SECURITY REPORT
LATINOAMÉRICA 2026

Panorama de la ciberseguridad
de las empresas de América Latina

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

El ESET Security Report (ESR) 2026 ofrece un diagnóstico profundo sobre la ciberseguridad corporativa en América Latina, basado en **1.563** respuestas de profesionales del sector. Para garantizar la solidez estadística, el análisis se concentró exclusivamente en los 10 países de la región que alcanzaron el umbral mínimo de participación, incluyendo Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, Honduras, México, Panamá y Venezuela. Los participantes representan a unas **962 organizaciones** distintas, validadas a través de sus dominios institucionales.

La muestra cuenta con un alto nivel de especialización: el **80,7 % trabaja directamente en el área de seguridad** (analistas, técnicos, gerentes y directores), garantizando un conocimiento real y técnico de las infraestructuras. **El 19,3 % restante corresponde a colaboradores fuera del área técnica**, lo que aporta una perspectiva clave sobre los hábitos y prácticas de seguridad del usuario final. En términos sectoriales, los participantes provienen principalmente de las áreas de Gobierno, Informática/Tecnología, seguidos por industrias estratégicas como Banca y Finanzas, Educación y Salud.

A partir de estos datos, el informe examina el índice de ciberataques frente a las brechas de visibilidad, los vectores de intrusión dominantes como el phishing, el vacío regulatorio y percepción de riesgo ante la Inteligencia Artificial, la adopción de herramientas de protección y la seguridad en entornos móviles corporativos. El resultado es una radiografía fiel para respaldar la toma de decisiones estratégicas en la región.

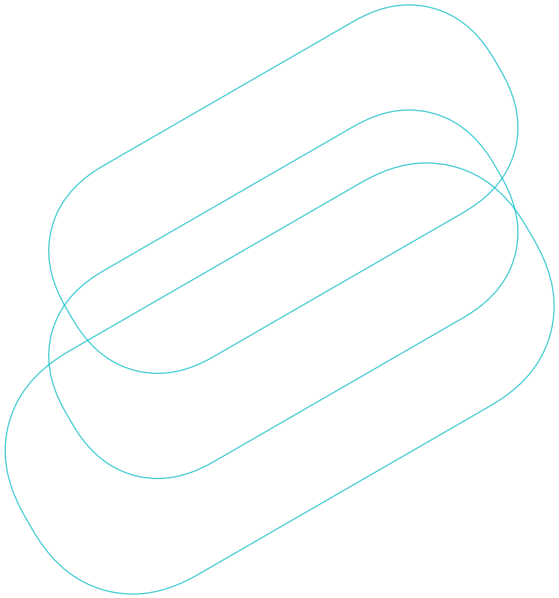
1. Incidentes y brechas de visibilidad

¿Qué porcentaje de las empresas opera a ciegas en la región? Diagnóstico inicial de detección de ataques.

El panorama regional revela una alta actividad delictiva acompañada de una notable falta de visibilidad en las plataformas corporativas.

52,7 %

de las empresas de la región confirmó haber detectado al menos un intento de ciberataque en los últimos 12 meses (equivalente a 824 respuestas asociadas a organizaciones encuestadas).

