SECURITY REPORT
LATINOAMÉRICA 2024

12 datos
sobre el estado de la ciberseguridad de las empresas de América Latina

ESET Digital Security
Progress. Protected.

20 AÑOS
ESET LATAM

Acerca de ESET Security Report

El **ESET Security Report** (ESR) es un informe anual elaborado por ESET que ofrece una visión general del estado de la seguridad en las empresas de América Latina.

Este documento se elaboró en base a encuestas realizadas a 2141 profesionales que trabajan en organizaciones de diversas industrias y en más de diez países de América Latina, mayormente profesionales que ocupan cargos en el sector TI o vinculados a la seguridad.

Además, el ESR 2024 complementa esta información con datos extraídos de la telemetría de ESET para el año 2023, lo que permite contextualizar la percepción de los encuestados con respecto a la actividad maliciosa detectada por ESET durante el último año en América Latina.

A través de la selección de los datos más relevantes de la encuesta, el informe ofrece una visión a nivel regional sobre la seguridad de las empresas, sin profundizar en situaciones específicas, y aborda temas como la cantidad de incidentes de seguridad que sufrieron las empresas; las amenazas más activas durante el último año; el estado del ransomware en la región; el grado de satisfacción con el presupuesto asignado a ciberseguridad; las prácticas de gestión más adoptadas; las preocupaciones en ciberseguridad en las empresas y las medidas de seguridad más adoptadas.

Esperamos que este informe proporcione una perspectiva sobre el estado de la seguridad de la información a nivel corporativo y contribuya a mejorar la conciencia sobre la importancia de la ciberseguridad para las empresas de la región.

Incidentes de seguridad

30%

de las organizaciones sufrió al menos un incidente de seguridad en 2023

Además, 1 de cada 5 empresas en América Latina que afirmaron no haber experimentado incidentes de seguridad durante el último año manifestaron que no disponen de la tecnología necesaria para asegurar que no sufrieron incidentes. Esto sugiere que existe un porcentaje de empresas que posiblemente hayan sido blanco de ataques, pero que no los registraron.

Los sectores que más intentos de ataque recibieron fueron Organismos de Gobierno, Informática/Tecnología, Banca/Finanzas.

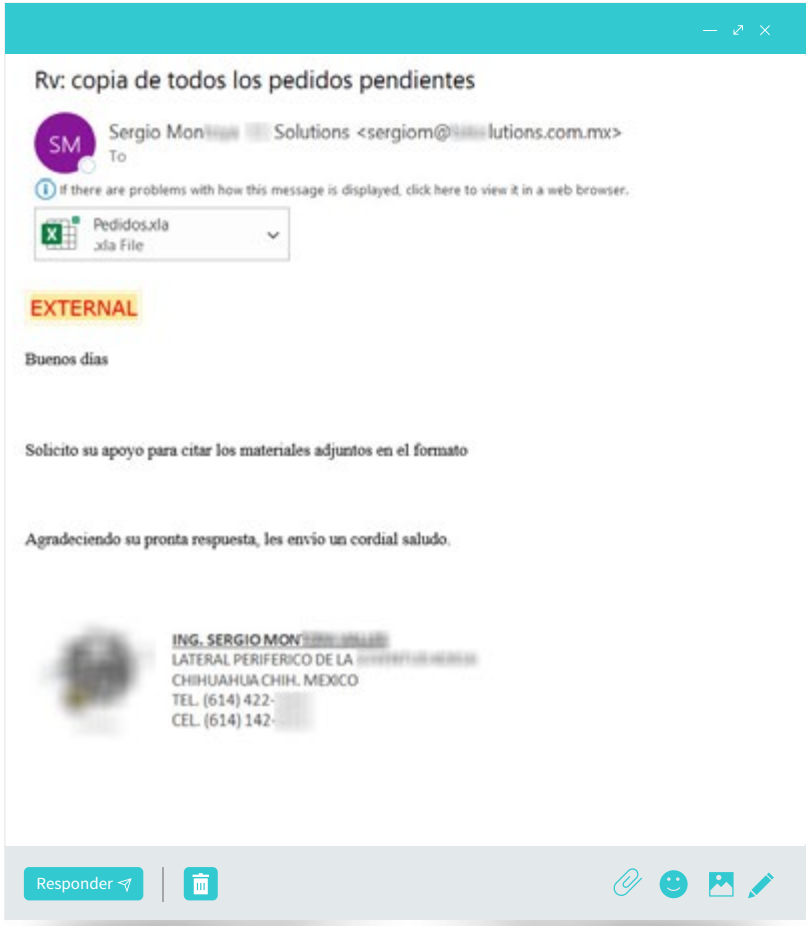
¿Cuáles fueron las amenazas más comunes en América Latina durante 2023?

