
THREAT LANDSCAPE
2025 → 2026
AXUR

Resumen

Mensaje de Axur

En 2025, la ciberseguridad vivió una paradoja evidente. Contamos con más datos, más visibilidad y más herramientas que nunca, y aun así, nunca hemos estado tan sobrecargados de alertas. El desafío ya no radica en saber qué está sucediendo, sino en transformar la información en acción.

El panorama ha cambiado. Los ataques a la cadena de suministro se han vuelto estratégicos, apuntando a la base: repositorios, bibliotecas y soluciones que sostienen ecosistemas completos. Y, cada vez más, grupos de amenaza han explotado a los insiders, el vector interno utilizado por actores maliciosos para comprometer entornos con precisión y discreción.

Es en este contexto que Axur viene fortaleciendo su misión de entregar datos estructurados, enriquecidos y priorizados. El lanzamiento de Axur Command representa un paso más allá, llevando las automatizaciones al siguiente nivel y permitiendo que las políticas de validación sean ejecutadas de forma autónoma.

Para 2026, nuestra visión es clara. La consolidación de los datos y la capacidad de actuar de manera integrada serán los grandes diferenciadores. Axur quiere ser, para la superficie de ataque, lo que las plataformas de observabilidad son para la ingeniería: un sistema nervioso central. Un punto único donde todo se conecta, se prioriza y se resuelve.

Este informe presenta nuestra lectura del panorama de amenazas de 2025, con tendencias, datos y perspectivas prácticas para el año que viene. Esperamos que ayude a los equipos de seguridad a priorizar mejor, actuar más rápido y, sobre todo, anticipar riesgos antes de que se conviertan en incidentes.

La tecnología sigue avanzando, y con ella llegan nuevas posibilidades. Nuestro papel es garantizar que ese avance ocurra con seguridad, confianza y responsabilidad.

Cuente con nosotros en esta jornada.

Fábio Ramos
CEO, Axur.

Resumen Ejecutivo

Principales cifras

- +6 mil millones de credenciales nuevas y únicas detectadas
- Los casos de phishing suman 71.399 páginas detectadas
- Los casos de uso fraudulento de marca crecen, con 454 mil incidentes
- Removimos más de 343 mil contenidos fraudulentos a través de los flujos automatizados de takedown
- 395 millones de tarjetas de crédito y débito detectadas
- El phishing crece un 65% para el sector financiero
- El registro de dominios similares crece más del +1000%
- Los perfiles falsos y la exposición de información continúan siendo utilizados para atacar ejecutivos y VIPs, con más de 19 mil incidentes

Boletines destacados

Crítico

Robo de 1,5 mil millones de dólares en Bybit perpetrado por el Grupo Lazarus: revelado el exploit

Obtenga más información ↗

Crítico

Explotación del Zero-Day en SAP NetWeaver: amenaza de ejecución remota de código

Obtenga más información ↗

Crítico

UNC6395 explota tokens OAuth en una sofisticada filtración de datos de Salesforce

Obtenga más información ↗

Alto

Brecha en el GitHub de Red Hat: una amenaza de alto riesgo para la cadena de suministro

