SECURITY REPORT

LATINOAMÉRICA 2025

Panorama del estado actual de la ciberseguridad corporativa en Latinoamérica: amenazas, brechas, prácticas y niveles de preparación frente a un entorno un siempre desafiante.

Progress. Protected.

Contenido

Acerca del 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 basa en encuestas realizadas a 3.034 profesionales que trabajan en organizaciones de diversas industrias en 15 países de la región. La mayoría de los encuestados ocupa cargos en el sector TI o en áreas vinculadas a la seguridad.

La información extraída de la telemetría de ESET durante 2024 permite contextualizar la percepción de los encuestados respecto de la actividad maliciosa detectada durante el últimoaño en América Latina.

El informe aborda aspectos clave relevados por la encuesta, como la cantidad de incidentes sufridos, las amenazas más activas del último año, la situación del ransomware en la región, el grado de satisfacción con el presupuesto asignado a ciberseguridad, las prácticas de gestión más frecuentes, las principales preocupaciones en materia de ciberseguridad y las medidas más implementadas.

El **ESR 2025** ofrece una visión regional sobre la seguridad de las organizaciones, con el objetivo de aportar una perspectiva que contribuya a fortalecer la conciencia sobre la importancia de la ciberseguridad para las empresas de América Latina.

27%

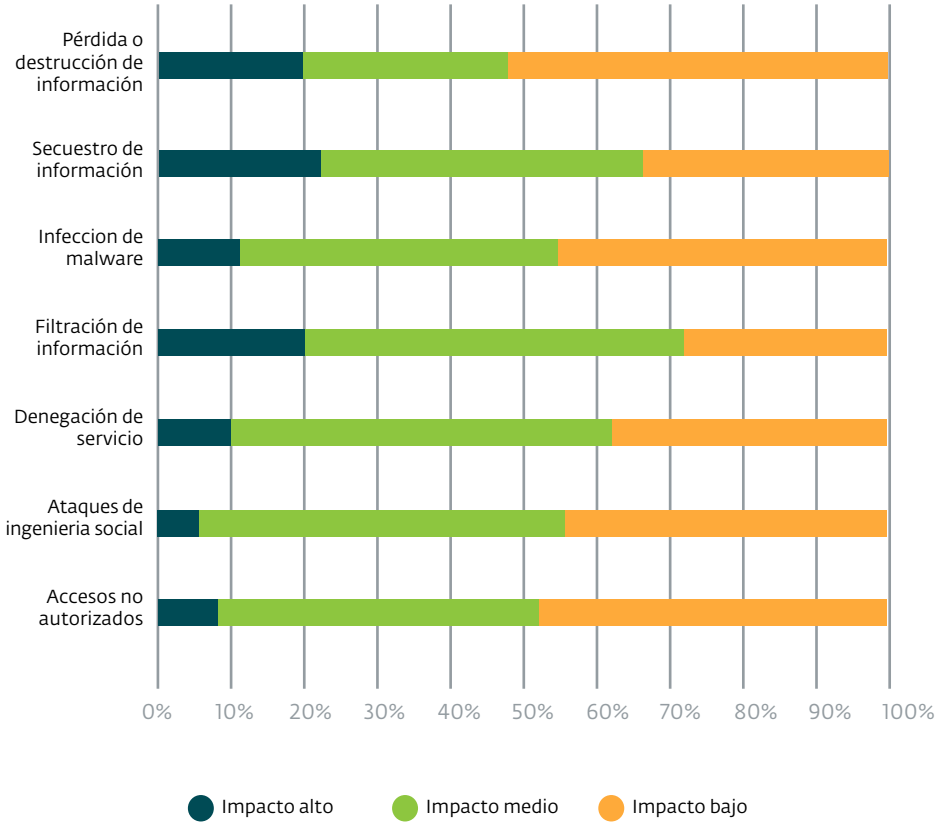
de las organizaciones afirmó haber sufrido un ciberataque en el último año

Si bien esto representa una baja del 3% con respecto al año anterior, esto no se traduce necesariamente en menos ciberataques a nivel corporativo. La realidad es que, entre las organizaciones encuestadas que no detectaron intentos de ciberataques, 2 de cada 5 también creen no contar con la tecnología suficiente para estar seguros de ello. En otras palabras, un 32% de los encuestados no cuenta con la visibilidad suficiente para afirmar o negar haber sufrido un ciberataque en su organización, y un subconjunto de ellos probablemente haya sido víctima sin saberlo. La visibilidad es un aspecto clave en la ciberseguridad: no es posible proteger lo que queda fuera del alcance de las herramientas de protección, tanto tecnológicas como humanas.