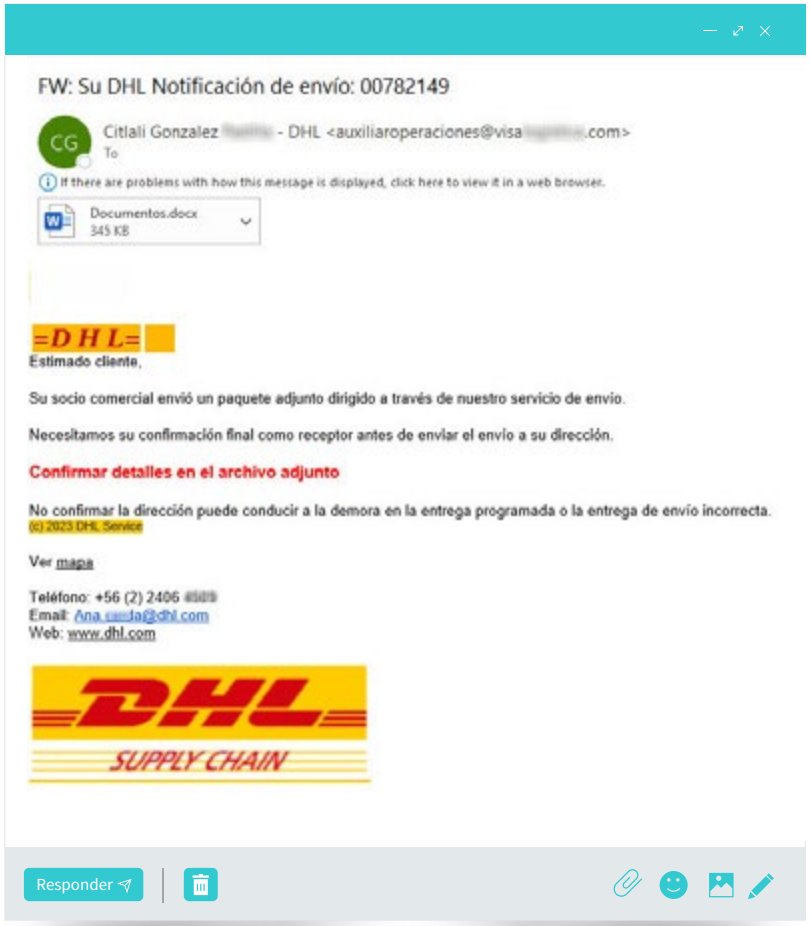
Si repasamos los datos de la telemetría de ESET y agrupamos el total de las detecciones maliciosas registradas por ESET en 2023 para América Latina, observamos que el código malicioso con más detecciones corresponde a un **exploit** para la vulnerabilidad **CVE-2017-11882** en Microsoft Office.

Si bien esta vulnerabilidad fue parcheada hace ya siete años, sigue siendo utilizada en campañas que buscan distribuir malware en la región a través del correo electrónico. En un artículo publicado en WeLiveSecurity compartimos algunos **ejemplos de correos** que circularon en 2023 con documentos de Microsoft como archivos adjuntos y que utilizaron técnicas de suplantación de identidad como el **email spoofing**.

Estas campañas se registraron de manera sostenida y en muchos casos propagaban malware multipropósito, como Troyanos de Acceso Remoto (RAT, por sus siglas en inglés) como Agent Tesla, el que hemos analizado en este **artículo**.

Ejemplos de correos que distribuyen malware en América Latina explotando vulnerabilidades de larga data en Microsoft Office





FW: Su DHL Notificación de envío: 00782149

CG Citlali Gonzalez - DHL <auxiliaroperaciones@visa.com>
To

If there are problems with how this message is displayed, click here to view it in a web browser.

Documentos.docx
345 KB

=DHL=

Estimado cliente,

Su socio comercial envió un paquete adjunto dirigido a través de nuestro servicio de envio.

Necesitamos su confirmación final como receptor antes de enviar el envío a su dirección.

Confirmar detalles en el archivo adjunto

No confirmar la dirección puede conducir a la demora en la entrega programada o la entrega de envío incorrecta.
(c) 2023 DHL Service

Ver mapa

Teléfono: +56 (2) 2406
Email: Ana.
Web: www.dhl.com

DHL SUPPLY CHAIN

Responder

Re: copia de todos los pedidos pendientes

V Ventas <ventas2@mex.com.mx>
To

If there are problems with how this message is displayed, click here to view it in a web browser.

Pedidos.xls
268 KB

Buenos días

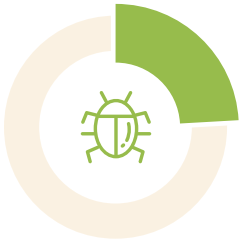
Solicito su apoyo para citar los materiales adjuntos en el formato

Agradeciendo su pronta respuesta, les envío un cordial saludo.

Luisa Mor
MEX, S.A. de C.V.
Tels: 01 (81) 83-77- EXT. 103
Correo: ventas2@mex.com.mx

Responder

Los Troyanos de Acceso Remoto (RAT) más activos en LATAM



Trojan.Win32/Ramnit

766869

Ramnit (24,1%)

Ramnit (también conocido como Nimnul) es un troyano de acceso remoto (RAT) que se propaga principalmente a través de archivos ejecutables y documentos de Office maliciosos. Puede robar información, registrar pulsaciones de teclas y permitir a los atacantes controlar remotamente el sistema infectado.

Backdoor.Win32/Rescoms

459604

Rescoms (14,4%)

Rescoms, también conocido como Remcos, Remvio o Socmer, es un RAT que se ha utilizado en campañas de espionaje cibernético. Puede recopilar información sensible, tomar capturas de pantalla y controlar la cámara y el micrófono del dispositivo infectado.

