos de seguridad por país

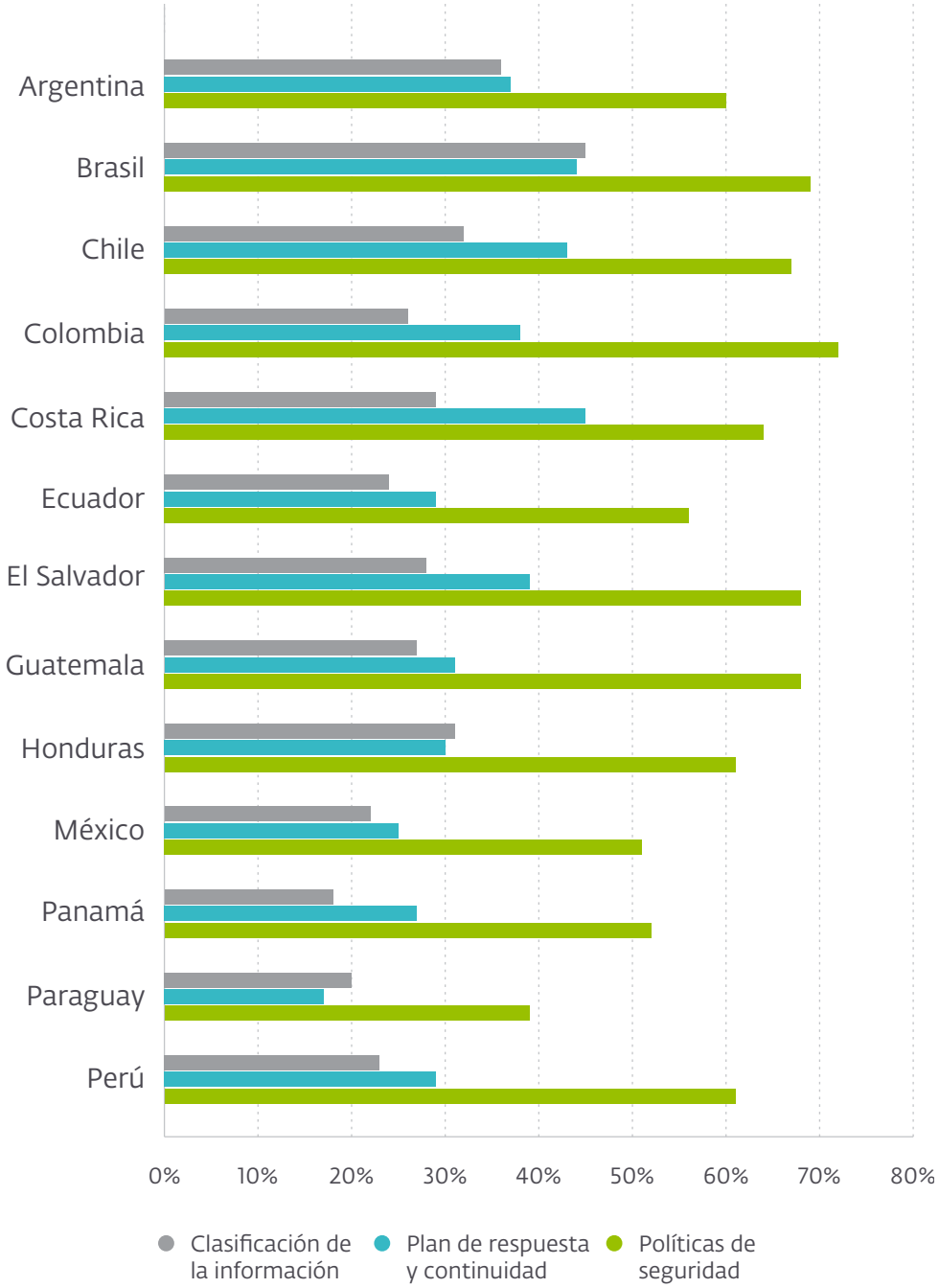


Dado el amplio abanico de posibilidades que tienen los atacantes para comprometer la seguridad de una empresa, en los últimos años han ido apareciendo nuevas tecnologías para complementar la protección. Sin embargo, notamos que su adopción aún es bastante baja. Por ejemplo, un segundo factor de autenticación es considerado solo por el 17% de las empresas encuestadas (apenas superior al 13% de la medición del año anterior), y el mismo valor se registra para las empresas que cuentan con un EDR (16% en 2018). Ambas soluciones se ven apenas superadas por el 19% de las empresas que cifran su información (18% en 2018).