Daños a la información, los ciberataques con más impacto

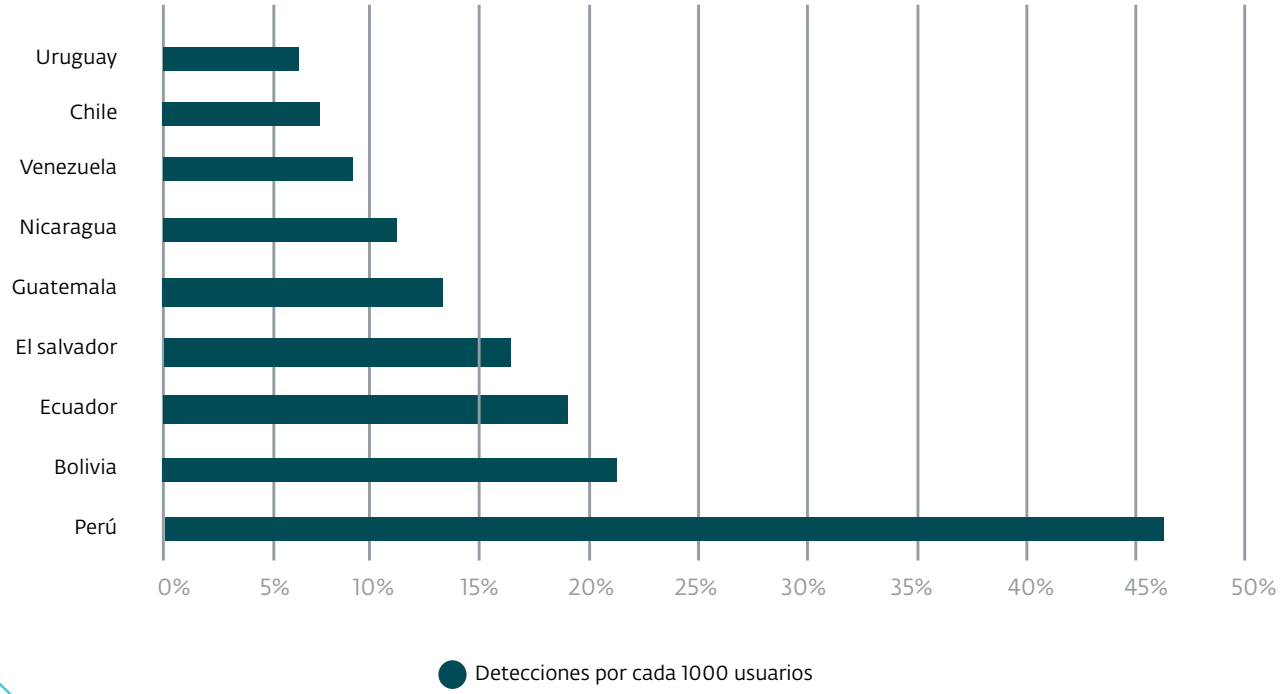
Un **20% de los encuestados que afirmaron haber sufrido secuestro, destrucción o filtración de información reportaron un alto impacto negativo** para la organización a la que pertenecen y afirmaron haber sufrido consecuencias legales, grandes pérdidas de dinero e incluso ruptura de contratos. A diferencia de activos físicos, la información puede ser copiada, vendida o destruida con facilidad, lo que la convierte en un objetivo atractivo para ciberdelincuentes motivados por el lucro o para espionaje o sabotaje.

Por otro lado, el impacto de estos incidentes no siempre es inmediato. En muchos casos, la verdadera magnitud del daño solo se manifiesta con el tiempo. Una organización puede saber que ha sufrido una filtración, pero no tener visibilidad sobre el uso que se hará de la información comprometida. Años después, un cliente o socio comercial podría descubrir que sus datos han sido explotados, lo que no solo genera perjuicios financieros y reputacionales, sino que también puede derivar en acciones legales contra la empresa afectada.



