
eset
5ECURITY
REPORT
LATINOAMÉRICA 2021

ÍNDICE

INTRODUCCIÓN

Como cada año, el *Laboratorio de Investigación de ESET Latinoamérica* publica el **ESET Security Report (ESR)**, un informe que se apoya en encuestas realizadas a profesionales de tecnología, para conocer el panorama de la seguridad corporativa en la región.

La edición 2021 de este documento es el resultado de consultas realizadas a cerca de 1000 ejecutivos y representantes de empresas en 17 países de Latinoamérica durante los eventos digitales del año pasado, pero además incluye información obtenida de los datos telemétricos de ESET, de los informes trimestrales de amenazas y de otros análisis emprendidos por ESET durante la pandemia a nivel global y regional.

A raíz de la *pandemia del COVID-19* y del enorme impacto social que ha tenido, el desafío para la realización de este reporte ha sido mayor, no solo porque disminuyó la cantidad de eventos en los que solemos recolectar las respuestas de los ejecutivos, sino también por tratar de comprender las preocupaciones e incidentes dentro de un nuevo entorno laboral para las empresas y sus trabajadores. En este contexto, el informe se enfoca en conocer las principales preocupaciones de los encargados de tomar decisiones y brindar protección a los activos más importantes en las empresas, así como los incidentes de seguridad más frecuentes en las organizaciones durante el último año. Esta información es complementada y sustentada con datos recopilados por la telemetría de ESET.

El conjunto de información recopilada y el cruce de datos obtenidos de diferentes fuentes ofrece un panorama amplio del estado de la seguridad en las empresas de Latinoamérica, así como de las prácticas de ciberseguridad adoptadas y adaptadas durante la pandemia.

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

HALLAZGOS

- Los *códigos maliciosos* son la principal preocupación (**64%**) y la primera causa de incidentes de seguridad (**34%)** en las empresas latinoamericanas.

- De acuerdo con la telemetría de ESET, las empresas en Brasil (**19%**) fueron las más afectadas por el *malware* según el total de las detecciones en Latinoamérica durante 2020, seguidas por las de México (**17,5%**) y Argentina (**13,3%**).

- Las campañas masivas de *ransomware* se redujeron **35%** en 2020, mientras que los ataques dirigidos con este *malware* se volvieron más agresivos y lucrativos, agregando características como *doxing, print bombing, cold call y ataques de DDoS.*

- El número *ataques de fuerza bruta* a los servicios de acceso remoto como RDP creció **704%**, mientras que los registros para usuarios únicos aumentaron **196%** durante 2020 en Latinoamérica.

EN AMÉRICA LATINA LOS ATAQUES DE FUERZA BRUTA AL RDP CRECIERON 704% DURANTE 2020.

- Brasil, México, Chile y Argentina son los países más afectados por más de una decena de familias de *malware bancario* que iniciaron sus operaciones en Latinoamérica y extendieron su propagación a Estados Unidos y Europa.

- El *malware* para la *minería de criptomonedas* aumentó su actividad hacia finales de 2020 en concordancia con el aumento en el valor de las criptodivisas. Tailandia (**17,9%**) fue el país con mayor porcentaje de detecciones, seguido de Perú (**10,1%**) y Ecuador (**5,1%**).

- Con base en la telemetría de ESET, las empresas de Brasil (**26,4%**) fueron las más afectadas por casos de phishing durante 2020, seguidas por las empresas de Perú (**22,8%**) y México (**12%**).

- Las soluciones *antimalware* son los controles de seguridad técnicos más utilizados con el **86%** de las respuestas obtenidas. La práctica de gestión de la seguridad más aplicada son las actualizaciones del *software* con el **71%** de respuestas afirmativas.

- Los dispositivos móviles son cada vez más utilizados para actividades corporativas como videoconferencias, acceso a correo electrónico o información, aunque un porcentaje muy bajo **(15%**) utiliza una solución *antimalware* en dichos dispositivos.

- Para el **76%** de los ejecutivos y responsables en la toma de decisiones, el presupuesto para el área de seguridad se mantuvo o se redujo con respecto a años anteriores, y el **81%** aseguro que los recursos con los que cuentan para seguridad resultan insuficientes.

- En cuanto a la concientización y educación en ciberseguridad, **78%** de los encuestados realiza actividades con este fin entre los colaboradores de manera ocasional.

CIBERSEGURIDAD EN TIEMPOS DE PANDEMIA

El mundo ha enfrentado enormes desafíos ante la pandemia. La crisis provocada por el coronavirus ha planteado grandes dificultades y retos para los gobiernos, las personas y las empresas en todos los sectores, lo que ha significado nuevos paradigmas en la forma de interactuar. El trabajo remoto en las organizaciones es tan solo una muestra de los cambios radicales que han acontecido en el mundo entero.

LA NUEVA NORMALIDAD IMPUESTA POR EL COVID-19 MODIFICÓ EL TRABAJO DE LOS RESPONSABLES DE LAS ÁREAS DE SEGURIDAD, OBLIGANDO A CAMBIAR PRIORIDADES, IDENTIFICAR NECESIDADES Y ESTABLECER CONDICIONES.

La nueva normalidad impuesta por el COVID-19 también modificó considerablemente el trabajo de los responsables de las áreas de seguridad, donde fue necesario cambiar prioridades, identificar necesidades y establecer condiciones. Se acentuaron tendencias observadas previo a la pandemia, por lo que fue necesario considerar, ampliar o acelerar la transformación digital de los negocios.

En muchos casos, las condiciones desfavorables para adoptar el trabajo remoto y plataformas en la nube jugaron en contra de los objetivos, a lo que se sumaron los presupuestos ajustados debido a la baja en los ingresos y la aparición de nuevas leyes y reglamentos, como las legislaciones en torno al teletrabajo. La pandemia ha significado nuevos retos, oportunidades, y al mismo tiempo, nuevos riesgos.

Si bien antes de la pandemia los ciberataques presentaban una tendencia al alza, ésta se mantuvo con los confinamientos, en particular las campañas de phishing y malware. La diferencia actual radica en el hecho de que los ambientes son cada vez más hostiles, si se considera que previo al confinamiento la oficina y el hogar se encontraban completamente separadas, salvo casos eventuales de trabajo desde el hogar.

Ahora la red de la empresa también incluye las redes hogareñas, en las que probablemente se aplican prácticas deficientes y se utilizan herramientas de seguridad precarias, a diferencia de los controles de seguridad implementados en las redes y sistemas corporativos. Las empresas se vieron en la necesidad de implementar esquemas de teletrabajo de forma rápida e improvisada, ocasionando que de un día para el otro los dispositivos personales de muchos colaboradores formen parte de la red corporativa, con la disparidad de condiciones de seguridad que eso implica.

Un estudio realizado por ESET encontró que **80%** de los representantes de las empresas reportaron estar más preocupadas por los riesgos de seguridad relacionados con factores humanos. En este mismo estudio se destaca también la percepción actual que se tiene sobre la ciberseguridad, ya que **42%** de los encuestados consideró que el nivel de riesgo del trabajo remoto durante el confinamiento equipara al cibercrimen o los ciberataques, ya que se encuentran aparejados, algo que quedó demostrado durante 2020.

En un contexto de nuevas modalidades, donde la pandemia todavía no concluye y continúa generando cambios radicales y acelerados, algunas prácticas llegaron para quedarse. Por ejemplo, **50%** de los encuestados considera mantener en el futuro los cambios implementados durante la pandemia, como el home office permanente o las plataformas en la nube implementadas durante el confinamiento.

La tendencia *Bring Your Own Device* (BYOD) que nunca terminó de ser completamente adoptada en las empresas, se vio reemplazado con algo que podemos entender como B*ring Home To Work:* traer la casa al trabajo; estas condiciones muestran la importancia de la transformación digital y de la ciberseguridad en cualquier lugar y en cualquier momento.

PREOCUPACIONES

Las preocupaciones de los que toman decisiones en materia de *Seguridad de la Información* están determinadas por distintos factores, como pueden ser la proliferación de amenazas informáticas, incidentes de seguridad más frecuentes, tendencias o pronósticos relacionados con las tecnologías, o bien, condiciones adversas de situaciones que incluso resultan poco frecuentes, como las observadas durante la pandemia.

El análisis de dichas preocupaciones es una actividad relevante en el proceso de aseguramiento de los activos de información, ya que el trabajo de identificación de escenarios riesgosos suele ser utilizado para definir o considerar medidas de protección para la información y otros activos, lo que implica el desarrollo de iniciativas para resolver problemas actuales o anticiparse a necesidades futuras.

Como resultado de las encuestas realizadas para el ESR 2021, las principales preocupaciones en materia de seguridad de las empresas latinoamericanas son los códigos maliciosos (**64%**), seguido del robo de información (**60%**) y accesos indebidos a los sistemas (**56%**).

LAS PRINCIPALES PREOCUPACIONES DE LAS EMPRESAS EN MATERIA DE SEGURIDAD SON LOS CÓDIGOS MALICIOSOS (64%), EL ROBO DE INFORMACIÓN (60%) Y EL ACCESO INDEBIDO A LOS SISTEMAS (56%).