> Gestión

Como mencionamos, la tecnología no lo es todo en el campo de la seguridad de la información, por lo que es necesario complementarla con una adecuada gestión. Si bien los niveles de implementación de políticas de seguridad acumulan un alto porcentaje (61% de las empresas declararon contar con ellas) los números aún no son los óptimos. En países como Paraguay, menos de la mitad de las empresas encuestadas dijo contar con este tipo de controles (39%) y en México apenas el 51%, es decir, 1 de cada 2 empresas asegura haberlo implementado.

GRÁFICO 12: Niveles de implementación de prácticas de gestión para la seguridad por país



Cabe destacar que, de las empresas que cuentan con una política de backup entre sus implementaciones de seguridad, solo el 71% integra además una política de clasificación de la información.

Al analizar los datos relevados, resulta preocupante también que solo una tercera parte (33%) de las empresas encuestadas cuenta con un plan de continuidad del negocio, número que no se modifica respecto del año anterior, a pesar del avance de la tecnología y de las campañas de concientización. De hecho, es crucial que las empresas sepan cómo responder en el caso de que ocurra un incidente que pueda poner en riesgo las operaciones del negocio. No se trata únicamente de tener una respuesta rápida y eficiente para la recuperación del incidente, sino también de adoptar una medida más de protección para identificar las fallas y evitar que vuelvan a presentarse incidentes similares a futuro. Además, debe destacarse el impacto que esto podría tener en sus finanzas y en su reputación frente a su cadena de valor (clientes y asociados).

SOLO UN **33%** DE LAS EMPRESAS ENCUESTADAS CUENTA CON UN PLAN DE CONTINUIDAD DEL NEGOCIO.

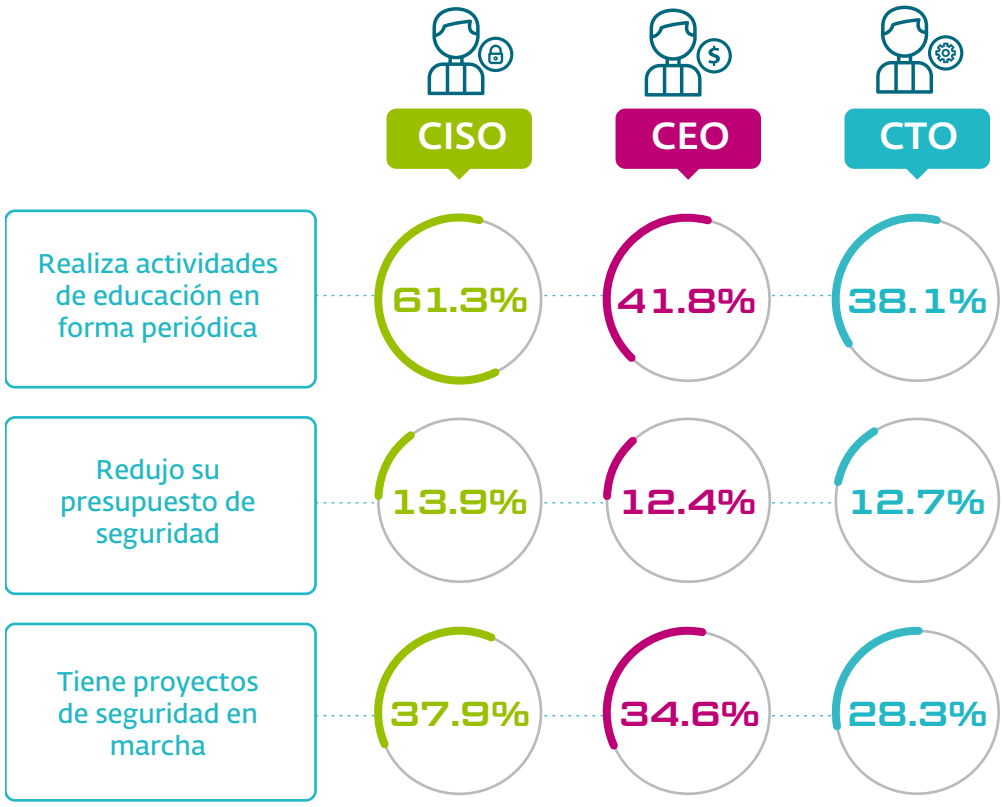
La baja adopción de metodologías para la clasificación de la información de las empresas es otro aspecto preocupante. A nivel regional, este tipo de prácticas alcanza apenas al 28% de las empresas encuestadas. Ya mencionamos que 2019 tuvo récords históricos en casos de fugas de información y brechas de seguridad. Por ello, resulta necesario que las empresas conozcan dónde está almacenada su información y qué características tiene para poder implementar los controles que realmente necesitan.