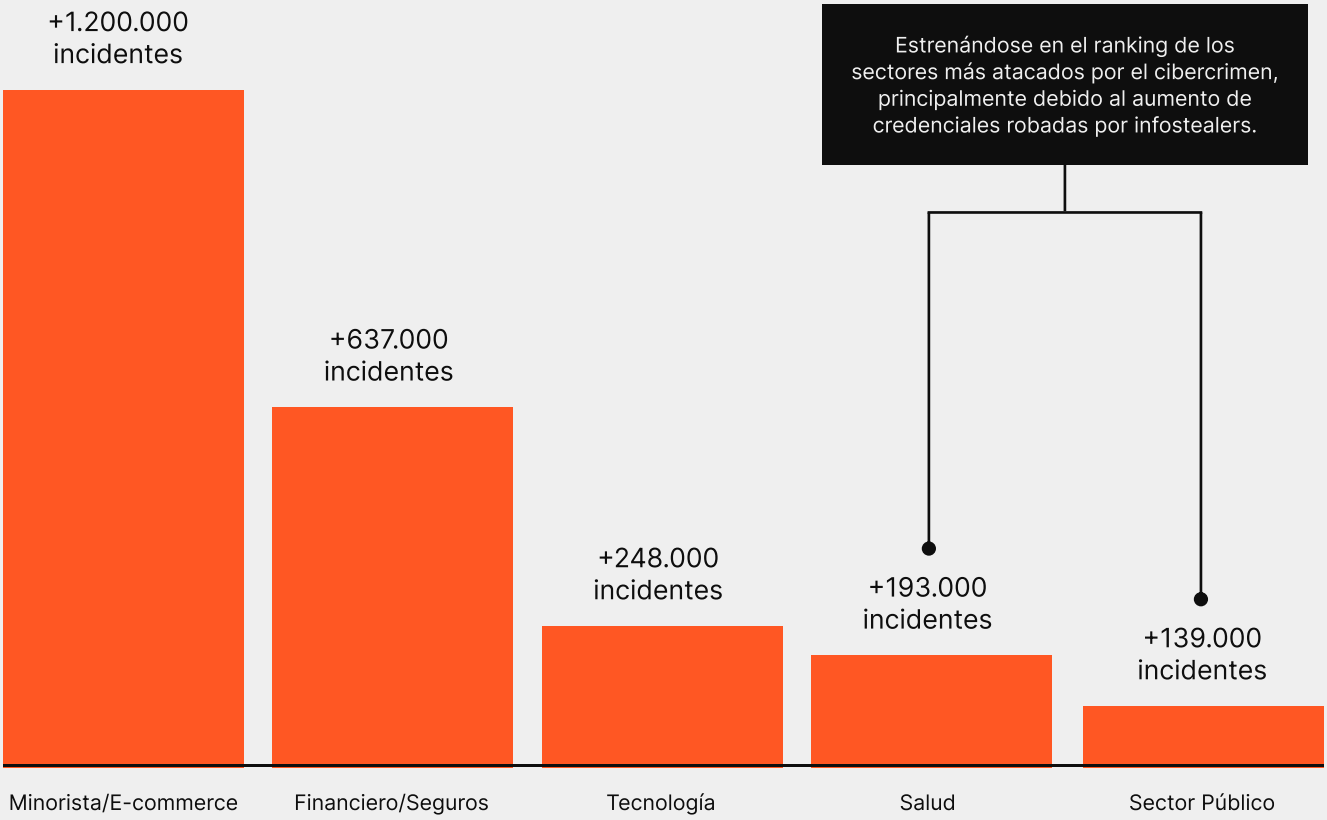
Obtenga más información ↗

Crítico

Cloudflare frustra un ataque DDoS récord de 22,2 Tbps

Obtenga más información ↗

Ranking de sectores por incidentes



Sectores más atacados por phishing

Financiero/Seguros +65%
24.959 páginas detectadas

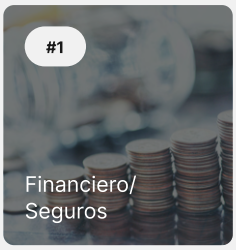
Minorista/E-commerce
21.558 páginas detectadas

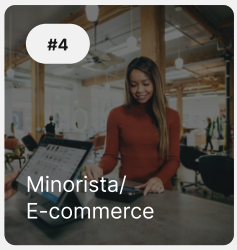
Tecnología
7.572 páginas detectadas

Alimentos/Bebidas
5.431 páginas detectadas

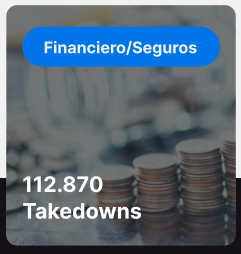
Transporte/Logística
3.594 páginas detectadas

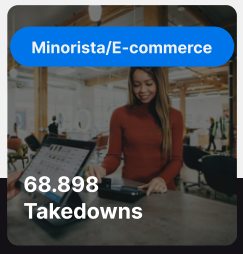
Sectores más atacados en la deep & dark web