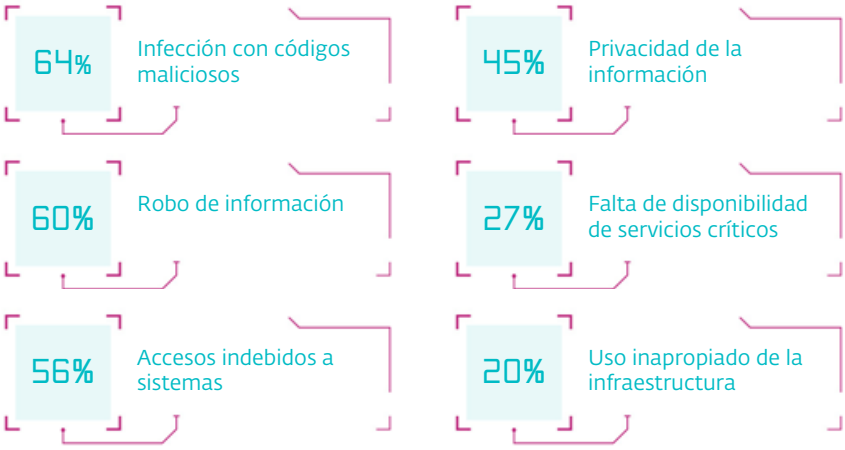

Gráfico 1. *Preocupaciones en materia de Seguridad de la Información de las empresas de Latinoamérica. Fuente: encuesta realizada por ESET a empresas durante 2020.*

El malware se posiciona como la principal causa de preocupación en esta edición del ESR, a diferencia de informes pasados, en particular el año anterior, donde la lista fue encabezada por el acceso indebido a la información y los sistemas.

Estos cambios podrían deberse en gran medida a la proliferación de los códigos maliciosos que resultan más rentables para los atacantes y las nuevas condiciones de trabajo, que en conjunto definen el ambiente de amenazas informáticas de los últimos meses.

> Secuestro de información:
la continua reinvención del ransomware

El *ransomware* merece una mención especial cuando se habla del malware. Este tipo de código malicioso mantuvo su actividad y efectividad durante 2020, entre otras razones, debido a las nuevas condiciones de trabajo en las organizaciones y a su continua reinvención. El uso de familias de ransomware en ataques dirigidos se consolidó durante el año pasado.

Al cifrado de los archivos en los equipos comprometidos para demandar un pago como rescate por la información se le sumó la práctica conocida como doxing, es decir, el robo de información y la posterior extorsión bajo la amenaza de hacer públicos los datos sensibles exfiltrados. En conjunto, ambas acciones aumentan la posibilidad de monetizar los ciberataques.

Además, se han agregado nuevas tácticas al *modus operandi* del *ransomware*, como lo que se ha denominado *print bombing*, que utiliza las impresoras disponibles en la red de las víctimas para imprimir la demanda del rescate. Otro medio de presión ejercido por las bandas de ciberdelincuentes son las "llamadas en frío" o *cold calls* al personal de las organizaciones afectadas que buscan evitar el pago del rescate respaldando su información, para intimarlos a pagar a través de amenazas y mecanismos de extorsión.

EL DOXING SE CONSOLIDÓ DURANTE 2020, CON VARIOS GRUPOS DE RANSOMWARE ADOPTANDO ESTA ESTRATEGIA QUE CONSISTE EN EL ROBO DE INFORMACIÓN Y LA AMENAZA DE PUBLICARLA EN CASO DE NO PAGAR EL RESCATE.

Como si fuera poco, a las medidas utilizadas para ejercer presión a las víctimas de *ransomware*, se han agregado *ataques DDoS* sobre los sitios Web de las organizaciones afectadas, con el propósito de obligarlas a reanudar las negociaciones.
La operación de los grupos de *ransomware* puede entenderse como amenazas persistentes ya que, en la mayoría de los casos, la ejecución del código malicioso resulta ser una de las últimas etapas de los ataques donde previamente fue comprometida la información y la infraestructura tecnológica.

Los grupos de ciberdelincuentes detrás de los ataques dirigidos se vuelven más agresivos, apuntando a todo tipo de organizaciones que van desde hospitales, universidades, organismos gubernamentales, bancos, pequeñas, medianas y grandes empresas. Si bien algunos grupos de ransomware prometieron no atacar a las instituciones de salud durante la pandemia, otros continúan apuntando a este sector crítico durante la contingencia sanitaria global.

En los últimos meses de 2020 y primeros meses de 2021, se observaron probablemente los montos más elevados vistos hasta la fecha en cuanto a los rescates solicitados por los atacantes, haciendo del ransomware un negocio cibercriminal bastante lucrativo, como es el caso del modelo *ransomware-as-a-service* (RaaS), donde los desarrolladores del malware obtienen comisiones de los grupos que utilizan sus herramientas maliciosas.

La tendencia a la baja identificada en los ataques de ransomware de difusión masiva puede ser atribuida a las ganancias superiores obtenidas mediante los ataques dirigidos, combinados con las tácticas ya mencionadas. Otra condición puede estar relacionada con el RaaS y el hecho de que diversas familias de ransomware son distribuidas por otros códigos maliciosos en instancias posteriores.

Lo anterior también puede ser la razón por la que, a pesar de que familias de ransomware como *Maze, Revil/Sodinokibi, DopplePaymer, NetWalker o Egregor* han ocupado los titulares en los medios de comunicación en la región y a nivel global en el último año, no aparecen como las familias más detectadas.

De hecho, durante 2020 WannaCry o WannaCryptor (**56,4%**) con sus características de gusano, fue la familia con mayor porcentaje de detección en Latinoamérica, seguida de STOP (**12,2%**), Crysis (**7,4%**), Phobos (**4,7%**) y Philadelphia (**1,9%**). Estas detecciones están vinculadas a hashes conocidos que continúan propagándose en redes con sistemas desactualizados.

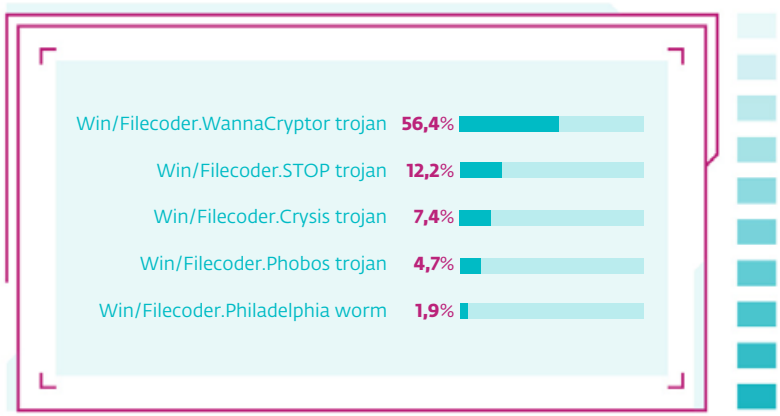

Gráfico 2. *Preocupaciones en materia de Seguridad de la Información de las empresas de Latinoamérica. Fuente: encuesta realizada por ESET a empresas durante 2020.*

Esto también explica por qué se identifican más familias de ransomware, mientras que las detecciones van a la baja. El año pasado se registraron **1498** familias y variantes de ransomware, **5,5%** más respecto del 2019, mientras que las campañas de propagación masiva presentaron una reducción de **35%** en las detecciones en el cuarto trimestre respecto al primero del 2020. Las tendencias vistas desde 2017 se acentuaron en el último año.

EN 2020 SE REGISTRARON 1498 FAMILIAS Y VARIANTES DE RANSOMWARE, LO QUE SIGNIFICA UN AUMENTO DEL 5,5% CON RESPECTO A 2019.

Los países con mayor cantidad de detecciones de *ransomware* a nivel empresas en Latinoamérica durante 2020 fueron Perú (**30%**), seguido por México (**14.9%**), Venezuela (**13.2%)**, Brasil (**11.3%**) y Colombia (**7.9%**).

> Aumento en la cantidad de ataques a accesos remotos

La pandemia cambió radicalmente la naturaleza del trabajo diario, obligando a conectar un mayor número de sistemas a Internet y a aumentar las conexiones remotas, en ocasiones con configuraciones inseguras. Sin ser ajenos a esta realidad, los ciberdelincuentes intentaron aprovechar estas condiciones que durante 2020 encontraron un blanco importante en los servicios remotos como el Protocolo de Escritorio Remoto (RDP).

Además de las condiciones impuestas por la pandemia, existen diversas motivaciones que encuentran los atacantes para comprometer servicios como RDP. Por ejemplo, para comercializar los accesos robados en el mercado negro. En este sentido, los sistemas comprometidos suelen ser utilizados para llevar a cabo más actividades maliciosas, como instalar herramientas adicionales en servidores, descargar y ejecutar programas maliciosos (principalmente ransomware o mineros

de criptomonedas), o bien, para filtrar información. Como resultado, los ataques a los servicios de acceso remoto tuvieron un importante incremento el año pasado.