03

La visión del C-Level

Ante el panorama de incidentes presentado, las preocupaciones recurrentes y la adopción de controles, resulta interesante entender cómo están organizadas las empresas para afrontar los retos relacionados, precisamente, con la gestión de la seguridad de la información. Además de los controles de seguridad, entran en juego aquí nuevas dimensiones que amplían el alcance de la gestión.

Dentro de las encuestas dirigidas al C-Level, obtuvimos información respecto de las actividades ligadas a la educación dentro de las organizaciones, las variaciones de presupuesto destinado a la seguridad y el desarrollo de proyectos de seguridad.



Sin lugar a duda, aquellas empresas que cuentan con un CISO a cargo de las actividades de seguridad parecen tener un mejor escenario para el desarrollo de una estrategia de seguridad, más allá de la adopción de tecnologías de seguridad. Por ejemplo, la imple-

mentación de actividades periódicas de educación en aquellas empresas donde hay un CISO (61,3%) es mayor que en aquellas donde no existe esta figura (41,8% y 38%).

El presupuesto para desarrollar este tipo de actividades será siempre un factor fundamental, y si bien, en líneas generales, el porcentaje de empresas que redujo su presupuesto en seguridad es menor al 15%, (cifra que en 2018 era menor en empresas que contaban con un CISO), este período pudo verse afectado por variables macroeconómicas de la región.

> Educación

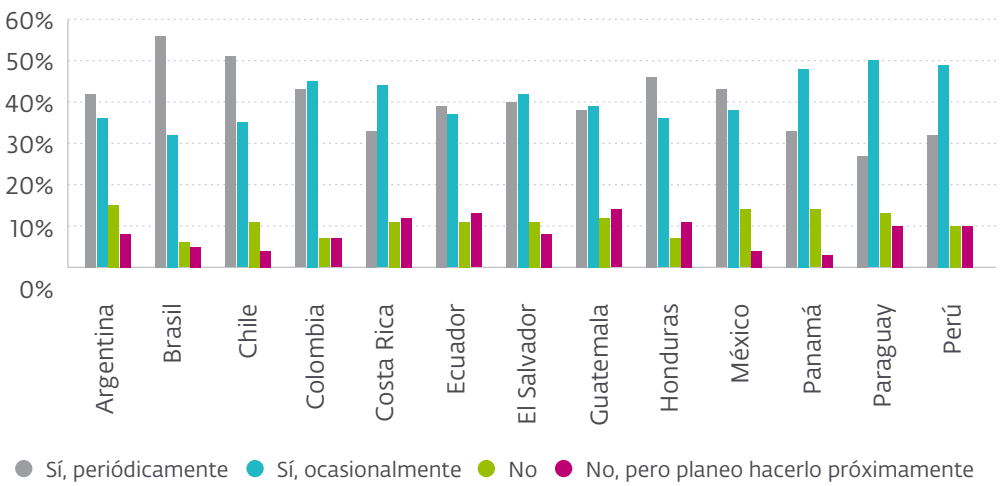
Nuevamente, cabe destacar que la figura de un responsable de seguridad genera un movimiento positivo en las actividades y proyectos relacionados con la seguridad dentro de la empresa. ¿Pero qué impacto tiene la realización de estas actividades?

Incidentes con códigos maliciosos
La incidencia de este tipo de ataques se reduce del **34%** al **29%** en aquellas empresas que implementan capacitaciones de seguridad de forma periódica.