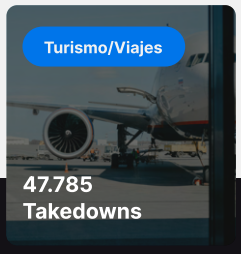


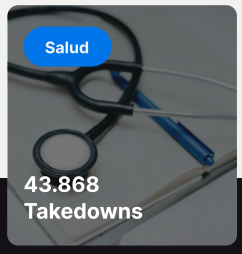


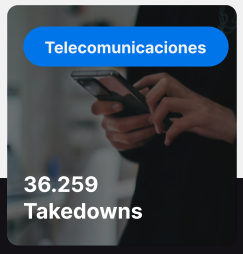
Ranking de takedowns



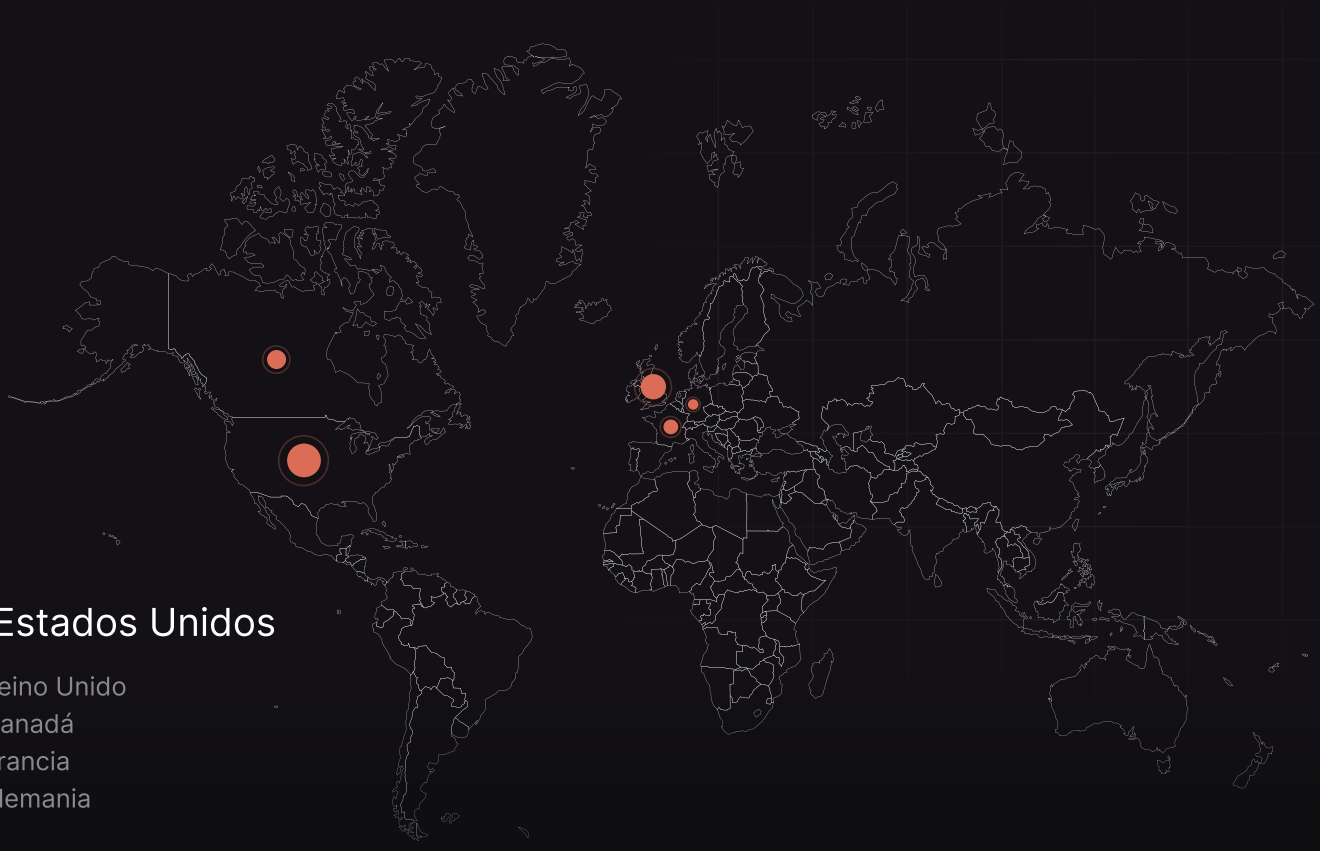








Localizaciones más afectadas



1º Estados Unidos

2º Reino Unido
3º Canadá
4º Francia
5º Alemania

Tendencias para 2026

Agentes de IA ganan autonomía

Herramientas que hoy actúan como asistentes pasarán a tomar decisiones operativas, escalando respuestas, priorizando investigaciones y activando remediaciones automatizadas. Esto acelera la defensa, pero también crea puntos de decisión que exigen una gobernanza estricta: ¿quién autoriza qué puede ejecutar la IA?

Los delincuentes consolidan el uso de IA

La misma capacidad de orquestar y aprender en tiempo real ha sido incorporada a los ataques, con la generación automática de campañas de phishing hiperpersonalizadas, fuzzing guiado por modelos y una variación masiva de payloads para evadir las detecciones.

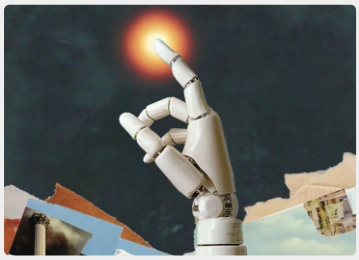
La carrera por la soberanía digital

Las regulaciones y políticas nacionales fragmentarán los flujos de datos y exigirán arquitecturas locales o híbridas, lo que redibuja las cadenas de confianza, incrementa la complejidad de cumplimiento normativo y crea nuevos vectores operativos para quienes no se adapten.

Amenazas olvidadas vuelven a la actividad

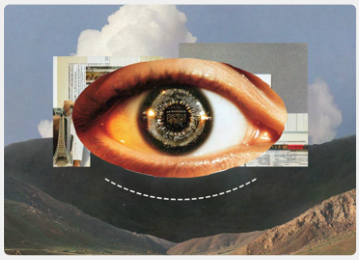
Hardware legado en entornos IoT/OT, mal mantenido o expuesto, está siendo reactivado como recurso en botnets y campañas persistentes.

Recomendaciones para los próximos desafíos



Prepárese para la era de los agentes

Los agentes autónomos están asumiendo tareas críticas de respuesta e investigación. Antes de delegar acciones, establezca políticas de autonomía, límites operativos y mecanismos de auditoría. Defina quién autoriza las ejecuciones automatizadas y cómo revocar instrucciones en caso de comportamiento anómalo.



Mire más allá del perímetro

La mayor parte de las exposiciones comienza fuera de los activos internos. Monitorear credenciales filtradas, artefactos de build y menciones de marca en fuentes externas es esencial para anticipar incidentes. La detección temprana en entornos externos reduce significativamente el tiempo medio de detección (MTTD).

Proteja los activos internos críticos

Desarrolladores y equipos de soporte siguen entre los principales objetivos de phishing y credential stuffing. Implemente MFA resistente a “push bombing”, segregación de funciones y monitoreo del uso de herramientas de acceso remoto. Ataques exitosos contra estos perfiles tienen un efecto multiplicador sobre toda la infraestructura.

Mapee la superficie de terceros

La alerta de CISA sobre el compromiso a gran escala del ecosistema npm evidenció el riesgo creciente en las cadenas de software. Dependencias, APIs y pipelines de socios amplían la superficie de ataque y exigen validación continua de integridad y permisos, ya que un único proveedor comprometido puede propagar código malicioso a todo el entorno.

Panorama de ciberseguridad

Es difícil resumir el escenario de ciberseguridad en unas pocas amenazas o desafíos. En cierta forma, el desafío está precisamente en la diversidad de amenazas y en el volumen de aspectos que requieren atención.

En los últimos años, la ciberseguridad se ha vuelto más sensible a las necesidades de cada negocio, lo que contribuye a la gestión de riesgos y a la priorización de proyectos. En este sentido, no podemos dejar de mencionar que el entorno de negocios también es desafiante, con incertidumbres regulatorias y comerciales a escala global que repercuten incluso en las pequeñas y medianas empresas.

El entorno tecnológico también ha cambiado. Algunas empresas han reducido la proporción de colaboradores trabajando de forma remota, pero ni siquiera el fin del trabajo remoto eliminaría el "dato remoto", almacenado en la nube, en socios y en terceros. Sin embargo, como esto no siempre es tan evidente, existe el riesgo de que la seguridad del acceso remoto sea descuidada.

Al mismo tiempo, hay una demanda creciente de servicios interactivos e inteligentes, ya sea en el comercio electrónico o en la prestación de servicios. Nuevas modalidades de interacción también abren oportunidades para los delincuentes.

> Todo esto viene ocurriendo sin que haya una tregua en la explotación de vulnerabilidades o en los incidentes de ransomware.

Al contrario: las vulnerabilidades en dispositivos de red son cada vez más preocupantes y ahora se mencionan en ataques de ransomware y filtraciones de datos. Mientras tanto, las estafas de ingeniería social se desplazan parcialmente de los usuarios finales hacia los profesionales de TI, alcanzando a un nuevo público de formas inesperadas.