Worm.Win32/Bundpil

215061

Bundpil (6,7%)

Bundpil es un RAT que se propaga principalmente a través de archivos adjuntos de correo electrónico maliciosos. Puede robar credenciales, registrar pulsaciones de teclas y permitir a los atacantes controlar el sistema afectado.

Worm.Win32/Phorpiex

198158

Phorpiex (6,2%)

Phorpiex (también conocido como Trik) es un RAT que se propaga a través de correos electrónicos de spam y descargas de archivos maliciosos. Puede robar información, propagarse a otros dispositivos y realizar ataques DDoS.

Backdoor.Win32/RanumBot

121006

RanumBot (3,6%)

RanumBot es un RAT que se propaga principalmente a través de archivos adjuntos de correo electrónico y enlaces maliciosos. Puede robar información, registrar pulsaciones de teclas y permitir a los atacantes controlar el sistema afectado.

81% de los ataques con exploits apuntó a vulnerabilidades antiguas en Office

Las campañas de *malspam* utilizando exploits con mayor cantidad de detecciones en América Latina durante 2023 apuntaron a dos vulnerabilidades de Microsoft Office descubiertas hace ya varios años y para las cuales existe un parche disponible, como son la CVE-2017-11882 (45%) y la CVE-2012-0143 (36%).

Estas dos vulnerabilidades representan el 81% de las detecciones de exploits y están asociadas a campañas masivas que se propagan a través del correo electrónico como archivos adjuntos.

Cuáles fueron las vulnerabilidades más explotadas

La CVE-2017-11882 es una vulnerabilidad en el editor de ecuaciones de Microsoft Office. El uso de exploits podría permitir que un atacante ejecute código arbitrario en la computadora vulnerable.

La CVE-2012-0143 afecta principalmente a Microsoft Excel 2003 SP3. Esta vulnerabilidad ocurre porque Excel no maneja adecuadamente la memoria al abrir archivos. Este error es aprovechado a través de exploits que se usan para permitir la ejecución de código arbitrario mediante una hoja de cálculo especialmente diseñada para ser maliciosa.

Estos tipos de exploits pueden instalar otras familias de malware o incluso tomar control total del sistema, especialmente si el perfil del usuario tiene permisos de administrador.

El restante 20% de las detecciones se reparte entre las siguientes vulnerabilidades:

LNK/Exploit.CVE-2010-2568
82281

Win32/Exploit.CVE-2017-0199
51451

Win32/Exploit.CVE-2012-0159
32052

JS/Exploit.CVE-2021-26855
24781

Win32/Exploit.CVE-2023-21716
17862

Otras vulnerabilidades destacadas:

CVE-2010-2568

- **Descripción:** Esta vulnerabilidad afecta a Microsoft Windows y Microsoft Windows Server. Permite a un atacante local o remoto ejecutar código arbitrario a través de archivos de acceso directo (.LNK o .PIF) maliciosos.
- **Impacto:** Puede resultar en la ejecución de código no autorizado en el sistema afectado.

CVE-2017-0199

- **Descripción:** Esta vulnerabilidad afecta a Microsoft Word. Permite a los atacantes descargar y ejecutar scripts de PowerShell en máquinas comprometidas.
- **Impacto:** Proporciona acceso adicional a los atacantes.

CVE-2012-0159

- **Descripción:** Esta vulnerabilidad afecta a varios productos de Microsoft, incluyendo Windows, Office y Silverlight. Permite a atacantes remotos ejecutar código arbitrario a través de archivos de fuente TrueType (TTF) manipulados.
- **Impacto:** Puede resultar en la ejecución de código no autorizado en el sistema afectado.

CVE-2021-26855

- **Descripción:** Esta vulnerabilidad afecta a Microsoft Exchange Server. Permite a los atacantes autenticarse como el servidor Exchange y enviar solicitudes HTTP arbitrarias.
- **Impacto:** Puede resultar en la ejecución remota de código en el servidor Exchange.

CVE-2023-21716

- **Descripción:** Esta vulnerabilidad afecta a Microsoft Word. Permite a los atacantes ejecutar código remoto con los privilegios de la víctima al abrir un documento RTF malicioso.
- **Impacto:** Proporciona acceso no autorizado al sistema.

¿Qué pasa con la explotación de vulnerabilidades más recientes?

Es lógico que los atacantes exploten en mayor medida vulnerabilidades viejas para comprometer la seguridad de usuarios y empresas en Latinoamérica. Sin embargo, los datos de la telemetría de ESET indican que también existen detecciones para vulnerabilidades más recientes. Esto muestra que el negocio del cibercrimen está compuesto por un ecosistema heterogéneo de actores maliciosos dispuestos a aprovechar el amplio espectro de vulnerabilidades existentes en busca de tecnologías desactualizadas. Incluso si esto implica ataques más sofisticados o que demandan el desarrollo de nuevos exploits.

A continuación algunos ejemplos de vulnerabilidades parcheadas en 2022 y 2023 para las cuales se detectó intentos de explotación:

CVE-2022-26904: vulnerabilidad en Windows 10 y Windows Server de severidad importante y que permite escalar privilegios en el sistema.

CVE-2022-21882: vulnerabilidad en Windows 10 catalogada como importante que permite a un atacante escalar privilegios.

CVE-2023-21608: vulnerabilidad del tipo *Use After Free* en Adobe Acrobat Reader que puede permitir ejecutar código arbitrario en un sistema comprometido.