DURANTE 2020 SE REGISTRARON 29 MIL MILLONES DE DETECCIONES DE ATAQUES A RDP Y ALREDEDOR DE 770 MIL USUARIOS ÚNICOS AFECTADOS; LO QUE REPRESENTA UN INCREMENTO DE 768% ENTRE EL PRIMER Y CUARTO TRIMESTRE DE 2020.

Los datos que aporta la telemetría de ESET confirman un importante aumento en el número ataques de fuerza bruta a RDP bloqueados. A nivel global, durante 2020 se registraron **29** mil millones de detecciones de ataques a RDP y alrededor de **770** mil usuarios únicos afectados; los registros representan un incremento de **768%** entre el primer y cuarto trimestre de 2020 y un aumento de **225%** para los usuarios únicos.

En el caso de Latinoamérica, si se compara el primer trimestre de 2020 contra el cuarto trimestre de ese mismo año, estos registros representan un aumento de **704%** en el número de detecciones de los ataques de fuerza bruta y un incremento de **196%** en el mismo periodo para el número de usuarios únicos afectados por estos intentos de comprometer los accesos remotos.

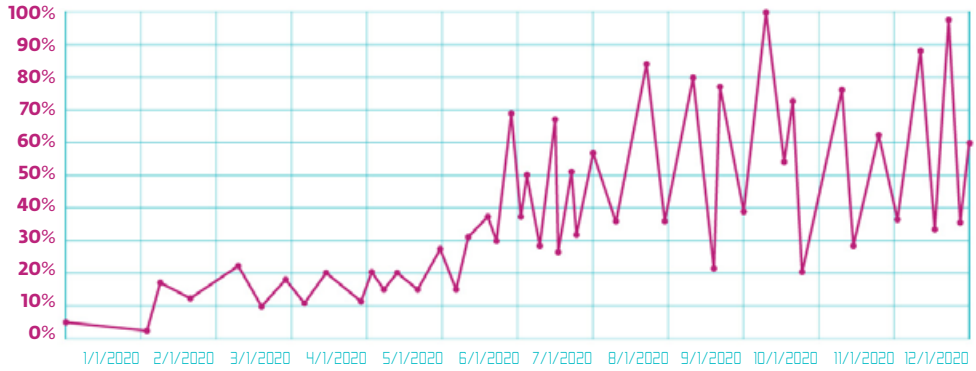

Gráfico 3. *Detecciones de ataques de fuerza bruta a RDP en Latinoamérica (2020). | Fuente: Telemetría de ESET.*

De acuerdo con una encuesta realizada por ESET en los primeros meses de la pandemia, solo el **24%** de los usuarios manifestó que la organización para la cual trabaja le brindó las herramientas de seguridad necesarias para trabajar remotamente y el **42%** de los participantes aseguró que su empleador no estaba preparado en cuanto a equipamiento y conocimientos de seguridad para hacerle frente al teletrabajo.

En otra encuesta realizada por ESET a finales de 2020, el **87,6%** de los participantes opinó que los cibercriminales han visto una oportunidad en el incremento del trabajo remoto para lanzar ataques dirigidos a las empresas, especialmente de ransomware, luego de comprometer los accesos remotos.

> Spyware y backdoors:
amenazas a la confidencialidad de la información

Una preocupación recurrente para los ejecutivos y profesionales responsables en la toma de decisiones en materia de ciberseguridad son las amenazas que atentan contra la confidencialidad de la información, que pueden desencadenar incidentes relacionados con acceso indebidos, robo de información, afectaciones a la privacidad de los datos, e incluso uso indebido de infraestructuras tecnológicas.

En este sentido, las amenazas comúnmente utilizadas con estos propósitos están asociadas al *spyware* (software espía) y *backdoors* (puertas traseras), que, aunque presentan tendencias a la baja durante 2020 a nivel global, según los datos de nuestra telemetría en Latinoamérica varios países presentan altos niveles de detección para estos tipos de amenazas.

DURANTE 2020, LOS PAÍSES QUE REGISTRARON LA MAYOR CANTIDAD DE DETECCIONES DE SPYWARE FUERON PERÚ, ISRAEL Y RUSIA.

Durante 2020, los países con la mayor cantidad de detecciones de *spyware* fueron Perú, Israel y Rusia; en el caso de *backdoors*, la lista la encabezaron Tailandia, Indonesia y Perú. Vale la pena destacar que estos códigos maliciosos, junto con los criptomineros, tienen una importante actividad en territorio peruano.

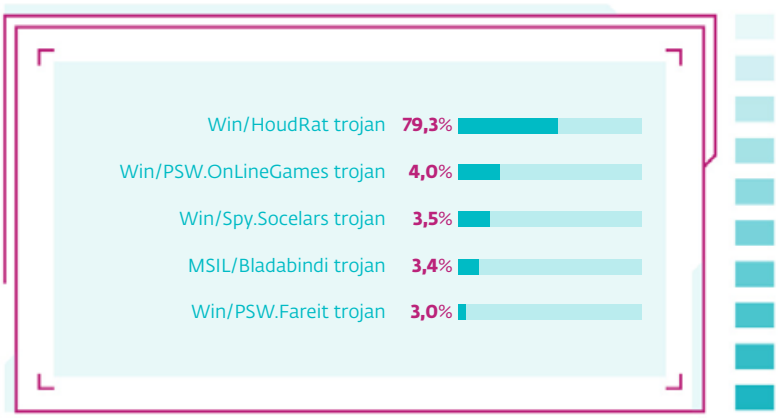

Gráfico 4. *Spyware más detectados en Latinoamérica (2020). | Fuente: Telemetría de ESET.*

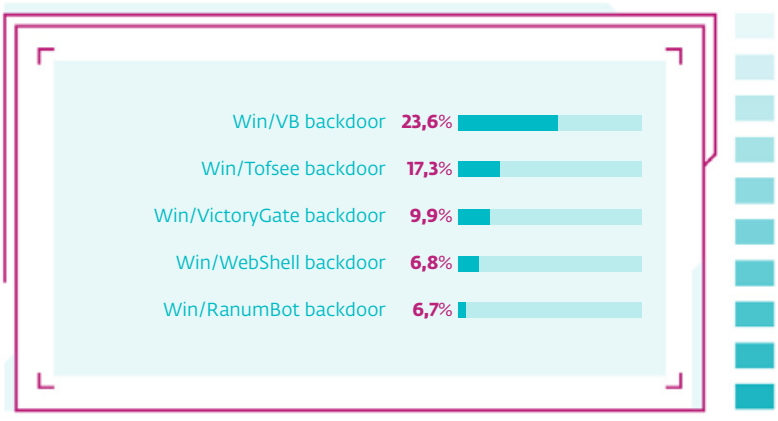

Gráfico 5. *Backdoors más detectados en Latinoamérica (2020). | Fuente: Telemetría de ESET.*

Vale la pena mencionar que estas categorías de *malware* son desarrolladas e identificadas como parte de campañas de espionaje sofisticadas, así como parte de ataques a la cadena de suministro identificados por ESET alrededor del mundo.

> Explotación de vulnerabilidades,
otra vía de accesos no autorizados

Además de los ataques de fuerza bruta, la explotación de vulnerabilidades es otra de las amenazas relacionada con las conexiones remotas y, en particular, al protocolo de escritorio remoto. Desde su aparición en mayo de 2019, *BlueKeep* ha mantenido una actividad importante, que se mantuvo durante 2020 con ligero descenso en el último trimestre.

El exploit relacionado con la vulnerabilidad CVE-2019-0708 identificada en *Remote Desktop Services*, permite la ejecución remota de código, por lo que busca ser aprovechada por atacantes de manera constante como una manera de comprometer los sistemas conectados a Internet. En 2020, *BlueKeep* tuvo una reducción de **8%** en la cantidad de detecciones para usuarios únicos y una disminución de **13%** en el total de intentos de explotación.

Del mismo modo, otro exploit utilizado de forma constante es *EternalBlue* (comúnmente asociado a campañas maliciosas como la de WannaCryptor), que también presentó una caída en el número de detecciones a usuarios finales de **8%**, mientras que las detecciones totales se mantuvieron prácticamente sin cambios durante 2020.

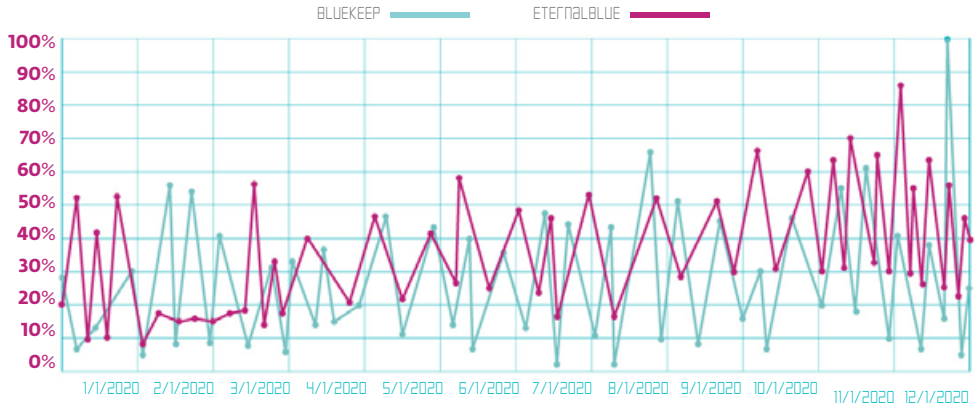

Gráfico 6. *Detecciones BlueKeep y EternalBlue en Latinoamérica (2020). | Fuente: Telemetría de ESET.*

Estas tendencias a la baja tanto de *BlueKeep* como de *EternalBlue* podrían deberse, entre otras razones, a equipos sin actualizaciones que están siendo reemplazados por *hardware* y *software* más reciente. También puede estar asociada a las prácticas de seguridad, ya que como se detalla en la tercera sección de este informe, la práctica de gestión de la seguridad más recurrida por las empresas es la actualización de aplicaciones.