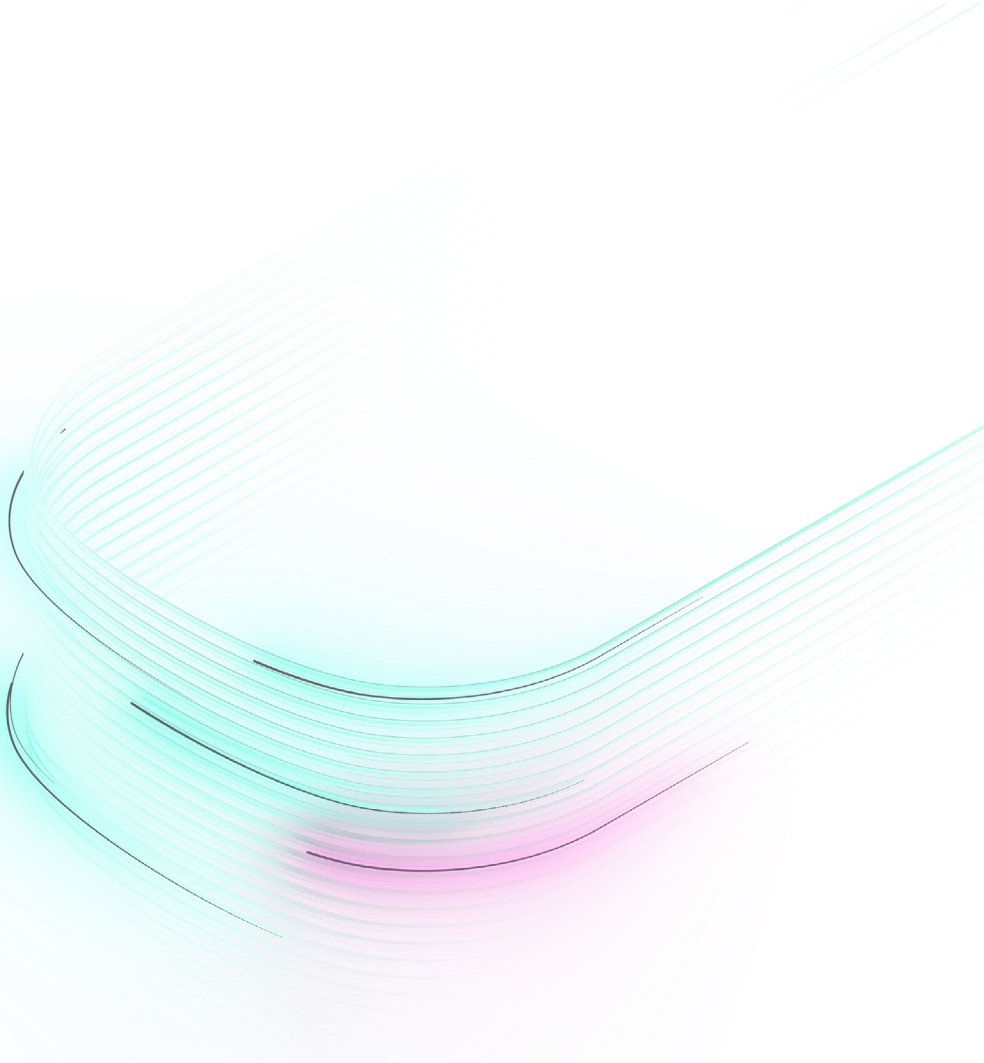


15,4 %

de las organizaciones de la región no puede confirmar si sufrió o no intentos de ciberataque, lo que evidencia una falta crítica de visibilidad en las redes.

Invisibilidad tecnológica y conclusión regional

Entre las empresas que no detectaron ataques, la sospecha de incidentes no registrados y el desconocimiento técnico revelan una vulnerabilidad estructural en la infraestructura analítica de las organizaciones de América Latina.