CVE-2023-22515: vulnerabilidad que afecta a Confluence Data Center y Server de Atlassian que permite que un atacante externo pueda crear cuentas de administrador no autorizadas y acceder a instancias de Confluence, lo que podría comprometer la integridad y confidencialidad de los datos almacenados.

Estas vulnerabilidades representan riesgos significativos y requieren atención inmediata para mitigar posibles daños.

Vulnerabilidades más explotadas en SO diferentes a Windows

Top 3 de exploits para vulnerabilidades en Linux

Trojan.Linux/Exploit.CVE-2021-3493

- **CVE-2021-3493:** Exploit que afecta al kernel de Linux y permite a los atacantes ejecutar código arbitrario mediante BPF maliciosos.
- **Impacto:** Ejecución de código no autorizado.

Trojan.Linux/Exploit.CVE-2021-3490

- **CVE-2021-3490:** afecta al kernel de Linux y permite a los atacantes ejecutar código arbitrario mediante eBPF.
- **Impacto:** Ejecución de código no autorizado.

Trojan.Linux/Exploit.CVE-2016-4557

- **CVE-2016-4557:** afecta al kernel de Linux y el exploit permite a los atacantes obtener privilegios o causar denegación de servicio.
- **Impacto:** Elevación de privilegios o denegación de servicio.

Top 3 de exploits para vulnerabilidades en Android

Trojan.Android/Exploit.CVE-2012-6636

- **CVE-2012-6636:** Afecta a la API de Android y permite a los atacantes ejecutar métodos arbitrarios en objetos Java.
- **Impacto:** Ejecución de métodos arbitrarios.

Trojan.Android/Exploit.CVE-2019-2215

- **CVE-2019-2215:** Afecta a Android y permite la elevación de privilegios desde una aplicación a Linux Kernel.
- **Impacto:** Ejecución de código con privilegios elevados.

Trojan.Android/Exploit.CVE-2016-5195

- **CVE-2016-5195:** Conocido como "Dirty COW", afecta al kernel de Linux y permite a los atacantes escribir en mapeos de memoria de solo lectura.
- **Impacto:** Elevación de privilegios.

Top 3 de exploits para vulnerabilidades en OSx

Trojan.OSX/Exploit.CVE-2015-1130

- **CVE-2015-1130:** Afecta a Apple OS X y permite a los usuarios locales obtener privilegios de administrador.
- **Impacto:** Elevación de privilegios.

Trojan.OSX/Exploit.CVE-2019-8565

- **CVE-2019-8565:** Afecta a iOS y macOS y permite a una aplicación maliciosa obtener privilegios de root.
- **Impacto:** Elevación de privilegios.

Trojan.OSX/Exploit.CVE-2018-4237

- **CVE-2018-4237:** Afecta a iOS, macOS, tvOS y watchOS y permite a los atacantes ganar privilegios a través de una aplicación manipulada.
- **Impacto:** Elevación de privilegios.

Ransomware

23%

de las empresas fue blanco de al menos un intento de ataque de ransomware en los últimos dos años

Las industrias o sectores que recibieron más intentos de ataque de ransomware en América Latina fueron Petróleo/Gas/Minería (36%), Telecomunicaciones (31%), Servicios Públicos (30%), y Retail/Mayorista (29%).

Además, el 96% de las empresas y organizaciones de Latinoamérica opina que el ransomware es una amenaza que preocupa.

86%

de las empresas no estaría dispuesta a negociar el pago de un rescate

Si bien el 14% de las empresas de América Latina aseguró que estaría dispuesta a pagar un rescate, es importante recordar que esto no asegura la obtención de un descifrador para recuperar los archivos, ni que los datos robados no serán publicados o comercializados, ni que la reputación de la organización no se verá afectada. Además, **pagar a los grupos de ransomware** contribuye al negocio del cibercrimen y puede dejar la puerta abierta a nuevos intentos de ataque.

23%

de las empresas tiene contratado un seguro contra riesgos cibernéticos

Informes recientes indican que la demanda de seguros cibernéticos creció a nivel mundial en los años de la pandemia ante el aumento de los ciberataques, la implementación de mayores regulaciones y el crecimiento de las economías digitales. De todas formas, es importante tener presente que la seguridad de una empresa debe estar enfocada en tomar todas las precauciones posibles y en hacer que la organización sea cada vez más segura.

¿Qué pasó con el ransomware durante 2023 en América Latina?

> El **ransomware continuó siendo una amenaza muy activa** a nivel global y también a nivel regional en América Latina durante 2023.

Nuestros reportes y los de otras organizaciones coinciden en que se registró un aumento importante en ese periodo, en comparación al 2022.

En Latinoamérica se detectaron varios casos de ataques de ransomware durante 2023 que fueron perpetrados por diferentes grupos que operan bajo el modelo de ransomware as a service (RaaS). En WeLiveSecurity repasamos algunos de los **ataques de ransomware más importantes durante el último año** en distintos países de la región.