Probablemente, las tendencias expuestas en esta sección del **ESET Security Report 2021** condicionan las preocupaciones de los tomadores de decisiones relacionadas con la ciberseguridad en las empresas latinoamericanas.

INCIDENTES

Los eventos indeseados e inesperados tienen una posibilidad significativa de comprometer las operaciones de las organizaciones y atentar contra la confidencialidad, integridad o disponibilidad de la información.

No es de extrañar que la principal preocupación de los tomadores de decisiones esté relacionada con los códigos maliciosos, cuando el malware se posiciona como la primera causa de incidentes en las empresas latinoamericanas.

Los códigos maliciosos (**34%**) son los principales responsables de los incidentes de seguridad en las empresas de la región, seguidos por los ataques de Ingeniería Social (**20%**) y los accesos no autorizados (**16%**). Por otro lado, **39%** de los participantes afirmaron no haber padecido ningún tipo de incidente de seguridad en sus organizaciones.

LOS CÓDIGOS MALICIOSOS (34%) FUERON LOS PRINCIPALES RESPONSABLES DE LOS INCIDENTES DE SEGURIDAD EN LAS EMPRESAS DE LA REGIÓN, SEGUIDOS POR LOS ATAQUES DE INGENIERÍA SOCIAL (20%) Y LOS ACCESOS NO AUTORIZADOS (16%).

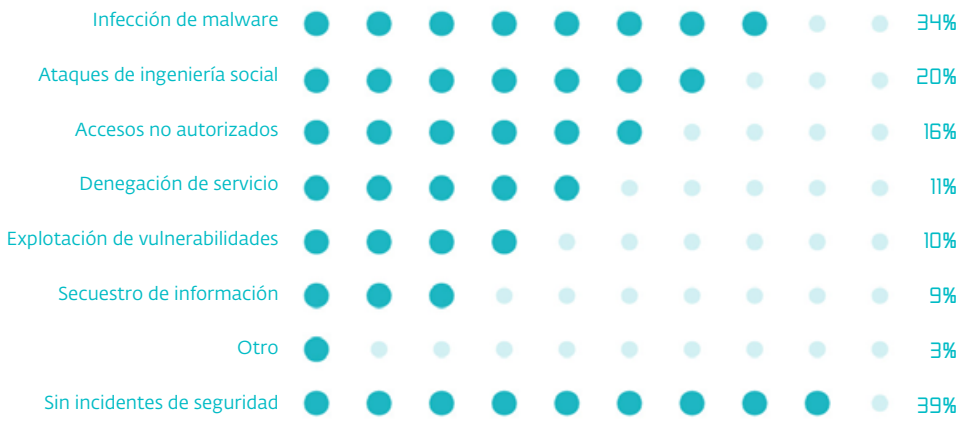

Gráfico 7. *Incidentes de Seguridad de la Información en las empresas de Latinoamérica.*
Fuente: encuestas realizada por ESET a empresas durante 2020.

De acuerdo con la telemetría de ESET, las empresas en Brasil fueron las más afectadas por malware con el **19%** de todas las detecciones en Latinoamérica durante 2020, seguidas por las de México (**17,5%**), Argentina (**13,3%**), Colombia (**10,6%**) y Perú (**8,9%**).

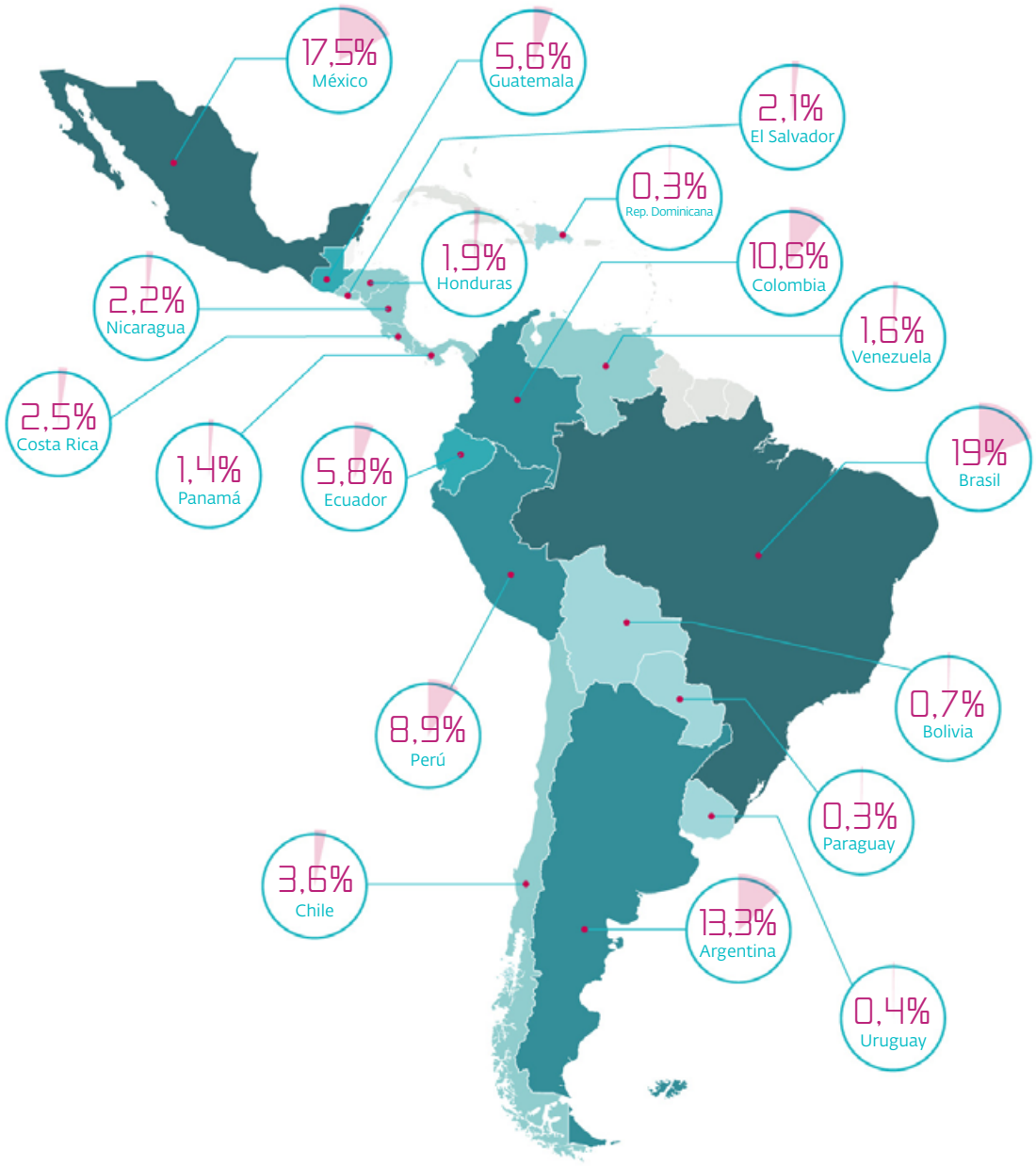

Gráfico 8. *Porcentaje de detección de malware en empresas de Latinoamérica en 2020. | Fuente: Telemetría de ESET.*

Los códigos maliciosos mantienen la primera posición como la causa de incidentes en las empresas de Latinoamérica desde hace algunos años en este informe. Esto puede explicar por qué se trata de la principal preocupación y también se puede entender por las diversas campañas maliciosas que se identifican continuamente en la región.

> Los códigos maliciosos más detectados en Latinoamérica

Las amenazas informáticas crecen en cantidad, complejidad y diversidad, condiciones que con la pandemia incrementaron el riesgo de padecer un incidente de seguridad debido al aumento de la superficie de ataque, una mayor dependencia de los recursos de Internet y la transformación digital. Por ende, también aumentaron las preocupaciones.

En cuanto a la cantidad, los laboratorios de ESET a nivel mundial reciben alrededor de 300 mil nuevas variantes de malware por día, lo que nos brinda una magnitud del problema y del dinamismo de los ciberatacantes. En el caso de dispositivos móviles, se identifican en promedio 300 nuevas muestras de malware para Android cada mes.

Del mismo modo, cada vez se desarrolla malware de mayor complejidad con mecanismos que dificultan su detección y erradicación, que emplean avanzadas técnicas de Ingeniería Social y explotación de vulnerabilidades. La sofisticación considera amenazas modulares, capaces de modificar su comportamiento según las características del sistema objetivo, con mecanismos de protección antianálisis para dificultar su estudio y una gran diversidad en su morfología.