Dispositivos de borde se convierten en un objetivo prioritario

Los ataques a dispositivos de borde (principalmente VPNs y firewalls) se destacaron en 2024 y se consolidaron en 2025.

La explotación de vulnerabilidades fue un punto especialmente preocupante en estos ataques, pero no el único. Los atacantes también lograron realizar intrusiones utilizando credenciales robadas e incluso ataques de fuerza bruta. Algunos de estos incidentes llamaron la atención por lograr evadir la autenticación en dos pasos, ya sea mediante el uso de vulnerabilidades o, posiblemente, gracias a la filtración de las claves utilizadas para generar códigos únicos.

El Catálogo de Vulnerabilidades de la Agencia de Ciberseguridad de los Estados Unidos (CISA) indica que dispositivos y softwares de diversos fabricantes tuvieron vulnerabilidades explotadas a lo largo del año. Broadcom, Cisco, Fortinet, Ivanti, Juniper, Palo Alto Networks y SonicWall son algunas de las marcas que aparecen en la lista de 2025.

> Los objetivos de la explotación de estos dispositivos fueron bastante diversos.

Parte de los ataques tuvo como finalidad invadir redes corporativas para instalar ransomware y llevar a cabo el ya conocido esquema de extorsión, en el que los atacantes exigen un rescate para recuperar los archivos cifrados o para no divulgar la información exfiltrada de los sistemas comprometidos.

Otro conjunto de ataques fue atribuido a actores vinculados a gobiernos. En estos casos, los objetivos eran normalmente empresas operadoras de infraestructura crítica, como compañías de telecomunicaciones, de energía o entidades gubernamentales.

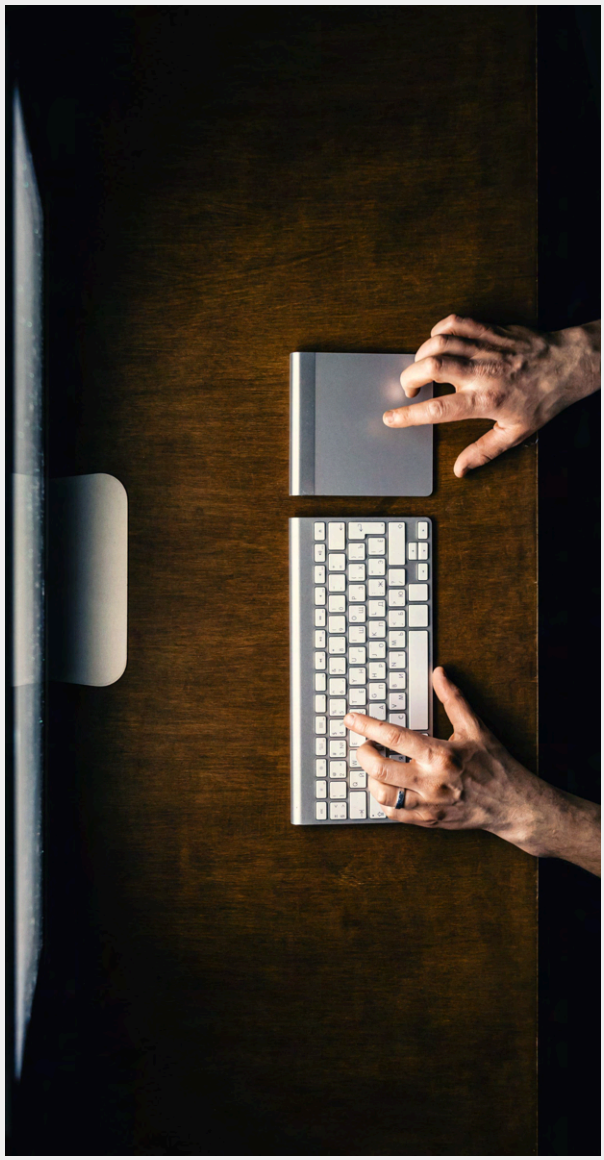
En el caso de los ataques contra routers domésticos, los invasores suelen instalar un malware para conectar el dispositivo comprometido a una red zombi. Estos equipos pueden entonces ser utilizados en ataques DDoS o como proxies de los delincuentes, ocultando el origen de otras actividades. Al menos parte de los códigos utilizados se basa en Mirai, un malware de IoT detectado por primera vez en 2016.

Ataques de ingeniería social apuntan a equipos de soporte y reclutamiento

Desde hace algunos años, la actuación del grupo Scattered Spider viene demostrando la efectividad de enfoques innovadores en ataques cibernéticos, principalmente mediante el uso de ingeniería social. Esto volvió a ocurrir en 2025,

> con intrusiones que comenzaron a partir de llamadas telefónicas ilegítimas pidiendo ayuda para restablecer contraseñas.

Esta estrategia de contacto con los equipos de soporte de TI se diferencia de lo que es más común en la ingeniería social, que son los ataques directos contra los usuarios finales. En estos nuevos casos, los estafadores se hacen pasar por usuarios que solicitan ayuda con sus credenciales y, de esa forma, logran obtener una credencial válida para acceder a la red de la empresa o a alguna plataforma.



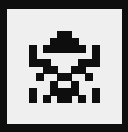
Los ataques más notorios con este enfoque ocurrieron en el Reino Unido, donde cadenas de retail se vieron afectadas y reportaron pérdidas significativas derivadas de las intrusiones.

Las tácticas de ingeniería social asociadas al empleo y al reclutamiento también merecen atención. Este tipo de fraude puede dirigirse tanto contra las empresas como contra los candidatos.

En el caso del fraude contra reclutadores, suele ocurrir especialmente en las etapas en que el candidato tiene la posibilidad de enviar algún material a la empresa. Cuando el reclutador abre el archivo recibido, puede terminar comprometiendo su propio sistema y, potencialmente, la red de la organización.