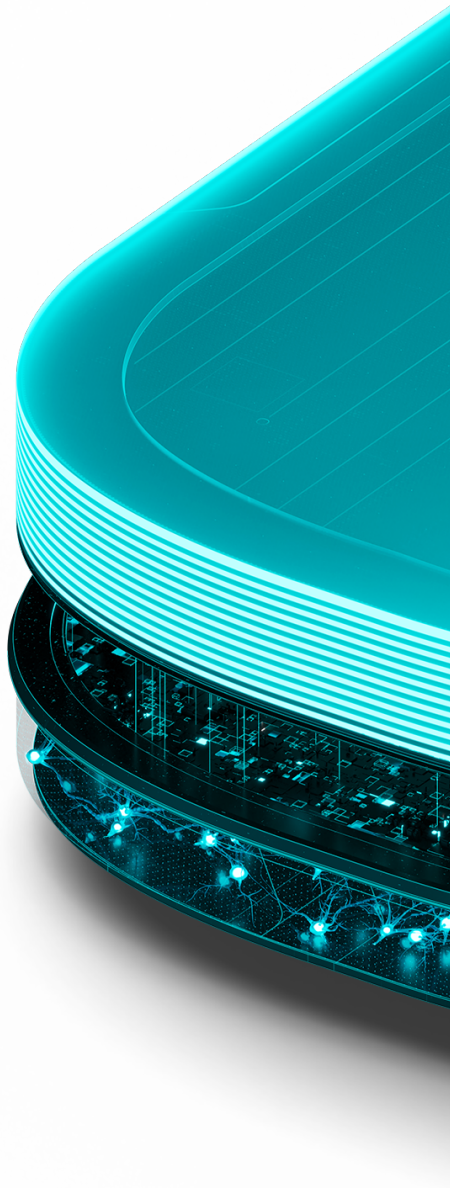
25,1 %

de las organizaciones que no detectaron ataques admite que las agresiones pudieron haber ocurrido sin que sus sistemas se enteraran, por no contar con la tecnología suficiente para detectarlo.

Conclusión: 4 de cada 10 organizaciones en América Latina carecen de la capacidad analítica suficiente para auditar su seguridad real, al considerar el desconocimiento técnico y la sospecha de incidentes no registrados.

Comportamiento por sectores industriales

El análisis del comportamiento sectorial demuestra cómo la exposición al riesgo se relaciona directamente con la visibilidad técnica, la tasa de incidentes y las brechas observadas en cada vertical de negocio.



Manufactura

Registra la tasa de incidentes más alta de la región, donde el 62,7 % de las empresas de manufactura detectó intentos de ataque. También concentra una de las tasas más altas de phishing: el 81,1 % de las firmas industriales reportó este tipo de incidentes. Además, presenta la menor tasa de incertidumbre, con el 5,1 % de las empresas encuestadas que manifestaron no saber si fueron blanco de ataque.

Banca/Finanzas

Casi 3 de cada 5 entidades financieras (57,8 %) detectaron intentos de ataque en el último año, lo que lo convierte en el segundo sector más atacado. Compensa este riesgo liderando la adopción de tecnologías avanzadas (DLP: 57,6 %, Threat Intelligence: 37,6 %, EDR: 69,1 %)

Incidentes y brechas de visibilidad

Gobierno, Educación y Salud completan la radiografía por sector, mostrando realidades opuestas entre la alta exposición ciudadana y la falsa sensación de seguridad por falta de detección.

Gobierno

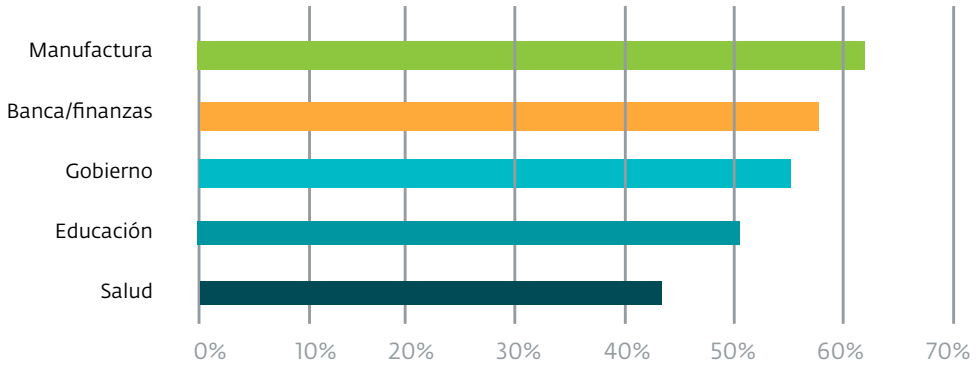
El 54,5 % de las instituciones gubernamentales encuestadas reportó actividad maliciosa. Exposición elevada de datos ciudadanos. El phishing lidera como vector con un 72,6%, seguido de accesos no autorizados (43 %).

Educación

Exactamente la mitad de las instituciones educativas (50,6 %) fue blanco de ataques. Presenta el índice de incertidumbre más alto de la muestra: 21,2% no sabe si fue atacado. El phishing alcanza aquí su pico regional (81,4 %).

Salud

Registró la cifra más baja de la región. El 44,7 % de los encuestados confirmó intentos de ataques. Sin embargo, esto no necesariamente indica que sea el menos atacado. Presenta la tasa de respuestas "No" más alta (42,1 %), pudiendo estar relacionado con una menor capacidad de detección real.