Familias de malware más detectadas

En la región, los países con mayor tasa de detecciones por usuario con acceso a internet son Perú, Bolivia, Ecuador, El Salvador, Guatemala, Nicaragua, Venezuela, Chile y Uruguay.



Dentro de la telemetría de ESET, en Latinoamérica encontramos las siguientes familias como las principales detectadas:

Expiro (5,29%)

Expiro es un malware de tipo infostealer con capacidades de backdoor que suele propagarse a través de ejecutables infectados. Se utiliza para robar información sensible del sistema, como credenciales y datos del navegador, además de permitir el control remoto del dispositivo comprometido.

Ramnit (3,41%)

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, pudiendo adoptar capacidades de botnet.

Zurgop (2,04%)

Zurgop es un RAT con capacidades avanzadas de espionaje y control remoto. Se distribuye mediante campañas maliciosas por correo electrónico y puede robar información sensible, grabar audio, capturar pantalla y operar el dispositivo comprometido de forma encubierta.

Rozena (2,02%)

Rozena es un troyano que instala una shell inversa en el sistema comprometido, permitiendo a los atacantes obtener acceso remoto. Se suele distribuir mediante documentos o scripts maliciosos y puede modificar configuraciones del sistema, abrir puertas traseras y exfiltrar datos.

Rescoms (1,64%)

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.

Vulnerabilidades más detectadas

Las vulnerabilidades son el resultado de errores de programación o configuración de piezas de software de todo tipo. Como contraposición a los vectores de infección vía ingeniería social, las vulnerabilidades como puntos de entrada no requieren interacción de los usuarios y, por lo tanto, son menos propensas a ser detectadas sin un enfoque reactivo.

En la región, hay una tendencia que año a año se solidifica: las vulnerabilidades más atacadas tienen años de antigüedad, llegando hasta la década en algunos casos, y ya cuentan con su parche en el sitio del fabricante. Esto habla de que el problema está en la implementación de esos parches, no en cantidad o gravedad de las vulnerabilidades, ya sea por ignorancia o falta de personal capacitado.

Puntualmente, las vulnerabilidades más explotadas según la telemetría de ESET en Latinoamérica en 2024 son:

CVE-2012-0143

Vulnerabilidad de Microsoft Excel que permite la ejecución remota de código arbitrario, que puede ser malicioso. En el año 2017, la familia de ransomware DoppelPaymer usó esta vulnerabilidad para campañas en Latinoamérica.

CVE-2012-0159

Vulnerabilidad en Microsoft Windows que también permite acceder remotamente y sin necesidad de autenticación a un sistema vulnerable. El fallo se descubrió en **2012** y fue utilizado, por ejemplo, en campañas de ransomware icónicas como las de "Petya" y "NotPetya" años atrás.

CVE-2016-3316

Vulnerabilidad en versiones antiguas de Microsoft Word para sistemas Mac y Windows que permite ejecutar código arbitrario vía corrupción de memoria, por la creación de un archivo particular. Por ello, esta explotación puede darse sencillamente por correo electrónico, en donde el atacante le envía a la víctima este archivo en puntual y, vía ingeniería social, convence al usuario de abrirlo.

CVE-2021-26855

Vulnerabilidad en Microsoft Exchange que abusa de funcionalidades de conexiones HTTPS del servidor para autenticar a usuarios externos, que pueden ser maliciosos. Esta fue noticia en 2021, cuando fue explotada en su versión Zero-Day para campañas centradas en compañías de alto nivel en todo el mundo.

CVE-2017-11882

Vulnerabilidad en Microsoft Office y Microsoft Wordpad que, similar a la CVE-2016-3316, es explotada con la creación y apertura de un archivo con ciertas características técnicas. Es utilizada por cibercriminales para distribuir distintos tipos de malware, como Agent Tesla y otros troyanos de acceso remoto.