Las estafas contra candidatos se desarrollan de forma similar. Los delincuentes envían ofertas de empleo falsas, invitando al profesional a participar en un supuesto proceso de selección. El material de apoyo para participar en el proceso estará contaminado con malware, y las consecuencias pueden alcanzar incluso la red corporativa, en caso de que el profesional se encuentre actualmente empleado.

Curiosamente, estas fraudes frecuentemente involucran vacantes y profesionales de TI. Es muy probable que los objetivos sean seleccionados cuidadosamente para impactar a empresas o proyectos específicos. Proyectos relacionados con el mercado de criptomonedas, por ejemplo, suelen estar entre los más buscados por los ciberdelincuentes.



Scattered Spider

Colectivo de ciberdelincuentes con motivación financiera, activo desde 2022 (Estados Unidos y Reino Unido).

Principales tácticas

Ingeniería social (spear phishing, smishing, vishing), intercambio de SIM, fatiga de MFA y uso de herramientas legítimas de acceso remoto (SupremoControl, AnyDesk, ConnectWise, Splashtop).

Malwares utilizados

BlackCat, Qilin, Akira, DragonForce; stealers como Racoon y Meduza.

Víctimas destacadas

MGM Resorts, Caesars Entertainment, Snowflake y grandes instituciones financieras.

Objetivo

Robo y extorsión de datos para obtener ganancias financieras.

Comentario del especialista

Pedro Moura

Investigador del
Axur Research Team

Aunque Scattered Spider se hizo conocido como afiliado de grupos como BlackCat/ALPHV y, más tarde, DragonForce, el colectivo evolucionó en 2025 para desarrollar su propio ransomware, abandonando el papel de intermediario. La CISA confirmó esta transición en una alerta reciente, destacando el aumento de la sofisticación operativa del grupo.

El supuesto “cese de operaciones” y el banner de incautación exhibido en sus dominios onion son ampliamente interpretados como acciones de PsyOps, diseñadas para confundir a la comunidad de seguridad y ocultar una posible reestructuración.

Extorsión triple vuelve el ransomware más difícil de contener

Los ataques de ransomware continúan representando una amenaza significativa para las empresas, y casi todas las actividades maliciosas registradas terminan teniendo algún tipo de relación con este tipo de ataque.

El modelo de RaaS (ransomware as a service – ransomware como servicio) establece una estructura en la que diversos "afiliados" se encargan de encontrar maneras de instalar el malware dentro de las redes corporativas. De este modo, un mismo ransomware puede estar asociado a múltiples estrategias de ataque.

Phishing, ataques a la cadena de suministro (supply chain), abuso de credenciales, reclutamiento de colaboradores internos, explotación de vulnerabilidades: todas estas tácticas se utilizan para invadir la infraestructura de TI e iniciar el golpe de ransomware.

Un punto de atención en el contexto del ransomware se refiere a las modalidades de extorsión en la fase final del incidente. Tradicionalmente, el ransomware cifra los archivos de los sistemas para paralizar las actividades del negocio y luego exige un pago a cambio de la clave capaz de restaurar los datos y recuperar los sistemas.

Ante la frecuencia de estos ataques, muchas empresas adoptaron procesos de recuperación robustos para restaurar los sistemas a partir de copias de seguridad protegidas, lo que redujo el poder de coacción de los delincuentes. Los estafadores respondieron entonces con tácticas de extorsión doble y triple, en las que la empresa también es amenazada con la exposición de datos corporativos y con ataques DDoS, situaciones para las cuales la organización puede no estar preparada o incluso no tener cómo evitar.

> Más recientemente, los criminales también han apostado por intentos de extorsión basados exclusivamente en la amenaza de exponer datos corporativos.

Aunque los atacantes prescindan del bloqueo de sistemas y archivos mediante cifrado, todas las demás características del golpe siguen el mismo patrón del ransomware.

Comentario del especialista

La extorsión doble ya está consolidada y aparece casi como una práctica obligatoria en el escenario actual. Además, existen extorsiones crecientes relacionadas exclusivamente con la filtración de datos, sin que necesariamente haya cifrado.

Alisson Moretto

Head de Threat Hunting en Axur

Al prescindir del cifrado de los datos, los delincuentes pueden intentar la extorsión incluso cuando no fue posible obtener acceso de escritura a determinados sistemas, o cuando saben que los archivos pueden recuperarse con facilidad (como en el caso del almacenamiento en la nube).

Los argumentos durante la "negociación" con las empresas también vienen evolucionando en esa misma dirección. Las bandas explotan el temor a repercusiones legales y a daños reputacionales derivados de la filtración de datos para convencer a la víctima de efectuar el pago, incluso recurriendo a supuestos "abogados" que dicen estar ofreciendo asesoría jurídica.

Ataques a la cadena de proveedores se vuelven recurrentes

Los ataques contra la cadena de proveedores (supply chain) se han consolidado como un vector robusto para incidentes de ciberseguridad. Los casos históricos más conocidos son posiblemente el de la minorista Target, que sufrió una filtración de datos a partir del acceso de un proveedor de servicios de climatización en 2013, y el de SolarWinds, cuya solución de software fue adulterada por un atacante para implantar backdoors en varios clientes.

En los últimos años, la noción de riesgos en la supply chain se ha ampliado en varios aspectos. El uso de plataformas estandarizadas y de soluciones de software como servicio (SaaS) hizo posible una nueva categoría de ataques masivos, con o sin el uso de vulnerabilidades específicas.

Los casos de MOVEit Transfer (2023) y Cleo (2024) son ejemplos de incidentes a gran escala que involucraron alguna vulnerabilidad en un software. En cambio, los ataques de robo de datos que explotaron los servicios de Snowflake (2024) y Salesloft (2025) utilizaron, respectivamente, credenciales robadas e ingeniería social.