El porcentaje de empresas que realizó actividades periódicas de educación y se vio afectada por incidentes de seguridad es menor que el de aquellas empresas en las que no se lleva adelante este tipo de actividades.

Si bien no hay manera de medir en forma directa la incidencia de este tipo de actividades, sí es posible identificar el rol que juega el nivel de educación de los usuarios como factor diferencial para garantizar la seguridad de la información. Esto es importante dado que la gestión de la seguridad es un proceso integral cuyo análisis no se puede limitar únicamente a la tecnología y a los controles que se implementan.

GRÁFICO 13: Lleva adelante actividades de concientización



> Inversión

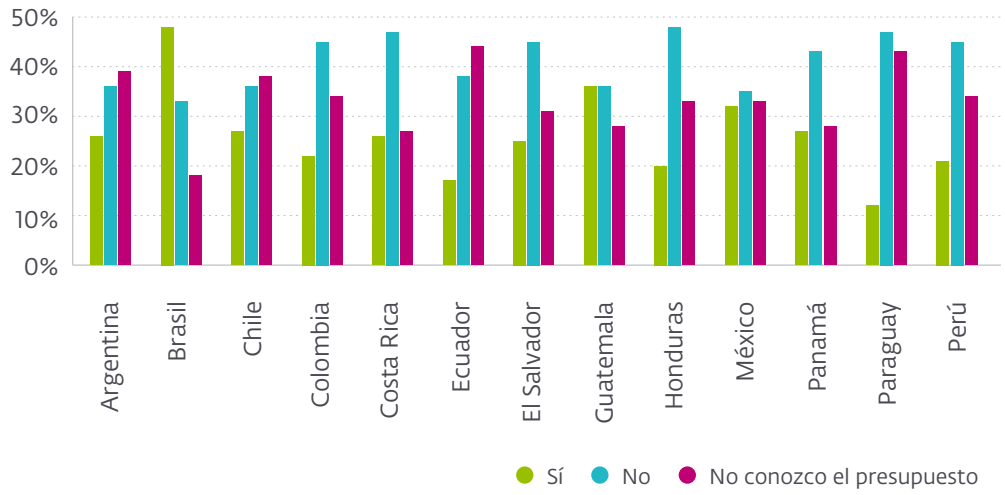
Quizá una de las quejas más recurrentes que se da en el interior de muchas empresas es la falta de presupuesto para el área de seguridad. Este reclamo ha mantenido cifras similares (64%) a lo largo del tiempo, aunque en 2019 el porcentaje de empresas que manifestaron la falta de presupuesto es del 75%.

EN 2019, EL **75%** DE LAS EMPRESAS MANIFESTÓ LA FALTA DE PRESUPUESTO DESTINADO AL ÁREA DE SEGURIDAD.

La variación del presupuesto asignado a los proyectos de seguridad sufrió una notable caída respecto del año anterior, que se mantenía en un promedio del 40%. Este año, solo el 20% de las empresas dijo haber aumentado el presupuesto de seguridad respecto del año anterior y, si bien cambia de acuerdo al tamaño de la empresa, solo el 9% lo redujo.