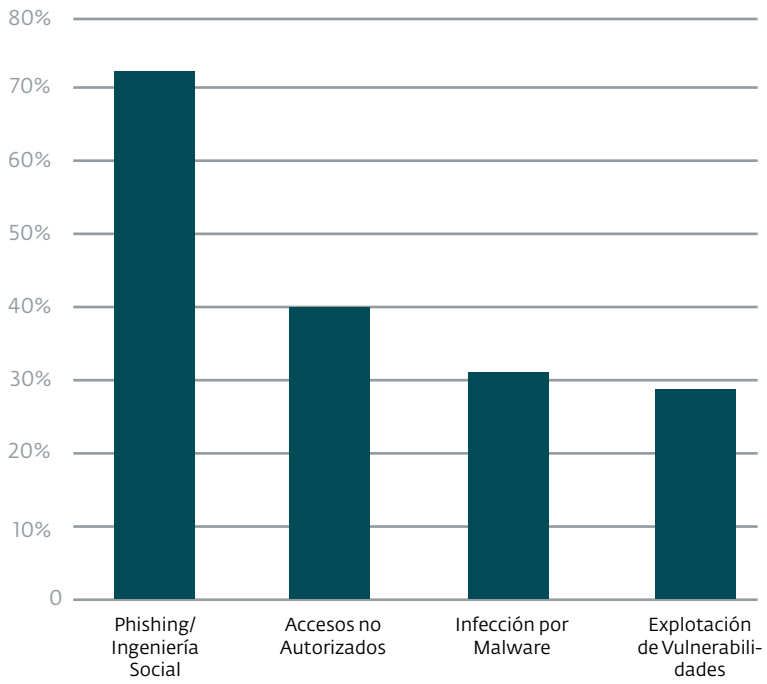
Tasa de Ataques Detectados por Sector

2. Vectores y tipos de ataques incidentados

Phishing, accesos no autorizados y malware. El análisis de las principales puertas de entrada utilizadas por los atacantes.

En las empresas que registraron incidentes, los principales tipos de ataque e incidentes detectados se distribuyeron de la siguiente manera, posicionando a la ingeniería social y las brechas de identidad a la vanguardia:

Principales Vectores e Incidentes de Ciberataques en la Región



Vectores y tipos de ataques incidentados

73 %

de las organizaciones fue blanco de ataques de phishing o ingeniería social

El phishing se posiciona como el vector dominante y transversal en la región. Afecta especialmente a Educación (81,4 %), Manufactura (81,1 %) y Banca (79,6 %). Salud se ubica como el sector menos afectado por esta vía, con un 67,6 %.

40 %

de las empresas sufrió accesos no autorizados

Segundo vector más común mediante fuerza bruta, secuestro de sesiones y credenciales expuestas. El sector más afectado es Educación con un 51,2 %, seguido de Informática/Tecnología (43,3 %) y Gobierno (43 %).

Intrusiones y vulnerabilidades

La falta de higiene básica en sistemas obsoletos y el secuestro de activos completan la escala de incidentes, variando significativamente su impacto según la infraestructura del sector.

31,6 %

Infección por Malware

Abarca ransomware, troyanos y spyware. El sector Salud duplica el promedio regional registrando un 52,9 % de incidentes por este vector.

29,2 %

Explotación de vulnerabilidades

Este vector suele asociarse a la falta de procesos de parcheo y actualización de sistemas. Lideran Salud (38,2 %) and Educación (30,2) por entornos con infraestructura más antigua y ciclos lentos.

8,4 %

Secuestro o Filtración de Información

Aunque es el de menor prevalencia, representa el de mayor impacto operativo. Informática/Tecnología tiene la tasa más alta (12,2 %). Los incidentes detectados se completan con accesos no autorizados (40%), infecciones con malware (31,6 %), explotación de vulnerabilidades (29,2 %) y secuestro o filtración (8,4 %).

3. El factor inteligencia artificial: entre el temor y la desregulación

Cómo se percibe el riesgo de la IA y el vacío de gobernanza interna en las empresas de América Latina.

La percepción del riesgo frente al desarrollo de la Inteligencia Artificial se enfoca principalmente en la automatización de amenazas avanzadas y la suplantación de identidad en sectores clave.