Durante ese período se observó el uso de nuevas tácticas y tecnologías, así como la consolidación de otras estrategias como la doble extorsión. Por ejemplo, se observó la prevalencia de dos métodos de infección inicial en los ataques de ransomware en la región: el uso de **commodity malware** mediante el correo electrónico o la explotación de vulnerabilidades zero-day. Además de esta tendencia, los grupos de ransomware continuaron intentando acceder a los sistemas corporativos mediante la explotación de vulnerabilidades conocidas en servicios expuestos a Internet, errores de configuración o a través del uso de credenciales robadas.

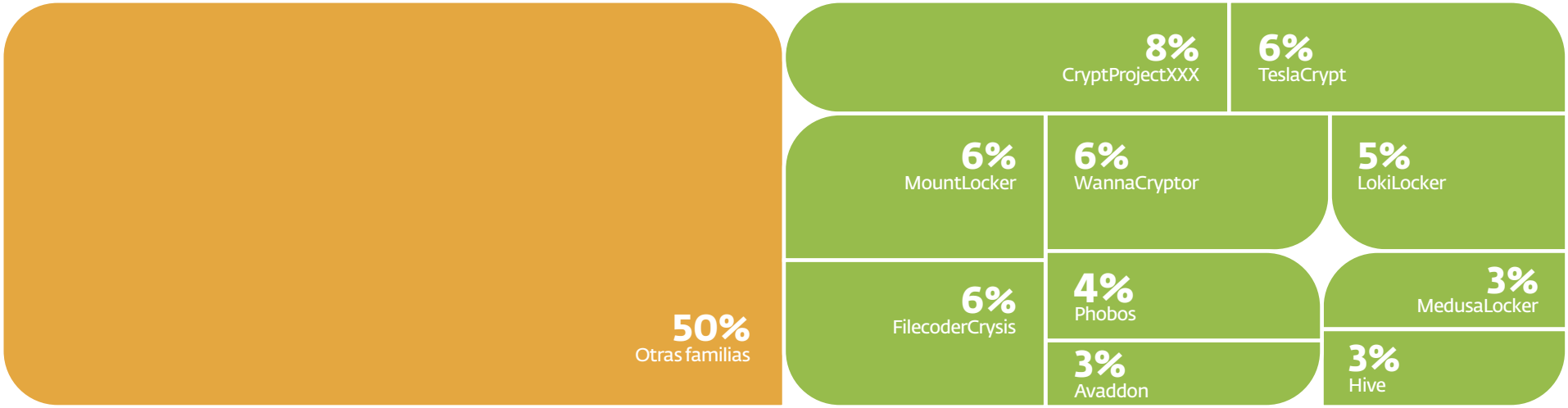
Otras de las nuevas estrategias que se observó en 2023 por parte de los grupos de ransomware fue el uso de malware del tipo wiper posterior al robo y cifrado de los archivos, y el despliegue de otras variantes de ransomware durante un mismo ataque.

¿Cuáles fueron las 5 familias de Ransomware con más detecciones en América Latina?

El ecosistema del ransomware es heterogéneo. Si bien en los ataques de ransomware qué más atención tuvieron observamos nombres de grupos de ransomware como LockBit, BlackCat, Clop, o Medusa, por nombrar algunos, es importante tener presente que estos grupos utilizan largas cadenas de infección y sus ataques suelen ser dirigidos. Por esta razón, muchos ataques que tienen como objetivo final la infección con estas familias de malware no son detectados ni vinculados a estas familias porque son bloqueados por las tecnologías de ESET en etapas más tempranas, detectando los downloaders o exploits utilizados para el acceso inicial, limitando la información sobre el payload final de muchos de estos ataques.

Por otra parte, en el diverso ecosistema del ransomware existen muchos códigos maliciosos que se distribuyen de manera masiva y con menos etapas, incluso intentando ejecutar el ransomware directamente desde un ejecutable o archivo adjunto.

Familias ransomware más detectadas | 2023 | LATAM



CryptProjectXXX

- **Características:** Se distribuye a través de kits de explotación como Angler y Neutrino. Tiene la capacidad de cifrar archivos además de robar credenciales de diferentes aplicaciones.
- **Impacto:** Cifrado de archivos y robo de información.

TeslaCrypt

- **Características:** Conocido por atacar a usuarios gamers, cifra archivos de juegos y otros tipos de archivos dentro del sistema afectado.
- **Impacto:** Cifrado de archivos y extorsión económica.

MountLocker

- **Características:** Operando como Ransomware-as-a-Service (RaaS), utiliza ChaCha20 para el cifrado de archivos y RSA-2048 para el cifrado de claves. Posee una funcionalidad opcional de
- borrado que, si no se paga el rescate en el tiempo especificado,
- eliminan todos los archivos del sistema y sobreescribe el MBR, inutilizando el sistema.
- **Impacto:** Cifrado de archivos, borrado de datos y posible inutilización del sistema.

Crysis (también conocido como Dharma)

- **Características:** Generalmente se infiltra a través de puertos RDP expuestos. Cifra archivos y demanda un rescate. Elimina todos los puntos de restauración del sistema, lo que dificulta la recuperación de los archivos.
- **Impacto:** Cifrado de archivos y eliminación de puntos de restauración.

LokiLocker

- **Características:** Cifra archivos con AES y protege las claves con RSA. Si no se paga el rescate en el tiempo especificado, tiene la capacidad de borrar todos los archivos del sistema y sobrescribir el MBR, inutilizando el sistema.
- **Impacto:** Cifrado de archivos y potencial borrado total del sistema.