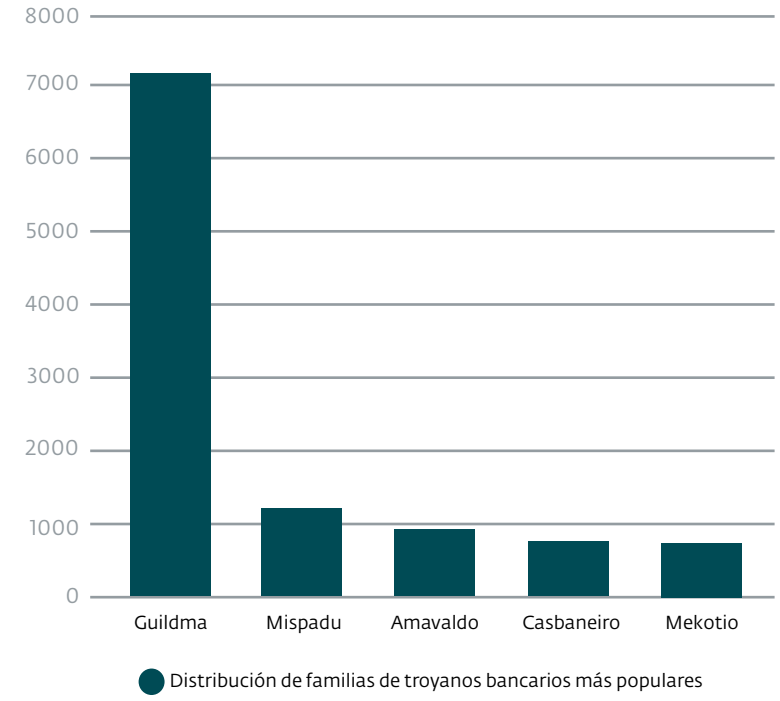
Troyanos bancarios, presencia constante en Latinoamérica

La presencia de troyanos bancarios en América Latina se ha mantenido constante a lo largo del tiempo, con períodos de mayor y menor actividad, pero sin desaparecer del panorama de amenazas. Las familias más detectadas en la región, considerando la cantidad de archivos únicos asociados, son Guildma y Mispadu, ambas superando ampliamente los mil archivos identificados. Les siguen Amavaldo, Casbaneiro y Mekotio, también con fuerte presencia, pero en menor volumen.

Estos troyanos apuntan principalmente al robo de credenciales bancarias mediante técnicas de phishing, superposición de ventanas y control remoto del dispositivo. Su distribución suele apoyarse en campañas maliciosas por correo electrónico, instaladores falsos y descarga encubierta desde sitios comprometidos. A pesar de las acciones de desarticulación y campañas de concientización, su actividad sigue siendo una de las más persistentes en la región.

En cuanto a su distribución, Brasil (61,2%) y México (24,48%) concentran la mayoría de las detecciones. Le siguen Argentina (5.24%), Perú (3.49%) y Colombia (2,62%).

Archivos únicos asociados a familias de troyanos bancarios más populares



22%

de las organizaciones afirmó haber sufrido un ataque de ransomware en los últimos dos años

El ransomware continúa siendo una de las amenazas más temidas por su alto impacto, a pesar de ser uno de los tipos de malware con menor cantidad de archivos únicos asociados —apenas superando los 15.000 en todo 2024 en la región, muy por detrás de otras categorías como los troyanos o el spyware—. Su notoriedad no radica en el volumen, sino en los estragos que causa: interrupciones operativas, pérdidas económicas y exposición de información sensible.

En los últimos años, además se consolidó la tendencia hacia un cambio en la selección de víctimas. En lugar de campañas masivas dirigidas a miles de usuarios individuales, los atacantes ahora apuntan a objetivos corporativos específicos para maximizar el daño y el rédito económico. Esta estrategia, conocida como big game hunting, combina la extorsión del cifrado de datos con la amenaza de filtrarlos, lo que transforma cada incidente en una crisis potencial para la organización víctima que va más allá de la pérdida de la información.

Gran preocupación, no tan gran preparación

95%

de los encuestados afirmó sentir preocupación especial por el ransomware como amenaza informática, lo cual no es sorprendente considerando el impacto financiero y operativo que estos ataques pueden generar en una organización.