Los grupos de cibercriminales utilizan técnicas novedosas en la ejecución y propagación del malware para lograr ataques cada vez más certeros, como el caso del denominado fileless malware, que tiene la capacidad de ejecutar un código malicioso enteramente desde la memoria del equipo, utilizar herramientas y procesos propios del sistema operativo para ejecutar la actividad maliciosa, sin crear ejecutables adicionales en el sistema.

En lo que a la diversidad se refiere, las distintas familias de códigos maliciosos y sus variantes han evolucionado para afectar un conjunto amplio de dispositivos inteligentes y sistemas operativos.

En el contexto de la principal preocupación de los encargados de la seguridad en las empresas latinoamericanas, es conveniente conocer cuáles son las principales detecciones maliciosas en la región. A continuación, se incluyen las cinco amenazas con mayor porcentaje de detección en Latinoamérica durante 2020 y una breve descripción de cada una de ellas.

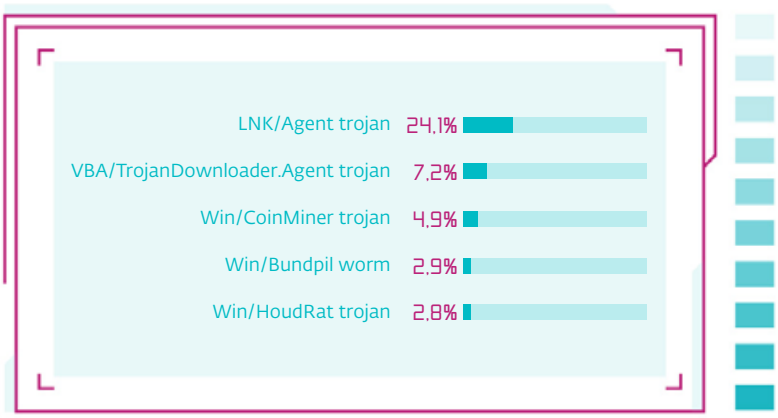

Gráfico 9. *Amenazas más detectadas en Latinoamérica durante 2020. | Fuente: Telemetría de ESET.*

LNK/Agent trojan

LNK/Agent es la detección de un troyano que utiliza archivos de acceso directo LNK de Windows para ejecutar otros archivos en el sistema; han ganado popularidad ya que generalmente son considerados inofensivos. Los archivos LNK/Agent no contienen ninguna carga útil y generalmente son parte de otro malware más complejo. A menudo son utilizados para lograr la persistencia o como parte del vector de compromiso inicial.

VBA/TrojanDownloader.Agent trojan

VBA/TrojanDownloader.Agent es un troyano relacionado con archivos de Microsoft Office que incluyen macros maliciosas. Luego de la ejecución, la macro descarga y ejecuta malware adicional. Los documentos maliciosos regularmente se envían como archivos adjuntos de correo electrónico, disfrazados como información importante para el destinatario, mediante el uso de técnicas de Ingeniería Social.

Win/CoinMiner trojan

Win/CoinMiner es un troyano que utiliza los recursos de hardware de los sistemas infectados para la minería de criptomonedas. Parte de su actividad maliciosa consiste en mantener la persistencia, por lo que crea una copia de sí mismo en el equipo infectado y crea llaves de registro para ejecutarse en cada inicio del sistema. Luego de su instalación, el troyano elimina rastros y recolecta información del sistema para enviarla a un equipo remoto.

Win/Bundpil worm

Win32/Bundpil es un gusano capaz de propagarse a través de medios extraíbles. Es parte de la botnet Wauchos, también conocida como Gamarue o Andrómeda. Bundpil fue diseñado para mejorar la persistencia de la botnet y hacer que sea más difícil realizar una eliminación global de su red. Debido a esto, utiliza Algoritmos de Generación de Dominios (DGA) para crear nombres de dominio casi de forma aleatoria.

Win/HoudRat trojan

Win/HoudRat es un troyano escrito en el lenguaje de scripting AutoIt. Funciona como un RAT (Remote Access Trojan) y es utilizado principalmente para el control de equipos informáticos mediante la creación de una puerta trasera que permite el acceso remoto a los atacantes. HoudRat es utilizado para el robo de información, en especial datos financieros de los usuarios, y se propaga principalmente a través de medios removibles.

> Malware bancario en Latinoamérica y otras regiones

Durante 2020 el malware bancario afectó a varios países de la región latinoamericana, principalmente a Brasil, Mexico, Chile y Argentina. La investigación realizada por el Laboratorio de ESET permitió identificar más de una decena de familias de troyanos bancarios, entre los que se encuentran Amavaldo, Casbaneiro, Grandoreiro, Guildma, Krachulka, Lokorrito, Numando, Mekotio, Mispadu, Vadokrist y Zumanek.

Las campañas de estos bankers son completamente focalizadas mediante la suplantación de reconocidas empresas que operan en los países en cuestión. Por ejemplo, más del **75%** de las detecciones de Mekotio se registraron en Chile y Argentina, mientras que más del **85%** de los registros de Amavaldo, Casbaneiro y Mispadu ocurrieron en México y Brasil.

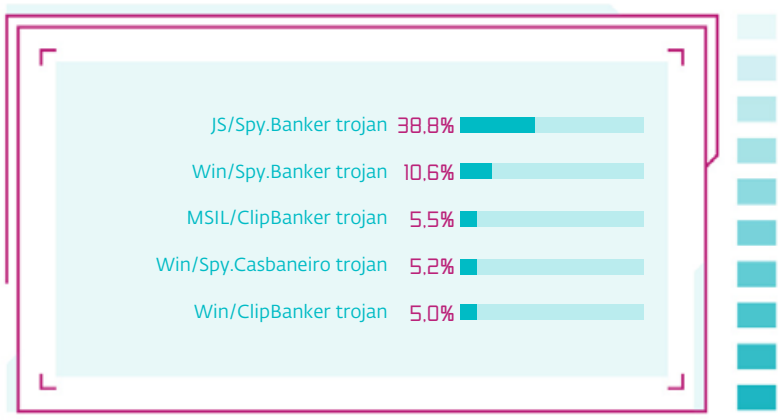

Gráfico 10. *Troyanos bancarios más detectadas en Latinoamérica durante 2020. | Fuente: Telemetría de ESET.*

En 2020 los troyanos bancarios identificados inicialmente en Latinoamérica han comenzado a distribuirse en Europa, afectando principalmente a España, aunque también se detectaron campañas en Francia, Bélgica, Italia y otros países europeos. Del mismo modo, Estados Unidos también se convirtió en un blanco para muchas de estas familias de malware bancario que son más comunes en América Latina.

En los últimos meses se ha identificado un decremento gradual en las detecciones del malware bancario, probablemente como consecuencia de otro tipo de actividad maliciosa como el ransomware que provee un mayor retorno de inversión a sus desarrolladores.

Otra razón que puede influir en esta tendencia a la baja puede ser la disrupción de algunos códigos maliciosos, como es el caso de TrickBot, utilizado por sus operadores principalmente como un troyano bancario para el robo credenciales de cuentas bancarias y recientemente utilizado para realizar ataques más dañinos, como distribuir ransomware.

Para disrumpir la actividad maliciosa de Trickbot ESET proporcionó análisis técnico, información estadística, nombres de dominio y direcciones IP de servidores de comando y control. Tan solo en 2020, ESET analizó más de **125.000** muestras maliciosas y descifró más de **40.000** archivos de configuración utilizados por Trickbot.

EN LOS ÚLTIMOS MESES SE IDENTIFICÓ UN DECREMENTO GRADUAL EN LAS DETECCIONES DEL MALWARE BANCARIO, TAL VEZ DEBIDO A OTRO TIPO DE ACTIVIDAD MALICIOSA COMO EL RANSOMWARE QUE PROVEE UN MAYOR RETORNO DE INVERSIÓN A LOS CRIMINALES.

> Cryptominers y la fiebre por las criptomonedas

La fiebre por las criptomonedas reaparece después de una tendencia a la baja en el número de detecciones de cryptominers (malware creado para la minería de criptomonedas), que registraban una caída constante desde 2018, una racha que se rompió en el último trimestre de 2020.

Este cambió probablemente se debió al aumento en el valor del Bitcoin y de otras divisas digitales como Ethereum o Monero. Además, durante 2020 aumentó la cantidad de ataques de ransomware dirigidos que demandaban el pago de un rescate en criptomonedas; lo cual en más de un caso provocó que las víctimas eligieran la opción de pagar y se vieran obligadas a adquirir criptomonedas.

Gráfico 11. *Tendencias de detecciones de cryptominers en Latinoamérica (2020) | Fuente: Telemetría de ESET.*

Por estas razones, no es de extrañar la proliferación de las amenazas informáticas en torno a minería de criptomonedas. En 2020, el país con mayor actividad maliciosa relacionada con la criptominería fue Tailandia con el **17,9%** de todas las detecciones, seguido por dos países latinoamericanos, Perú (**10,1%**) y Ecuador (**5,1%**).