Presupuesto asignado a ciberseguridad

62%

de las organizaciones considera que el presupuesto asignado a ciberseguridad no es suficiente

Entre las industrias encuestadas, se observa que las que reportaron menores niveles de presupuesto son Gobierno, Agricultura y Ganadería, con un 79% de las entidades encuestadas, seguidas por Retail/Mayorista, con un 74%, y Petróleo, Gas y Minería, con un 69%.

Los sectores más satisfechos con el presupuesto asignado son Informática y Tecnología (54%) y Telecomunicaciones (51%).

Preocupaciones de las organizaciones

28%

de las empresas considera que la ciberseguridad es un asunto de máxima preocupación

Para comprender la importancia de la ciberseguridad para las empresas de América Latina, evaluamos el nivel de preocupación asociado con diversos riesgos, como accesos indebidos a los sistemas, falta de disponibilidad de servicios críticos, extorsión, robo o fuga de información, y uso malicioso de recursos e infraestructura. Según la percepción de los encuestados, el 28% considera que estos riesgos son de máxima preocupación, mientras que el 42% los clasifica como de preocupación alta.

Nivel de preocupación que representa para las empresas la ciberseguridad

28%
Preocupación máxima

42%
Preocupación alta

20%
Preocupación significativa

7%
Preocupación moderada

3%
Mínima preocupación

La principal preocupación del C-Level (77%) es la Falta de Disponibilidad de servicios críticos, lo cual se alinea con la continuidad operativa del negocio.

Las principales preocupaciones para los equipos técnicos (Administradores de Red/Analistas/Soporte) son el Acceso Indebido a sistemas (79%) y el Robo/Fuga de información (79%).

Adopción de medidas de seguridad

85%

de las empresas cuenta con soluciones de backup

Consultamos cuáles son las tecnologías de seguridad más utilizadas por las empresas en la actualidad y encontramos que el Firewall es la más ampliamente adoptada, con un 88% de las organizaciones implementándola, seguida de soluciones de backup (85%) y de VPN (80%). Además, se destaca que las soluciones antimalware tienen una tasa de adopción por encima de la media, ya que el 64% de las empresas cuenta con esta tecnología.

En el caso de las organizaciones gubernamentales, el Firewall es la tecnología más implementada (94%), mientras que en sectores como Banca, Informática y Tecnologías, Hidrocarburos, Retail, Salud y Servicios públicos las soluciones de backup son las más comunes.

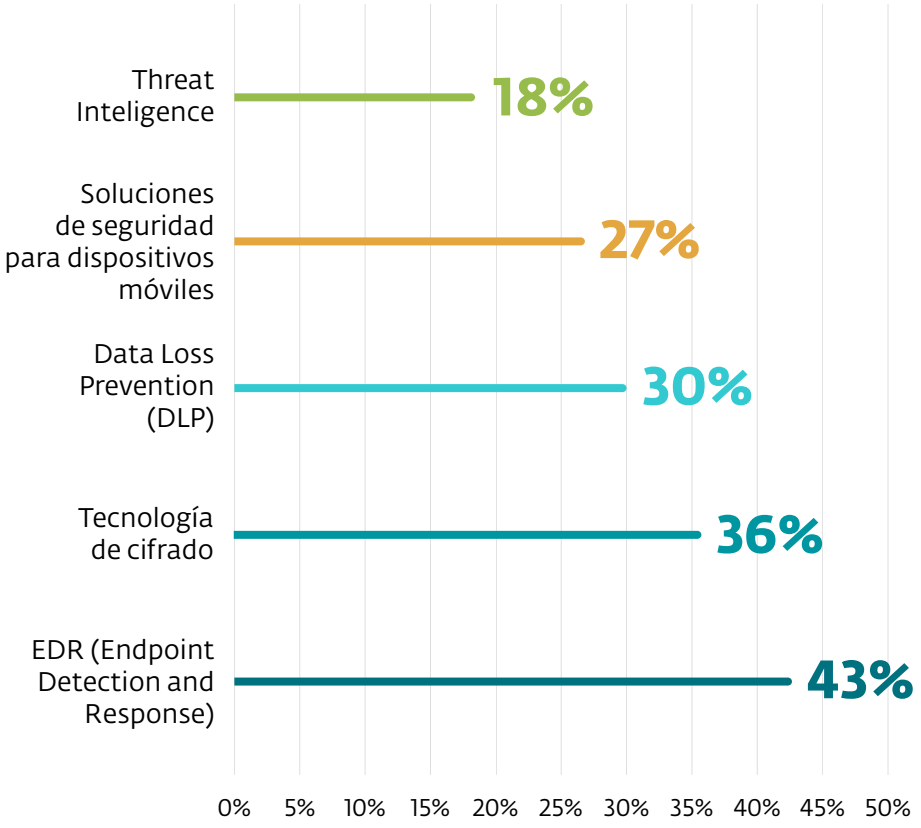
Tecnologías de seguridad implementadas por menos del 50% de las organizaciones

Ciertas tecnologías avanzadas, **como las soluciones de EDR**, permiten hacer frente a la constante evolución de las amenazas informáticas y las nuevas TTPs usadas para los ataques. Sin embargo, este tipo de tecnología tiene bajos niveles de adopción en empresas de la región: **apenas 2 de cada 5 encuestadas la implementa**.