Sin embargo, la adopción de tecnologías y prácticas clave para prevenir una infección o minimizar sus consecuencias sigue siendo baja. Menos de la mitad de las organizaciones encuestadas aplican soluciones como el **Data Loss Prevention** (o DLP) y tecnologías de cifrado, o prácticas como la clasificación de la información. La única excepción notable es el respaldo de datos o Backup con un 85% de adopción, lo que sugiere que el enfoque corporativo sigue siendo orientado más a la recuperación que a la prevención. Esto deja abierta una brecha de seguridad significativa, sobre todo teniendo en cuenta lo cambiante que es el mundo de las ciberamenazas.

El ransomware en Latinoamérica

Durante 2024, el ransomware protagonizó numerosos ataques en la región latinoamericana. Universidades, centros de salud, empresas y organismos gubernamentales de Argentina, Brasil, Chile, Colombia, México, Perú, entre otros, fueron blanco de algún grupo de ransomware.

Entre los actores más activos del año destacaron LockBit 3.0, Vice Society, ALPHV (BlackCat) y Medusa. Sin embargo, el grupo con mayor protagonismo fue RansomHub, que desde su aparición a comienzos del año logró afectar a más de 200 organizaciones a nivel global.

También hemos observado la actividad de grupos emergentes como Qiulong y Cactus, que han puesto su ojo y recursos con ataques sobre la región.

27% de las organizaciones tienen contratado un seguro contra riesgos cibernéticos

La gran adopción de seguros contra incidentes informáticos por parte de las organizaciones encuestados demuestra una creciente conciencia sobre el impacto que tienen las amenazas informáticas en el mundo corporativo. Sin embargo, es importante comprender que los seguros no son una herramienta de prevención, sino una medida de mitigación para las consecuencias de un incidente ya sufrido. Por ello, y aun siendo un componente válido dentro de una estrategia de ciberseguridad, no reemplaza la inversión en prevención y protección proactiva contra amenazas.

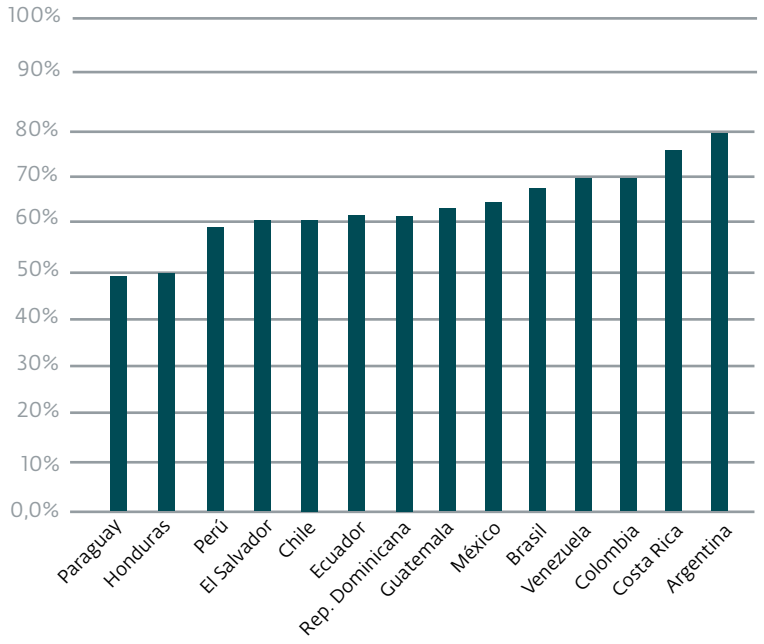
38%

de las organizaciones no implementa una solución antimalware centralizada

Si bien las soluciones antivirus o antimalware se posicionan como las terceras de mayor adopción, solo superadas por las herramientas de firewall (88%) y las tecnologías de Backup (85%), el porcentaje sigue siendo bajo.

Entre los países con menor tasa de adopción de antivirus encontramos a Paraguay (49.5%), Honduras (51%) y Perú (58,5%).

Porcentaje de adopción de soluciones antimalware centralizadas



Apenas 1 de cada 4 empresas protege los dispositivos móviles corporativos

Los dispositivos móviles corporativos son un atractivo para los cibercriminales por la cantidad de información que contienen y por el trato descuidado que los colaboradores y empresas suelen darle con respecto a la ciberseguridad.