56,3 %

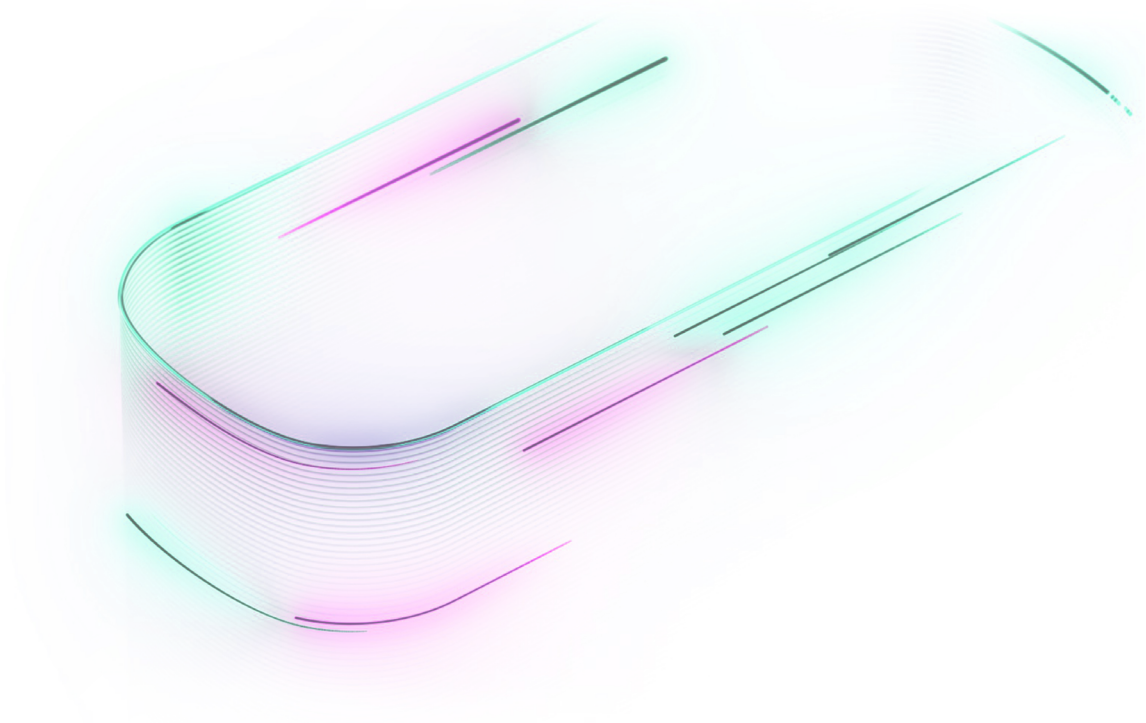
de profesionales

identifica el desarrollo de ataques más sofisticados y automatizados como la principal amenaza de la IA. Esta percepción escala al 74,6 % en Manufactura y al 63,5 % en Educación. El sector de Manufactura registra el nivel de preocupación más alto: el 74,6 % de los profesionales ve en la IA una amenaza de alta sofisticación.

19,6 %

de encuestados

señala la suplantación de identidad mediante deepfakes como el peligro principal, siendo el sector de Informática/Tecnología el más preocupado por este vector (24,2 %).



Políticas y madurez regulatoria interna

La adopción de herramientas de IA muestra una asimetría marcada en el control corporativo, dividiéndose el mercado entre un vacío absoluto y regulaciones que varían por sector.

Principales hallazgos

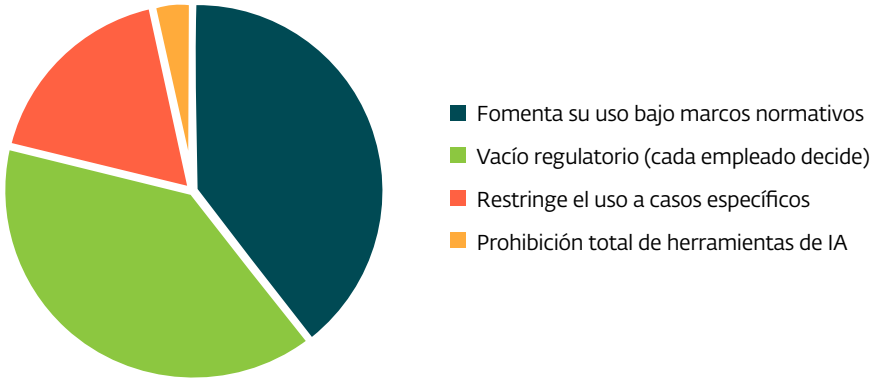
39,2 %
opera en vacío regulatorio absoluto dejando la decisión al empleado;