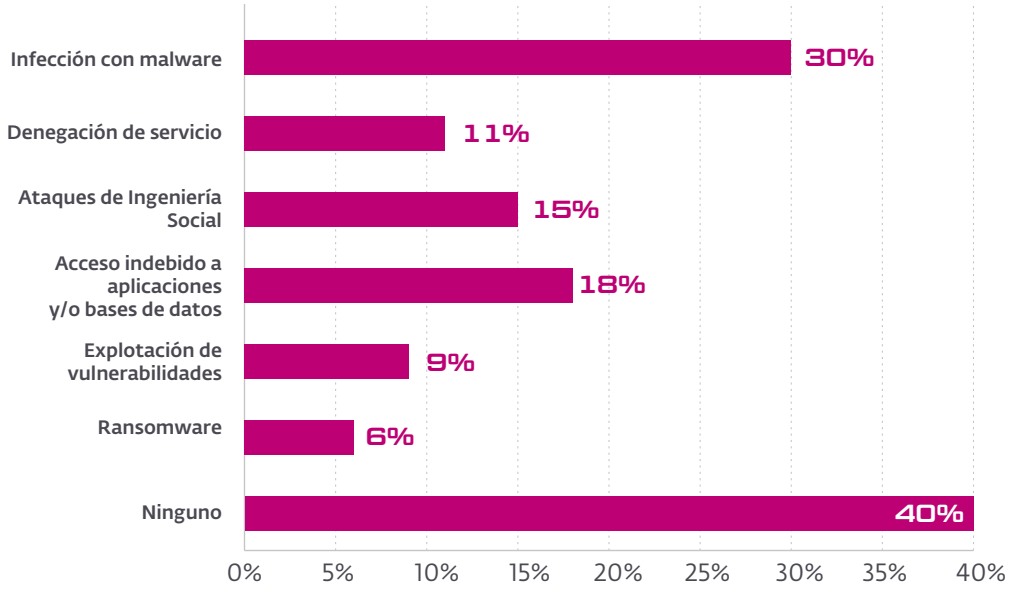
Estas cifras reflejan la necesidad de que las empresas piensen en alternativas diferentes para desarrollar sus proyectos de seguridad. Quizá se requiera mayor esfuerzo a la hora de invertir tiempo y recursos para lograr los resultados óptimos.

GRÁFICO 14: ¿Considera suficiente el presupuesto asignado al área de seguridad de su empresa?