Por otra parte, el uso de contraseñas débiles es la causa de muchas de las intrusiones a los sistemas mediante ataques de fuerza bruta. Pero, solamente **el 50% de las empresas asegura contar con un segundo factor de autenticación** a pesar de que es una alternativa efectiva para contrarrestar este problema.

Incorporar alternativas que permitan hacer Inteligencia de Amenazas para conocer a los adversarios y ser más eficientes con la distribución de recursos en seguridad, es un gran paso en la madurez de las organizaciones. No obstante, este tipo de tecnología es la de menor adopción en la región, **apenas 1 de cada 5 empresas cuentan con esta tecnología**.

Por otro lado, si bien la fuga de información se constituye como la mayor preocupación de las empresas, **apenas el 30% de las organizaciones cuentan con una solución de DLP**.



Prácticas y políticas de gestión

83%

de las organizaciones cuenta con una política de seguridad

Dentro de las prácticas y políticas de gestión de ciberseguridad más adoptadas por las empresas en Latinoamérica, la política de seguridad es la práctica de gestión más extendida, ya que el 83% de las empresas asegura contar con una. Le siguen el plan de respuesta ante incidentes, que solo el 52% de las organizaciones implementa, y el plan de continuidad de negocio con el 46% de adopción.

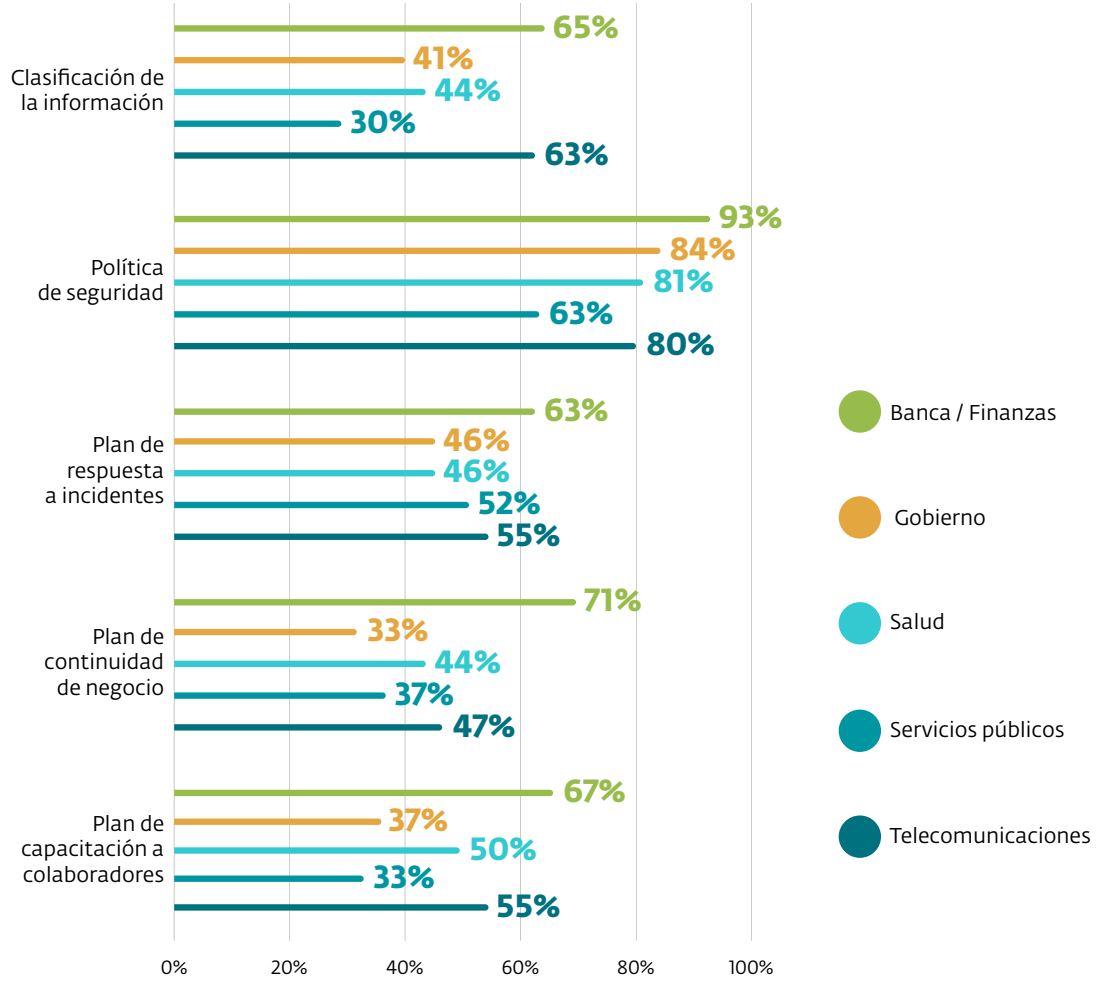
Los planes de capacitación son una práctica de gestión que tiene poca adopción, ya que apenas la mitad de las empresas incluye la capacitación como parte de su plan de acción. De hecho, solo el 25% de las empresas realiza más de dos capacitaciones anuales y el 32% realiza este tipo de actividades una sola vez al año.