Aquí, las amenazas se materializan con correos maliciosos visualizados en una pantalla más pequeña que una computadora, aplicaciones dañinas en tiendas oficiales, y hasta **la instalación a partir de pop-ups de aplicaciones web (como PWAs) que pasan desapercibidas.**

Herramientas de Threat Intelligence, las de menor adopción

Un 19% de las organizaciones encuestadas afirmó utilizar alguna herramienta de inteligencia de amenazas: desde feeds de noticias, listas actualizables en tiempo real o reglas, hasta bases de datos y APIs interactivas, tanto gratuitas —incluso, algunas de código abierto— como pagas.

Los ciberatacantes suelen centrar sus campañas en compañías de rubros, tamaños, países o regiones similares, por lo que la recopilación de información vital es una herramienta valiosa de predicción. Observar solapamientos en tácticas, técnicas y procedimientos de las ciberamenazas más detectadas en la actualidad permite a las organizaciones hacer un análisis interno de su estado de protección, que considere las soluciones implementadas, los procedimientos a seguir y las prácticas de gestión a realizar.

Los accesos indebidos a sistemas y el robo de información, las mayores preocupaciones de las empresas

Más de la mitad de las organizaciones encuestadas calificó a los accesos no autorizados como la mayor preocupación ante posibles ciberataques, con una dispersión baja que indica un gran consenso sobre el riesgo que representan los actores malintencionados. Sea por credenciales comprometidas, errores de configuración o ataques dirigidos, los atacantes pueden obtener acceso a infraestructuras e información y comprometer la seguridad de la organización.

El robo de información obtuvo un promedio de 4.3 de 5 puntos en materia de preocupación por parte de las organizaciones encuestadas, lo que indica que es percibido como un riesgo significativo en el mundo corporativo.

Esta inquietud se ve respaldada por más que sensaciones: al consultar a quienes sufrieron un ciberataque de este tipo, un 21.6% afirmó que el robo de información había tenido un alto impacto, siendo el ataque más dañino entre los reportados.

La mitad de las organizaciones no cuentan con un plan de continuidad del negocio

Apenas un 47% de las organizaciones encuestadas afirmó contar con un plan práctico para recuperarse y restaurar las funciones operativas en el caso de una irrupción, ya sea accidental o intencional como un ciberataque. Esto es especialmente preocupante dado el factor económico: además de la pérdida de información o sistemas, la recuperación de un ciberataque puede superar fácilmente los cientos de miles de dólares entre tiempos de inactividad, recuperación, multas regulatorias y daño reputacional. Sin una respuesta preparada, un solo incidente puede afectar directamente la viabilidad económica de una empresa, especialmente en sectores donde cada minuto de inactividad tiene un alto costo operativo.

1 de cada 4

empresas nunca realizó un pentesting

Esto lo posiciona como uno de los ejercicios de seguridad menos realizado entre las organizaciones encuestadas, con diferencia por sobre otros, como el análisis de vulnerabilidades. Además, entre quienes afirmaron realizar pruebas de penetración de forma regular, la mitad lo hace una vez al año. El pentestiing puede detectar puntos de entrada, como vulnerabilidades o servicios expuestos, antes de que los ciberatacantes, de modo que pueden subsanarse a tiempo.

Capacitaciones, una necesidad todavía no instalada

Menos de la mitad de las organizaciones afirmó tener un plan estructurado de capacitación a sus colaboradores. Si bien un 31% realiza capacitaciones una vez al año y un 29% lo hace dos veces al año, estas instancias suelen llevarse a cabo de forma aislada, sin un enfoque estratégico sostenido.

Contar con un plan estructurado marca una diferencia significativa. Este tipo de abordaje contempla revisiones periódicas y actualizaciones constantes de los contenidos y también permite adaptar la formación a nuevas amenazas y escenarios. Los ejercicios puntuales, si no están acompañados de seguimiento y evaluación, pueden no alcanzar el mismo nivel de impacto.

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

Su enfoque combina el poder de la inteligencia artificial con la experiencia humana para anticiparse a 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 son 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

Digital Security
Progress. Protected.

esetla @esetla @esetla ESET Latinoamérica