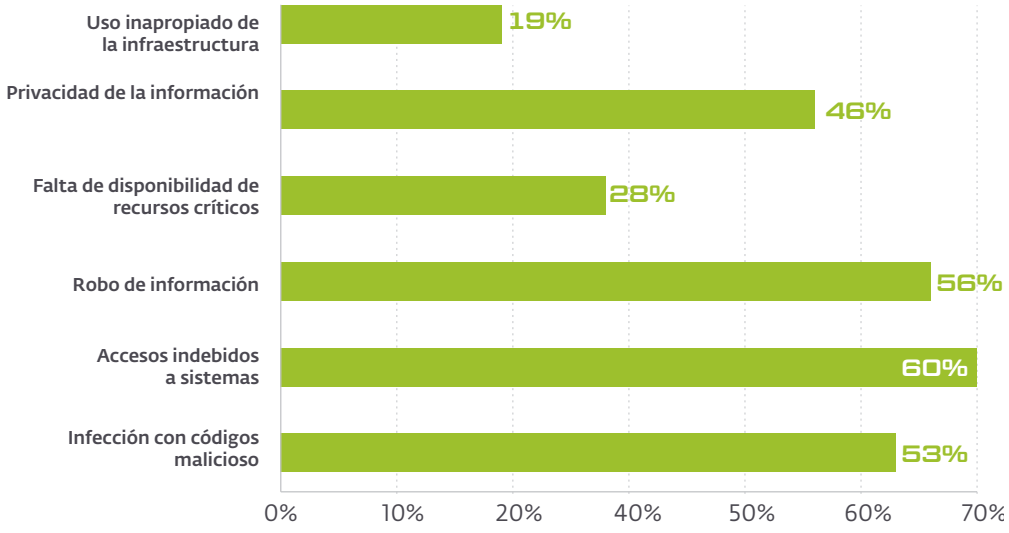


Anexo:
datos estadísticos

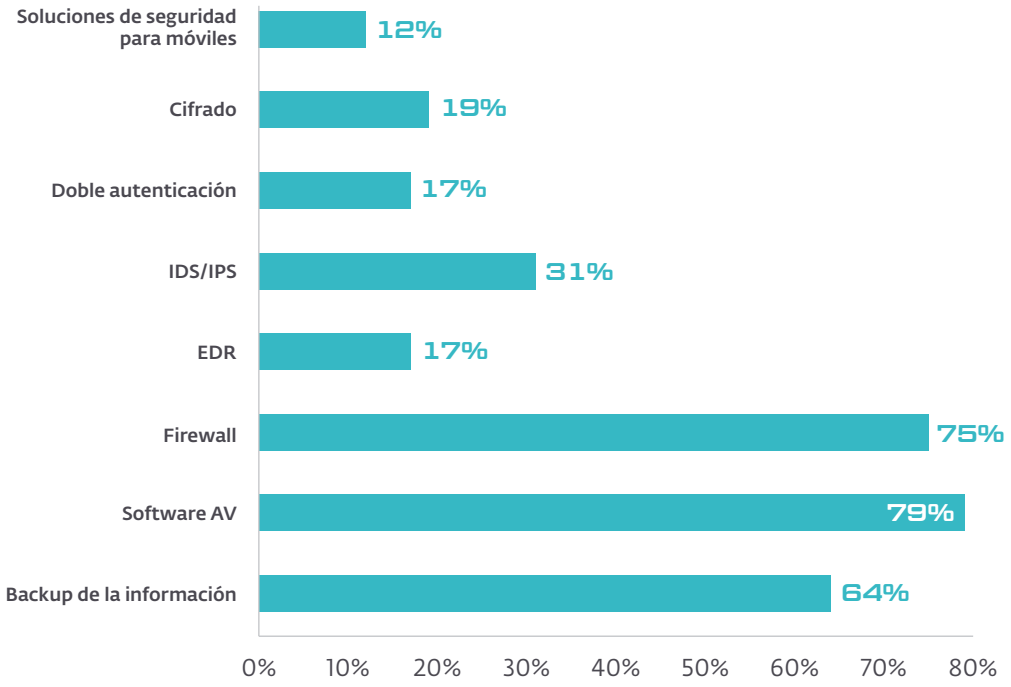
INCIDENTES DE SEGURIDAD



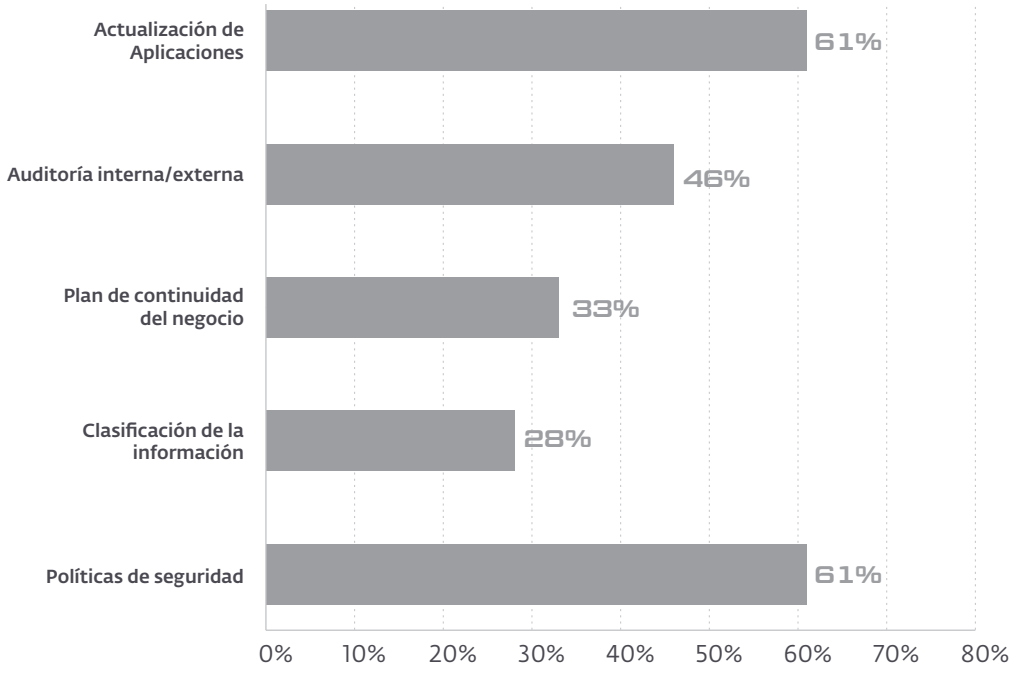
PREOCUPACIONES RELACIONADAS CON LA SEGURIDAD



CONTROLES BASADOS EN TECNOLOGÍA



CONTROLES BASADOS EN GESTIÓN



SOBRE ESET

+ 110 millones de usuarios en todo el mundo	**13** centros en el mundo de investigación y desarrollo
+ 400 mil clientes corporativos	**200** países y territorios

Para conocer más información acerca de ESET visite: www.eset.com/latam

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