El año pasado, ESET disrumpió la actividad de la botnet VictoryGate utilizada para minar criptomonedas, que afectó principalmente a Perú. La botnet estaba conformada por alrededor de **35.000** equipos ubicados en Latinoamérica, donde más del 90% de los dispositivos comprometidos se localizaban en territorio peruano.

> Ingeniería Social en torno a las vacunas y el COVID-19

Las campañas de Ingeniería Social durante 2020 utilizaron con frecuencia la pandemia como señuelo. Diversas campañas de phishing aparecieron para suplantar reconocidas empresas, donde se ofrecían supuestos obsequios como cubrebocas o artículos deportivos, e incluso instituciones de gobierno de diversos países fueron afectadas al ser utilizado su nombre para engañar a los usuarios con aparentes programas de ayuda social, para mencionar algunos ejemplos.

En los últimos meses del año pasado y primeros meses de 2021, las campañas engañosas continuaron haciendo alusión al coronavirus, pero ahora enfocadas principalmente a estafas relacionadas con las vacunas contra el COVID-19. Este tipo de engaños se registró en varios países de América Latina y del mundo.

Debido al teletrabajo y la manera en la que se emplean las computadoras, tanto para fines laborales como personales, un incidente de seguridad que antes solamente tenía repercusiones personales para los colaboradores ahora podría tener un impacto negativo para las organizaciones y viceversa.

Por ejemplo, en México aparecieron publicaciones a través de redes sociales y falsos sitios que intentaban engañar a los usuarios con la venta de vacunas de Pfizer, Moderna o AstraZeneca, al igual que estafas relacionadas con la venta de tanques de oxígeno en los momentos más críticos de la pandemia.

En Colombia circularon estafas a través de mensajes SMS ofreciendo turnos prioritarios para la aplicación de las vacunas a cambio de dinero; en Honduras circularon mensajes a través de WhatsApp en los que se anunciaba la venta de la vacuna Sputnik V; mientras que en Argentina se reportaron casos de estafas telefónicas dirigidas a adultos mayores para acceder a la vacuna.

El impacto de este tipo de engaños es cada vez mayor, ya que representan un daño patrimonial debido a que no hay garantía de obtener la vacuna una vez que se realice el pago; en el remoto caso de que se logre obtener el producto, implica un riesgo a la salud debido a la dudosa procedencia de las supuestas vacunas.

El caso más representativo de la Ingeniería Social es el phishing, una amenaza comúnmente utilizada para el robo de información sensible. De acuerdo con los datos de la telemetría de ESET, las empresas en Brasil fueron las más afectadas por casos de phishing con el **26,4%** de todas las detecciones en Latinoamérica durante 2020, seguidas por las de Perú (**22,8%**), México (**12%**), Colombia (**9,1%**) y Argentina (**7,1%**).

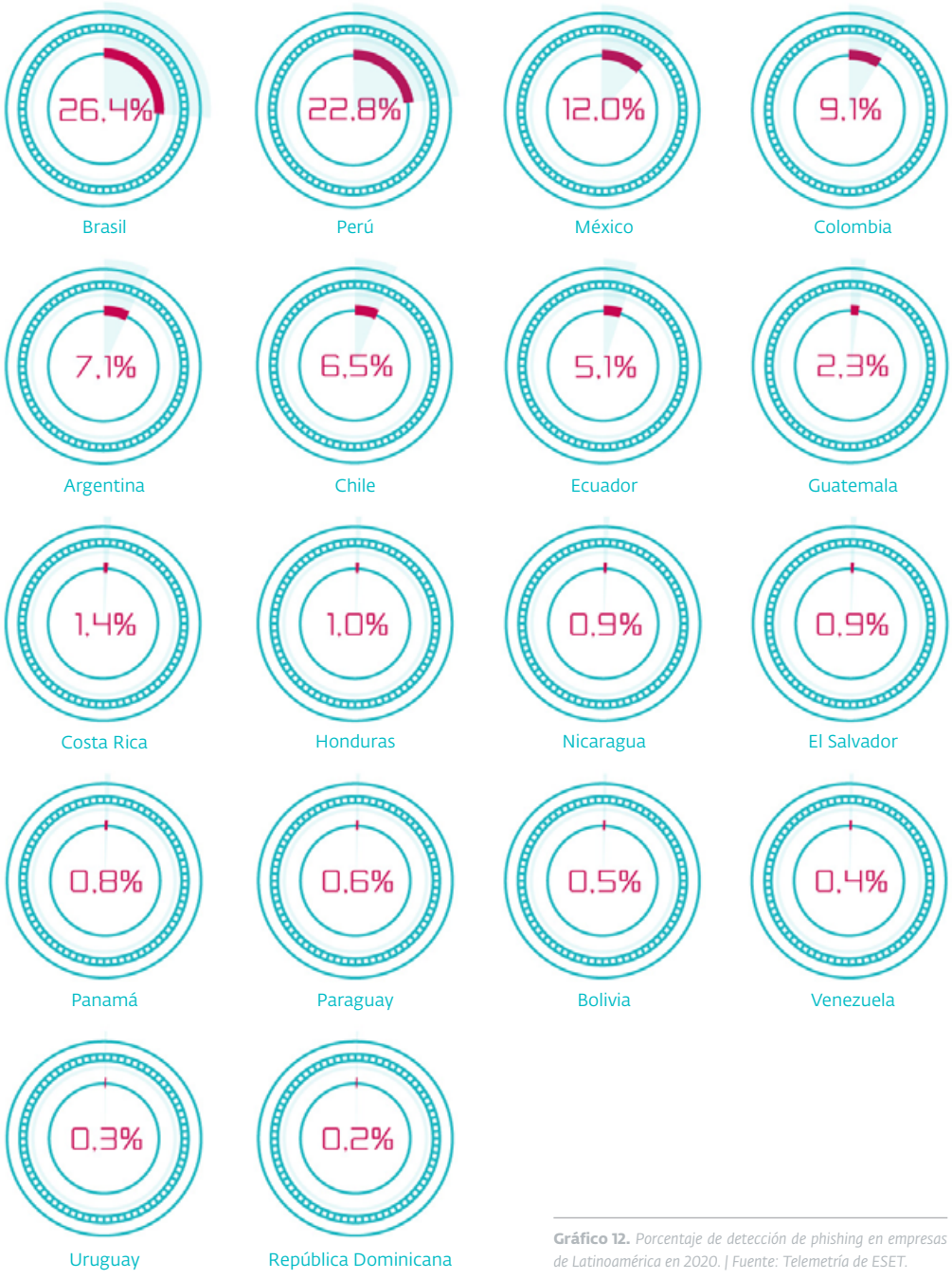

Gráfico 12. *Porcentaje de detección de phishing en empresas de Latinoamérica en 2020. | Fuente: Telemetría de ESET.*

En la encuesta realizada en junio del 2020 sobre ciberseguridad en tiempos de pandemia a usuarios de ESET, el **44,2%** afirmó haber recibido correos de phishing que utilizaban el COVID-19 como anzuelo para llevar adelante el engaño, lo que sustenta la cantidad de campañas de phishing que circulan en torno a la pandemia.

SEGÚN DATOS DE UNA ENCUESTA REALIZADA POR ESET EN 2020, EL 44% DE LOS USUARIOS AFIRMÓ HABER RECIBIDO CORREOS DE PHISHING QUE UTILIZABAN EL TEMA DEL COVID-19 COMO ANZUELO.

CONTROLES

Con frecuencia los recursos asignados para la implementación de controles de seguridad e iniciativas orientadas a mejorar y aumentar las medidas de protección son el resultado de los análisis relacionados con las preocupaciones e incidentes de seguridad, que al mismo tiempo pueden estar acompañados de evaluaciones de riesgos.

El objetivo de los controles es la mitigación de riesgos, ya sea mediante la reducción de la probabilidad de ocurrencia, o la disminución de su impacto; en el mejor de los casos se puede incidir sobre ambas variables.

> Soluciones de seguridad tecnológicas en la pandemia

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

Con base en el resultado de las encuestas, los principales controles de seguridad implementados en las empresas son las soluciones antimalware (**86%**), firewalls (**75%**) y soluciones de respaldo de información (**68%**).

LAS SOLUCIONES ANTIMALWARE (86%) REPRESENTAN EL PRINCIPAL CONTROL DE SEGURIDAD QUE IMPLEMENTAN LAS EMPRESAS DE LA REGIÓN, SEGUIDO POR FIREWALLS (75%) Y SOLUCIONES DE RESPALDO DE INFORMACIÓN (68%).