39,7 %
fomenta el uso bajo marcos internos;

17,8 %
restringe a casos específicos y

3,4 %
aplica una prohibición total.

Modelos de gobernanza de IA en organizaciones de la región



Los extremos sectoriales

Educación es el sector más desregulado; el 58,8 % de las instituciones no tiene ningún tipo de regla sobre la IA. En contraste, en Banca financiera el 47,6 % de las entidades fomenta su uso, pero bajo estrictas normativas internas.

4. Madurez tecnológica: la brecha de las defensas

Análisis de la asimetría entre la adopción de herramientas perimetrales básicas y capacidades analíticas avanzadas.

El análisis demuestra una marcada asimetría entre las defensas básicas perimetrales y las herramientas analíticas avanzadas. Esta distancia presenta un modelo más reactivo que proactivo.

Nivel de adopción de tecnologías Firewall (85 %), Backup (82 %), VPN (73 %), Doble autenticación (2FA) (57 %), EDR (52 %), DLP (36 %) y Threat Intelligence (23 %).

Observaciones: La industria financiera se presenta como la más madura con mayor adopción de tecnologías avanzadas. Gobierno registra la vulnerabilidad más preocupante en controles de acceso: solo el 41,6 % implementó la doble autenticación. Threat Intelligence es la tecnología menos adoptada en América Latina.

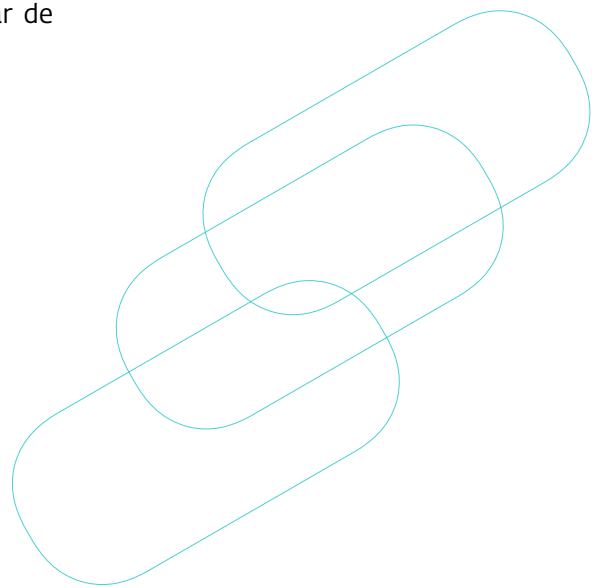
5. Hábitos de los usuarios

El eslabón humano es uno de los más importantes. Compartimos datos sobre la adopción del uso de antivirus, doble factor de autenticación y la protección de los dispositivos corporativos.

El análisis enfocado en empleados no técnicos (19,3 % de encuestados) expone vulnerabilidades críticas asociadas al factor humano, revelando una brecha entre la seguridad de equipos tradicionales y la protección de la identidad.

Dispositivos corporativos desprotegidos.
Aunque el 81,4 % utiliza antivirus en sus equipos de trabajo, el descuido de la identidad es alto: solo el 52,2 % activa el doble factor de autenticación en sus cuentas laborales, y 1 de cada 2 lo implementa en sus accesos de carácter personal.

Seguridad en dispositivos móviles (el gran olvidado)
El teléfono móvil corporativo se consolida como el punto más vulnerable. 1 de cada 4 empleados (26,9 %) reconoce abiertamente que no utiliza ninguna solución ni medida de seguridad en su dispositivo celular de trabajo.



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

Cybersecurity
Progress. Protected.

esetla @esetla @esetla ESET Latinoamérica