Cuáles son los sectores con más medidas de seguridad implementadas

El sector de Banca y Finanzas es el que tiene mejores niveles de adopción de prácticas de gestión. Si bien todos los sectores pueden mejorar, es a nivel Gobierno y Servicios públicos donde más oportunidad de crecimiento hay, considerando que ambos sectores son parte fundamental de las infraestructuras críticas y por lo tanto es importante garantizar altos estándares de protección.

Uno de los vectores de ataque más utilizado en campañas maliciosas en la región es la explotación de vulnerabilidades. Si bien 2 de cada 5 empresas aplican parches de seguridad en sus sistemas más de dos veces al año, cerca del 25% lo hace únicamente 1 vez en el año, dejando expuestas a las organizaciones por más tiempo a la explotación de nuevas vulnerabilidades.

Prácticas de gestión más adoptadas en diferentes sectores



69% de las empresas realiza análisis de riesgo de seguridad al menos una vez al año

Los análisis de riesgo son una gran herramienta para conocer el estado de seguridad de la organización y saber cómo orientar los recursos humanos y económicos. El 69% de las empresas encuestadas realizan esta práctica de gestión por lo menos una vez en el año.

Probar la efectividad de las medidas de protección a través de un Pentesting es una práctica habitual. Y si bien el 64% de las empresas encuestadas lo realizó por lo menos una vez, el 25% nunca ha realizado está actividad.

Trabajo remoto

77%

considera que su organización está preparada para trabajar de forma remota y a la vez segura

Muchas organizaciones en la región no volvieron a una presencialidad total luego de la pandemia. De las empresas encuestadas, el 62% funciona actualmente bajo un modelo de trabajo híbrido y solo el 3% mantiene un modelo totalmente remoto.

Las entidades de Gobierno son las que en mayor porcentaje (54%) tienen un modelo presencial de trabajo, en contraposición a sectores como el de Banca/Finanzas (73%) o Informática/Tecnología (73%) que mantienen un esquema híbrido.

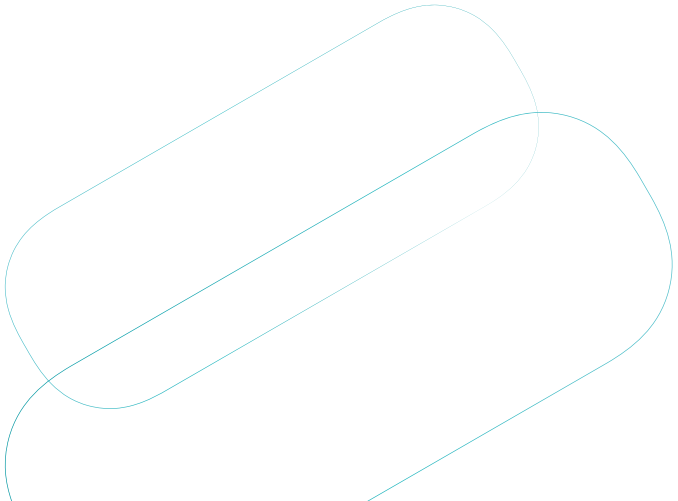
Los sectores que tienen una percepción más alta de inseguridad con respecto al trabajo remoto son el sector Educación (45%) y el sector Logística & Transporte (33%).

Qué opinan los colaboradores de las empresas

27%

de los colaboradores recibe capacitaciones periódicas en temas de seguridad

Los cursos de capacitación (47%) y las charlas internas (33%) son los mecanismos más utilizados por las empresas para concientizar a sus colaboradores. Si bien el 51% de los colaboradores encuestados manifestó que recibe capacitaciones esporádicas por parte de su empresa, 1 de cada 5 aseguró que no cuenta con este tipo de formación. Por otra parte, 1 de cada 4 colaboradores encuestados manifestó no sentirse capacitado en temas de ciberseguridad y apenas el 16% se siente capacitado para identificar posibles ataques.



Acerca de ESET

ESET® es una empresa que ofrece **soluciones de seguridad digital de vanguardia** para prevenir ataques antes de que ocurran.

Combinando el poder de la inteligencia artificial con la experiencia humana, ESET se mantiene a la vanguardia de las amenazas cibernéticas conocidas y emergentes, asegurando empresas, infraestructuras críticas y personas. Ya sea protección para endpoints, la nube o dispositivos móviles, nuestras soluciones y servicios nativos de IA y basados en la nube siguen siendo altamente efectivos y fáciles de usar.

La tecnología de ESET incluye una detección y respuesta robustas, cifrado ultra seguro y autenticación multifactorial. Con defensa en tiempo real las 24 horas, los 7 días de la semana y un sólido soporte local, mantenemos a las personas seguras y los negocios funcionando sin interrupciones. Un paisaje digital en constante evolución exige un enfoque progresivo en seguridad y ESET asume este compromiso proporcionando además una investigación de clase mundial y una poderosa inteligencia de amenazas, respaldada por centros de Investigación y Desarrollo a nivel global, incluido América Latina, y una sólida red global de socios comerciales.

Para obtener más información, visita www.eset.com o síguenos en LinkedIn, Facebook, Instagram y X.

SOBRE ESET

+ 110 millones de usuarios en todo el mundo

+ 400 mil clientes corporativos

13 centros de investigación y desarrollo en el mundo

200 países y territorios

ESET Digital Security
Progress. Protected.