Estas campañas recurrentes muestran que la estrategia de atacar proveedores y terceros se ha consolidado entre los atacantes. Los ataques contra terceros siempre fueron posibles, por supuesto, pero ahora son intencionales y estratégicos, incluso para obtener información privilegiada (como credenciales) o acceder a un camino más sencillo para invadir la red del objetivo final.

La software supply chain se convierte en un vector de infección

Un subgrupo de los ataques a la supply chain son los ataques a la infraestructura de desarrollo de software, lo que normalmente se resume en el concepto de software supply chain. Esta definición puede incluir casos como el de SolarWinds y otras situaciones en las que los softwares son adulterados directamente, pero existe una categoría aún más específica de ataques centrada exclusivamente en los procesos de desarrollo de software.

En estos ataques, los delincuentes crean o modifican paquetes en repositorios como npm y PyPI, que son utilizados por ingenieros en otros softwares. De esta forma, el comportamiento malicioso se propaga a otros proyectos, alcanzando soluciones corporativas que usan ese código.

Es bastante común que pequeñas aplicaciones improvisadas para actividades administrativas de TI utilicen estos repositorios, por lo que no se puede descartar el riesgo directo solo porque la empresa no actúe formalmente en el desarrollo de software.

Además, existe un riesgo indirecto considerable cuando la organización utiliza otros softwares que dependen de paquetes presentes en estas bibliotecas o en servicios de apoyo al desarrollo que puedan ser comprometidos.

A lo largo de 2025, se observaron varios paquetes maliciosos en npm y PyPI. Los atacantes crearon múltiples paquetes falsos y alteraron paquetes legítimos, lo que fue posible tras el robo de las credenciales de los mantenedores.

Incidente de Salesloft muestra cómo la supply chain amplía el alcance de las intrusiones

Un incidente que afectó a Salesloft y a sus clientes, en agosto de 2025, ejemplifica varias de las estrategias de ataque que marcan el panorama del año. Se trató de un ataque a la cadena de suministro (supply chain) que comenzó con ingeniería social dirigida a colaboradores del área de TI para robar credenciales.

Los atacantes comprometieron a un ingeniero de la empresa, posiblemente mediante ingeniería social, para obtener una credencial de GitHub. Esa credencial fue utilizada para acceder a la infraestructura en la nube, desde donde los delincuentes extrajeron los tokens OAuth asociados a Drift, un chatbot de Salesloft.

Drift necesitaba estas autorizaciones OAuth para vincularse a las instancias de CRM de Salesforce de los clientes y acceder a los datos que sustentaban la experiencia personalizada ofrecida por el chatbot. Como esos tokens de OAuth daban acceso a datos corporativos de los clientes de Salesloft, varias empresas resultaron comprometidas.

Lea más ↗

2025 en cifras

Credenciales

La plataforma de Axur detectó 6 mil millones de nuevas credenciales únicas en 2025. Es importante destacar que, hasta el año pasado, nuestro informe traía el número total de credenciales detectadas. El cambio se debe a procesos implementados para ofrecer una verificación más precisa de los datos recopilados, en la misma línea de lo que comentamos sobre menos ruido y más alertas relevantes.

Con el aumento de grandes recompilaciones de datos divulgadas como si fueran una filtración nueva, es más importante que nunca ofrecer a los equipos de seguridad alertas curadas que eviten el retrabajo de revisar credenciales que se vuelven a compartir con frecuencia en grupos y foros del cibercrimen. Así, una credencial única se contabiliza como un conjunto de usuario y contraseña compartido solo una vez.

Esta cifra muestra que aún existe mucha actividad maliciosa con el objetivo de robar credenciales. Esas credenciales comprometidas circulan en los espacios del submundo criminal, alimentando diversas amenazas y estafas.

> Un punto de atención es que la mayoría de las nuevas credenciales (52,2 %) está vinculada a sistemas corporativos.

Es posible que estas credenciales otorguen acceso a sistemas que almacenan información comercial o personal cuya exposición podría perjudicar las actividades de la empresa o su reputación. En varios países, la filtración de datos personales también genera consecuencias legales.

Un ejemplo recurrente en 2025 fueron los ataques que utilizaron credenciales de VPNs y otros dispositivos de borde de red (edge devices).

Aunque la adopción de MFA reduzca los riesgos derivados de credenciales filtradas, los delincuentes han logrado combinar estas credenciales con fraudes de phishing, convenciendo a un analista de soporte para desactivar o reconfigurar la MFA. Como la contraseña ya está en manos de los atacantes, eso es suficiente para comprometer la cuenta.

La filtración de credenciales también incrementa el riesgo asociado a vulnerabilidades que permiten eludir la MFA.

Por estas razones, el monitoreo de credenciales filtradas es un mecanismo importante para aumentar la resiliencia de los procesos de autenticación en todos los sistemas corporativos, incluso cuando ya se utiliza una solución de MFA.

Phishing

> Axur detectó 71.399 páginas de phishing en 2025.

El phishing es uno de los fraudes cibernéticos más conocidos y constantes. En Axur, contabilizamos las páginas web donde el phishing ocurre, sin importar cuál sea el canal utilizado para llevar esas páginas a las víctimas. Así, además de los enlaces a sitios falsos difundidos por correo electrónico, también se incluyen páginas de smishing (phishing por SMS) y sitios promovidos mediante anuncios pagados.

Tras un aumento significativo en la detección de páginas de phishing en el año anterior, el volumen total de páginas se mantuvo estable en 2025.

La detección de phishing puede ser una aliada en el proceso de takedown para retirar la fraude del aire, reduciendo el impacto sobre la marca y los consumidores. Con el uso de Clair (Cyber Lens for Anomaly and Impersonation Recognition), nuestro modelo de inteligencia artificial, es posible identificar páginas de phishing de forma confiable y automatizada.

Además, los atributos identificados por Clair se convierten en filtros que permiten una detección que va más allá del uso de palabras clave.