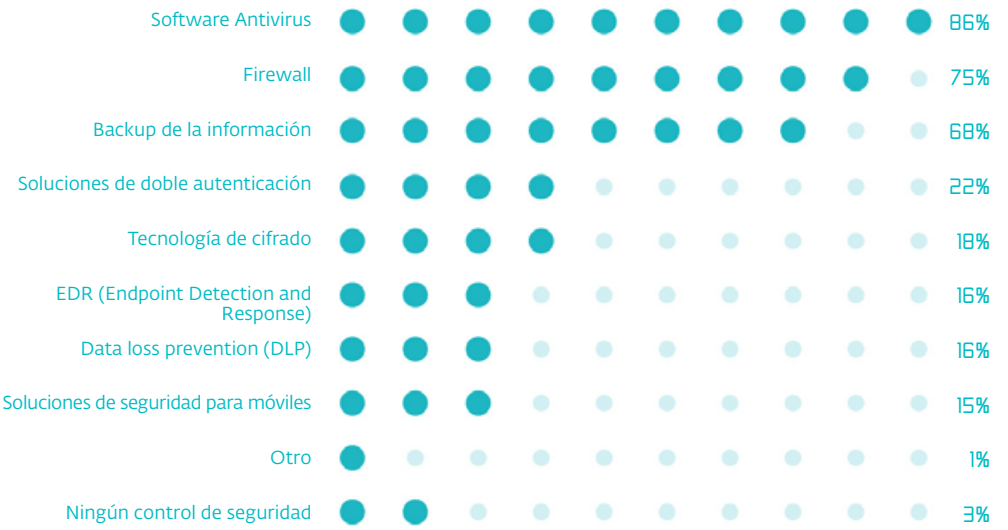

Gráfico 13. *Controles de seguridad tecnológicos utilizados en las empresas de la región. | Fuente: encuestas a empresas realizada por ESET en 2020.*

Resulta lógico que el control tecnológico más utilizado en las empresas de la región sean las soluciones antimalware (**86%**), en condiciones donde los endpoints requieren estar protegidos fuera de las redes corporativas y en un ambiente donde el perímetro es practicamente inexistente en la actualidad.

Del mismo modo, resulta interesante que los firewalls se mantengan como una de las herramientas de seguridad más utilizadas en la actualidad, probablemente debido a los modelos tradicionales de seguridad que se han mantenido a lo largo de los años y su continua evolución, o quizá por la aplicación del principio de protección brindado por este tipo de herramientas, que además de implementarse a nivel de red para proteger el perímetro, también son aplicados a nivel de host o Web Application Firewall (WAF).

Por otro lado, el porcentaje de empresas que utilizan una solución y procedimientos de respaldos de información podría considerarse relativamente bajo, sobre todo por la cantidad de incidentes de ransomware identificados en los últimos años u otras amenazas que atentan contra la disponibilidad o la integridad de la información. A pesar de mantener una tendencia al alza en las últimas ediciones del ESET Security Report: 2019 (**63%**), 2020 (**64%**) y 2021 (**68%**), todavía existe una brecha importante por reducir.

Sin embargo, otras soluciones que podrían contribuir a este control de la información en un ambiente poco controlado u hostil, no son ampliamente utilizados. Es el caso de las tecnologías de cifrado con solo el **18%** de aplicación entre los encuestados, o el **16%** de soluciones DLP. Se destaca también el bajo porcentaje de las empresas que utilizan controles de seguridad en los dispositivos móviles (**15%**), dado que en la actualidad muchos de estos aparatos son utilizados para actividades laborales y se maneja información cada vez más sensible desde los teléfonos inteligentes.

SOLO EL 15% DE LAS EMPRESAS IMPLEMENTAN CONTROLES DE SEGURIDAD EN LOS DISPOSITIVOS MÓVILES

En el estudio realizado por ESET sobre la ciberseguridad en tiempos de COVID-19, los datos demuestran también que las herramientas de seguridad que más proporcionaron las empresas fueron las soluciones antimalware (**32%**) seguida por las conexiones VPN (**20%**), soluciones de cifrado de información (**13%**) y soluciones de doble factor de autenticación (**8%**).

> Prácticas de gestión de seguridad durante el confinamiento

Según los datos de la encuesta realizada por ESET a empresas de la región en 2020 la actualización de aplicaciones (**71%**) es la práctica de gestión de la seguridad más adoptada, seguida por la implementación de políticas de seguridad (**68%**) y la realización de auditorías (**40%**), tanto internas como externas.

LA ACTUALIZACIÓN DE APLICACIONES (71%) ES LA PRÁCTICA DE GESTIÓN DE LA SEGURIDAD MÁS ADOPTADA, SEGUIDA POR LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD (68%) Y LA REALIZACIÓN DE AUDITORÍAS (40%), TANTO INTERNAS COMO EXTERNAS.

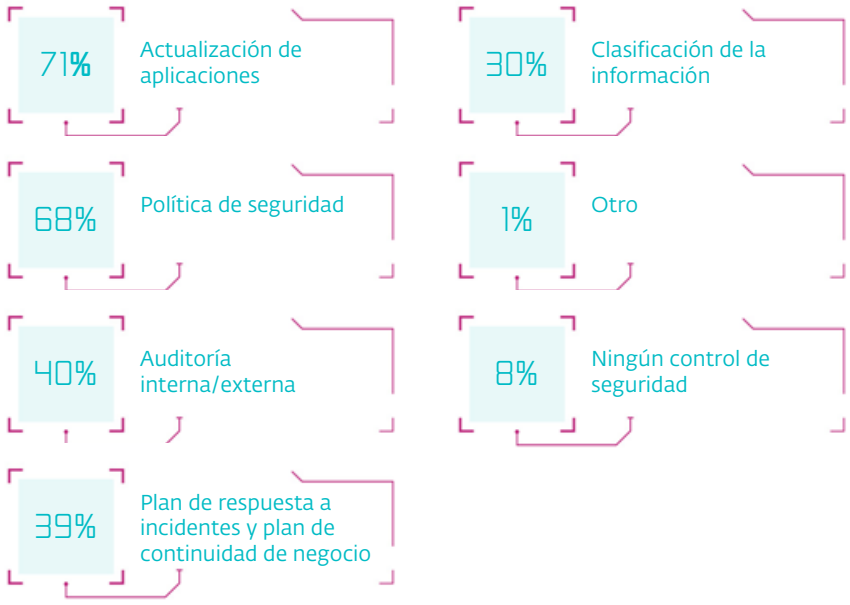

Gráfico 14. *Prácticas de gestión aplicadas en las empresas de Latinoamérica. Fuente: encuestas a empresas realizada por ESET en 2020.*

Vale la pena mencionar que el **8%** de los participantes en esta encuesta afirmó no implementar ninguna práctica de gestión de la seguridad. Esto puede resultar contraproducente, ya que la seguridad no puede limitarse solo a los controles de índole tecnológico, requiere la combinación e integración de controles administrativos, físicos y técnicos.

> Inversión en ciberseguridad, una necesidad en el corto plazo

De forma paralela a la crisis sanitaria, también se padece una crisis económica como resultado de los confinamientos, lo que lamentablemente aumenta las adversidades para las empresas. En un campo como el de la seguridad de la información que presenta muchos desafíos, el presupuesto con el que cuentan las organizaciones resulta fundamental para lograr sus objetivos, mismo que en ocasiones no es suficiente.

De los encuestados para el ESR 2021, el **63%** manifestó conocer el presupuesto asignado para el área de ciberseguridad, contra el **37%** que desconoce esta información. Del grupo de encuestados que conocen los recursos que le son asignados, solo el **19%** lo consideró suficiente; un porcentaje bajo si se toma en cuenta el ambiente adverso que enfrentas las organizaciones a raíz de la pandemia.

Por otro lado, del conjunto de entrevistados que afirmaron conocer los recursos asignados al área de seguridad, el **44,4%** indicó que el presupuesto se mantuvo con respecto al año anterior, **24%** que aumentó, mientras que el **22,5%** afirmó que se redujo.

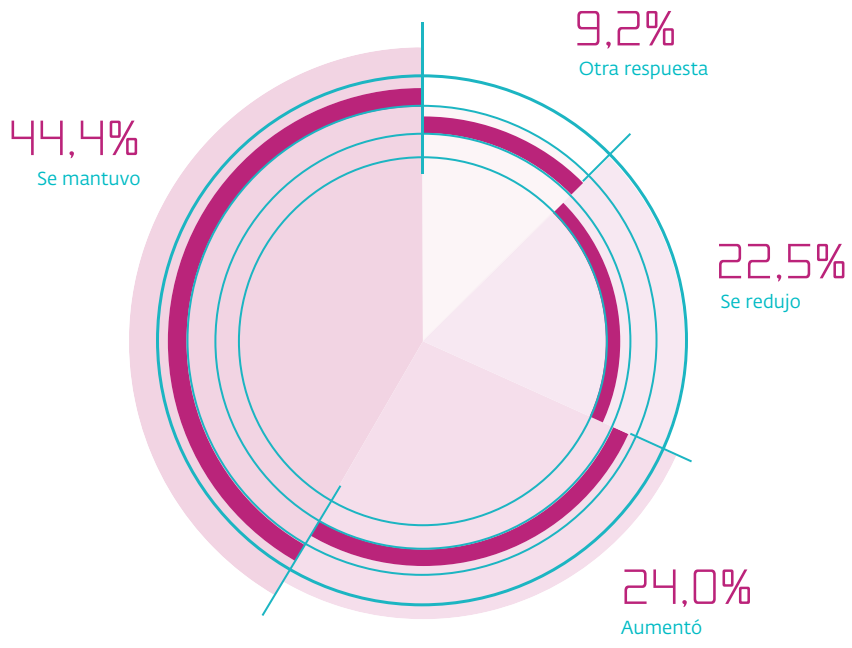

Gráfico 15. *Variación del presupuesto de seguridad para las empresas.*
Fuente: encuestas a empresas realizada por ESET en 2020.