El 70 % de los fraudes de phishing no utilizan una palabra clave en el dominio

El 18 % no incluye la palabra clave en el código HTML de la página

Los casos de phishing que utilizan los colores de la marca, por ejemplo, se detectan mediante el monitoreo automatizado y pueden ser objeto de takedown automático. Además, es posible utilizar Threat Hunting para buscar URLs con diversos atributos.

Algunas búsquedas posibles:

→ Imitación de marca por elementos visuales: identifica sitios que imitan marcas conocidas o exhiben logotipos específicos. Por ejemplo, detectar distintos niveles de imitación de “NombreDeLaMarca” o encontrar sitios que muestren el “LogoDeLaMarca”.

→ Tipo de contenido y solicitudes de datos sensibles: sitios de phishing según el tipo de contenido, como páginas de inicio de sesión, páginas de error o sitios de comercio electrónico. También es posible identificar aquellos que solicitan información sensible, como contraseñas o datos de pago.

→ Análisis de dominio y ciclo de vida: dominios según sus fechas de creación o expiración, o con filtro por fechas recientes de detección para encontrar nuevas amenazas.

→ Referencias y atributos de URL: examina URLs o referencias específicas y filtra por atributos de dominio, subdominio o dominio de nivel superior (TLD) para refinar las búsquedas.

→ Contenido HTML: busca términos específicos presentes en el código de las páginas detectadas, como correos electrónicos, números de teléfono y otros datos.

Amenazas específicas por idioma y región: investigaciones en determinados idiomas o regiones permiten identificar campañas de phishing más localizadas.

División por sector

Al analizar el volumen de páginas de phishing según el sector de la marca utilizada en el fraude, observamos un aumento en la proporción de ataques dirigidos a bancos y entidades financieras. En el año anterior, el retail mantenía una ventaja cómoda en la parte superior de la lista, pero este no fue el caso en 2025.

Cabe recordar que fraudes que utilizan marcas del comercio minorista pueden fácilmente adoptar narrativas para robar tarjetas de crédito y otros datos financieros. Por lo tanto, una diferencia en el tipo de marca utilizada no caracteriza por sí sola un cambio en los intereses de los delincuentes.

Los datos de 2025 indican un cambio relevante en el foco de las campañas de phishing en Brasil. El sector Financiero/Seguros registró un aumento del 65 % en las detecciones, superando a Venta Minorista/E-Commerce. Este movimiento sugiere que los agentes de amenaza están redirigiendo esfuerzos hacia instituciones financieras, atraídos por el potencial de ganancia directa.

El sector de Transporte también mostró crecimiento. Estas estafas explotan el ecosistema de rastreo de entregas y el uso de páginas falsas de transportistas, ampliando la superficie de ataque contra consumidores y empresas del sector.

Evolución de los sectores más atacados por phishing entre 2024 y 2025

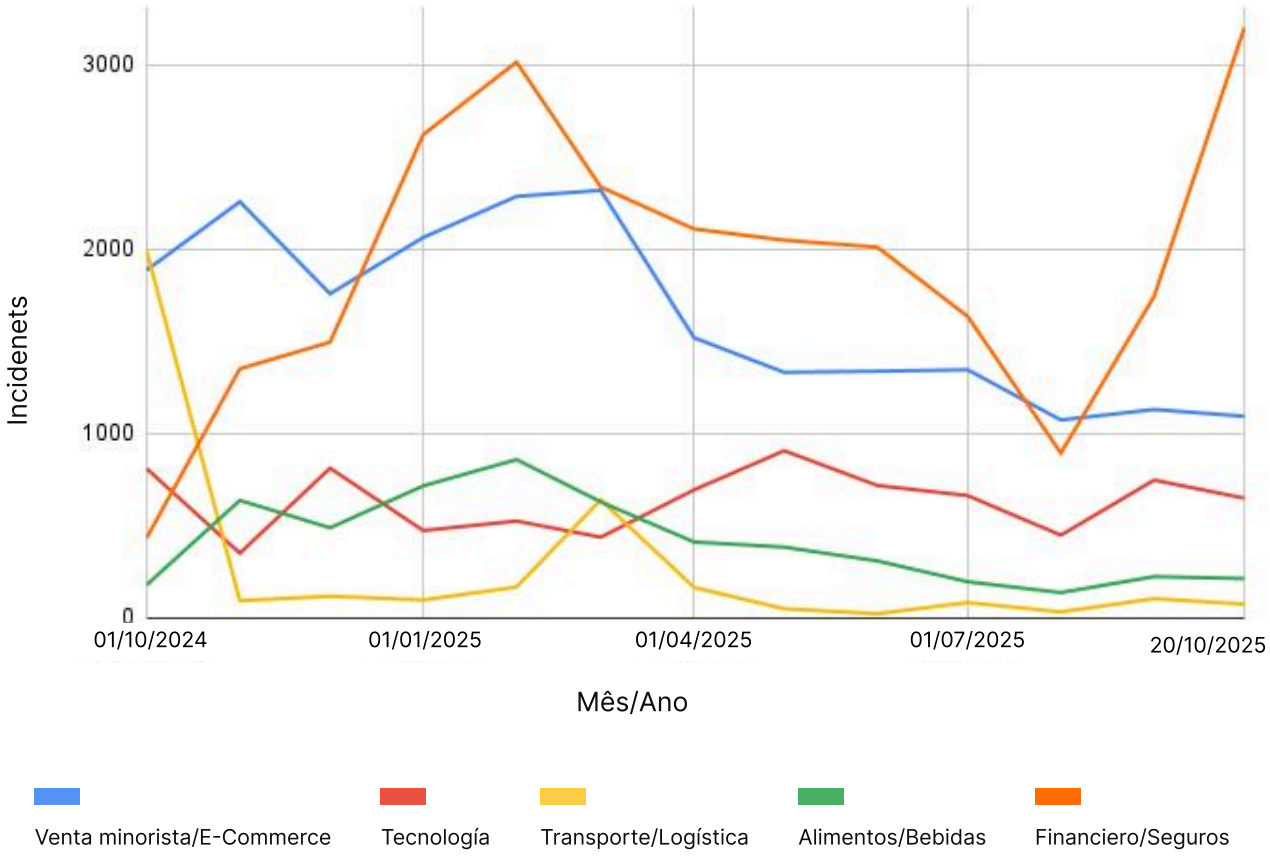
	2024	2025	
Venta minorista/E-Commerce	27.305	21.558	↓ -21%
Bancos/Financieras	18.915	24.959	↑ +65%
Tecnología	9.502	7.752	↓ -18%
Alimentos	3.462	5.431	↑ +56%
Transporte	3.330	3.359	↑ +0,87%