Si lo observamos desde otra perspectiva, para el **76%** de los participantes se mantuvo, se redujo o desconocen si hubo alguna variación en el presupuesto asignado para sus labores. Del mismo modo, el **81%** de los encuestados considera insufi-

ciente los recursos destinados a seguridad para cumplir con sus objetivos. Estos resultados se condicen con otros estudios que realizó ESET durante la pandemia y muestran la necesidad de aumentar los presupuestos para las áreas de seguridad. De acuerdo con el informe global titulado Cyberchology: The Human Element, uno de los principales desafíos que reportaron las organizaciones durante el confinamiento por COVID-19 está relacionado con la falta de presupuesto para el área de seguridad. Según la encuesta realizada para este informe, el **46%** de los participantes manifestó la necesidad de mayores inversiones en seguridad para el corto plazo, aunado a las necesidades que con conllevan el trabajo remoto.

EL 81% DE LOS ENCUESTADOS CONSIDERA INSUFICIENTE LOS RECURSOS DESTINADOS A SEGURIDAD PARA CUMPLIR CON SUS OBJETIVOS.

> Educación y concientización: factores clave para la seguridad

Entre tantas consecuencias negativas que provocó la pandemia es posible destacar como aspecto positivo que se han mantenido las actividades de educación y concientización en materia de seguridad.

De acuerdo con las respuestas para el ESR 2021, **37%** de los participantes afirmó realizar actividades de educación o concientización de forma periódica, mientras que **41%** lo realiza de manera ocasional. Un **19%** no realiza este tipo de acciones, lo que podría resultar contraproducente en el contexto actual.

EL 37% DE LAS EMPRESAS REALIZA ACTIVIDADES DE EDUCACIÓN O CONCIENTIZACIÓN DE FORMA PERIÓDICA, MIENTRAS QUE 41% LO REALIZA DE MANERA OCASIONAL.

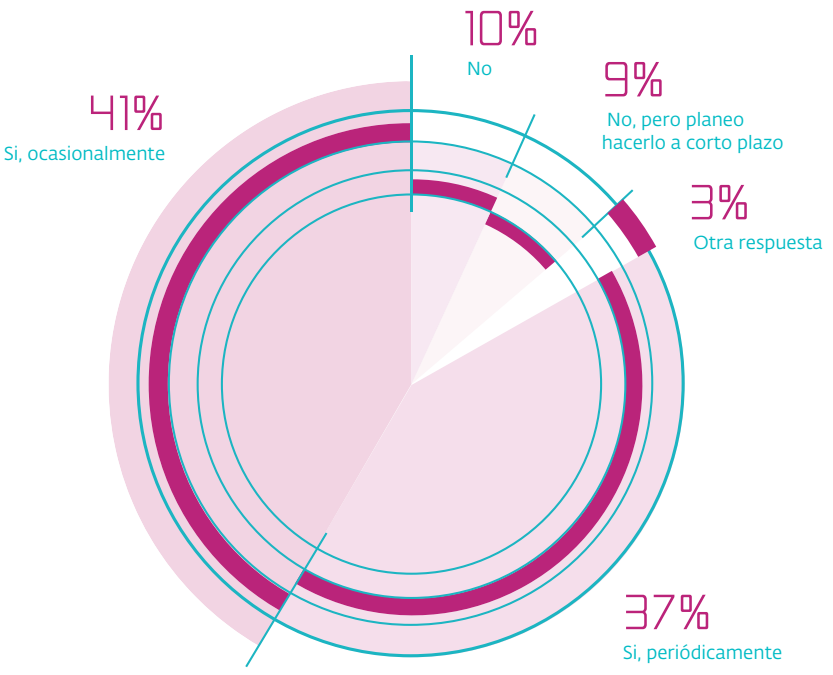

Gráfico 16. *Actividades de concientización en las empresas latinoamericanas. Fuente: encuestas a empresas realizada por ESET en 2020.*

La encuesta realizada por ESET en 2020 identificó que la gran mayoría de los consultados (**95%**) consideró útil o necesaria la realización de capacitaciones de seguridad informática especialmente ligadas al teletrabajo, lo que demuestra la conciencia adquirida por los colaboradores en torno la ciberseguridad durante este período.

De hecho, otro relevamiento realizado por ESET en noviembre del 2020 sobre ciberseguridad y teletrabajo da cuenta del cambio de perspectiva sobre la importancia de estar capacitado en seguridad, ya que casi el **90%** de los participantes considera que el aumento del teletrabajo supone una oportunidad para los cibercriminales y opina que las empresas deberían cambiar su enfoque de seguridad de acuerdo a esta ralidad. De forma contraria, solo el **20%** afirmó haber recibido capacitaciones en el ámbito laboral sobre configuraciones seguras y buenas prácticas de teletrabajo.

La capacitación y concientización resultan elementos clave para reducir los incidentes de seguridad en las organizaciones. Con frecuencia suele calificarse a los usuarios como "el eslabón más débil" en el ámbito de la ciberseguridad, un adjetivo que podría resultar cierto si se consideran la cantidad de amenazas informáticas orientadas a "explotar vulnerabilidades en las personas", principalmente mediante el uso de Ingeniería Social, donde el ejemplo más representativo es el phishing.

Los usuarios informados y capacitados tienen más herramientas para tomar mejores decisiones. Esto es clave en estos tiempos de teletrabajo y con la gran cantidad de campañas maliciosas que, como vimos anteriormente, aprovechan temas relacionados con la pandemia.

CONCLUSIÓN

La vida cambió radicalmente de un año a otro, en prácticamente todos los aspectos. De forma repentina, las preocupaciones de distinta índole aparecieron, principalmente relacionados con la salud, el trabajo y la economía. A estas condiciones, también se sumó el estrés provocado por los ciberataques. Las afectaciones han sido de toda índole y a todos niveles.

Entre tantos cambios es importante destacar que la pandemia se convirtió en un catalizador que impulsó la transformación digital en casi todas las industrias, sobre todo por la mayor dependencia de la tecnología para realizar actividades cotidianas.

Los hábitos personales también han cambiado. Por ejemplo, el uso de de los dispositivos electrónicos ha aumentado desde el comienzo del aislamiento social, las compras en línea han tenido un crecimiento considerables y, por supuesto, no se pueden dejar de lado las actividades como el teletrabajo, la educación a distancia o el entretenimiento en línea.

Lamentablemente han emergido más amenazas informáticas y otras se han consolidado afectando tanto a usuarios como empresas e incluso gobiernos. Tal es el caso del malware y phishing, que han aprovechado el tema del COVID-19 para sus campañas, así como las noticias falsas que circulan por Internet y las estafas que casi a diario se distribuyen a través del correo electrónico, redes sociales o aplicaciones de mensajería.

Por ello, la ciberseguridad se ha convertido en una de las consideraciones más importantes para cualquier negocio moderno, donde la mayoría de las organizaciones permanecen en línea de algún modo y donde la tecnología es un elemento clave para sus operaciones.

Las consideraciones que de forma cotidiana se realizaban, resultan más vigentes y necesarias que nunca, como mantener la seguridad y visibilidad en los equipos que se encuentran fuera de la red corporativa, llevar a cabo la actualización de los sistemas para mitigar las amenazas conocidas y

emergentes, así como la concientización y educación de los colaboradores.

Las prácticas de gestión de la seguridad de las empresas han comenzado a colarse poco a poco en las actividades cotidianas que realizan los colaboradores en sus hogares para proteger la información. La delgada línea que separaba la seguridad corporativa de la hogareña se fue difuminando, dejando de manifiesto que la seguridad es esencial y que nos debe acompañar en cualquier lugar y a todo momento.

Es importante destacar que, ante una infección con ransomware, la posibilidad de recuperar la información y la forma de hacerlo dependerá del tipo de amenaza específica.

En general, ante un ransomware del tipo lockscreen es posible recuperar el acceso al sistema limpiando la infección o restaurando el equipo. Además, en estos casos, si los archivos no son cifrados es posible recuperarlos del disco afectado. Sin embargo, en algunas variantes, especialmente aquellas que afectan dispositivos móviles, el bloqueo no permite la recuperación del equipo, por lo que la única solución terminará siendo un reseteo de fábrica, borrando toda la información.

En el caso de los ransomware del tipo filecoder la recuperación puede ser más complicada. Si bien en la mayoría de los casos un buen software de seguridad tendría que ser capaz de quitar el ransomware del equipo, los archivos seguirán cifrados. Con algunas familias de ransomware, especialmente las que utilizan el cifrado simétrico y guardan la clave dentro del código malicioso, es posible recuperar los archivos utilizando la herramienta específica de descifrado. Sin embargo, los archivos que fueron afectados por un tipo más sofisticado de ransomware, como Cryptolocker, son imposibles de descifrar sin la clave correcta.

En cualquier caso, si ocurre una infección es recomendable limpiar el equipo de la infección, ya sea utilizando una herramienta de seguridad o reinstalando el sistema, y luego recuperar la información y los archivos mediante un respaldo limpio.

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