Tendencias en phishing: evolución por sector

En el recorte por sector, se observa un cambio relevante en la distribución de los incidentes de phishing. El segmento financiero/seguros asumió el liderazgo en volumen de ataques, superando al retail y e-commerce, que había ocupado la primera posición el año anterior. Esta inversión puede estar relacionada con el aumento en la explotación de credenciales corporativas y con el uso de integraciones SaaS como vector de acceso inicial.

Los sectores de transporte y logística presentaron oscilaciones puntuales, mientras que alimentos y bebidas mantuvieron una estabilidad relativa, con volúmenes menores.

Distribución de los incidentes de phishing por sector económico entre 2024 y 2025



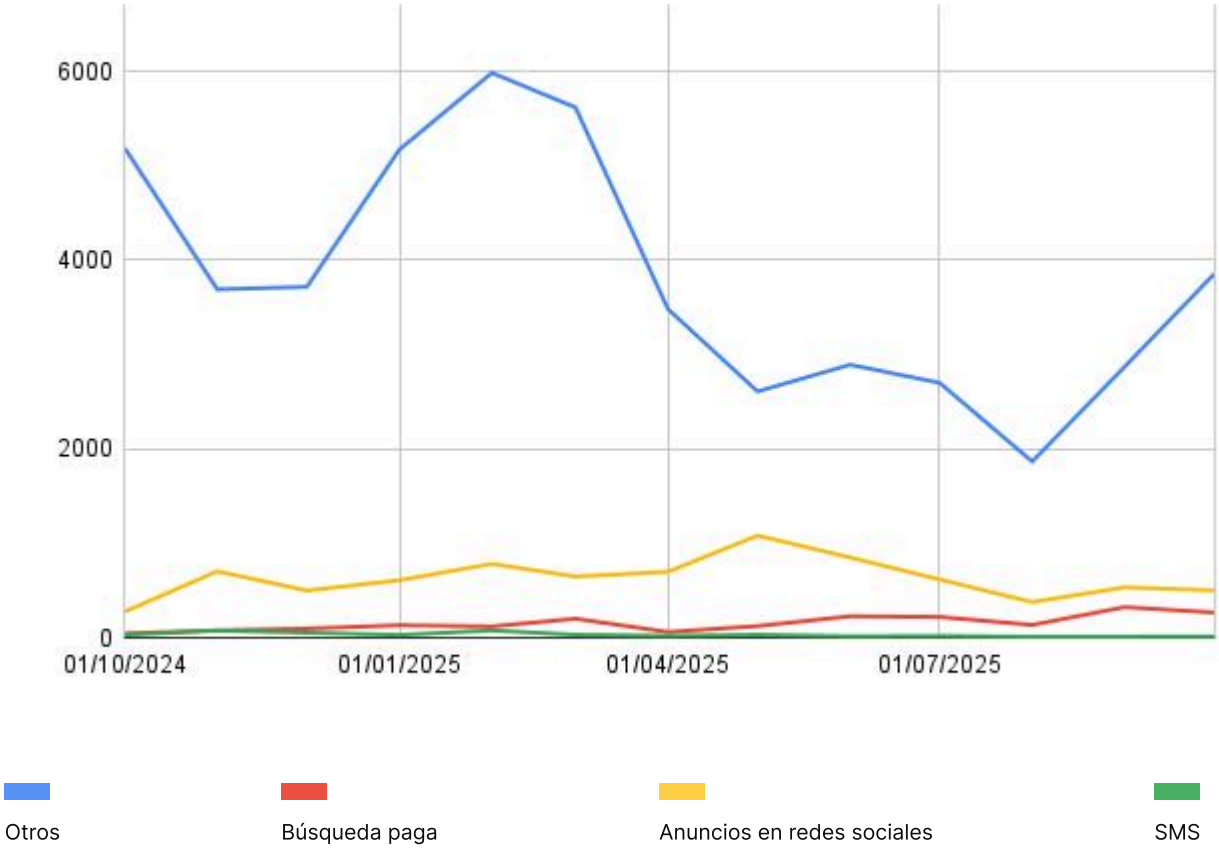
Tendencias en phishing: evolución por vector de ataque

En cuanto a los vectores de ataque, se observó una variación considerable a lo largo del año. Las campañas más tradicionales, agrupadas en la categoría otros —que incluye páginas falsas y sitios clonados— siguieron siendo predominantes, pero con un comportamiento irregular y picos concentrados en el primer trimestre.
Entre los canales específicos, los anuncios en redes sociales mantuvieron una presencia constante, mientras que el uso de búsqueda paga presentó un crecimiento gradual.
Los ataques mediante SMS se mantuvieron en un nivel reducido, aunque siguen utilizándose en campañas de corto alcance dirigidas a públicos específicos.

La diversificación de los objetivos y la ampliación de los canales de fraude sugieren que los atacantes vienen distribuyendo esfuerzos entre sectores y plataformas para maximizar el impacto de sus campañas.

Este escenario refuerza la necesidad de enfoques más amplios de monitoreo y correlación de amenazas, capaces de contemplar el ecosistema de exposición digital como un todo.

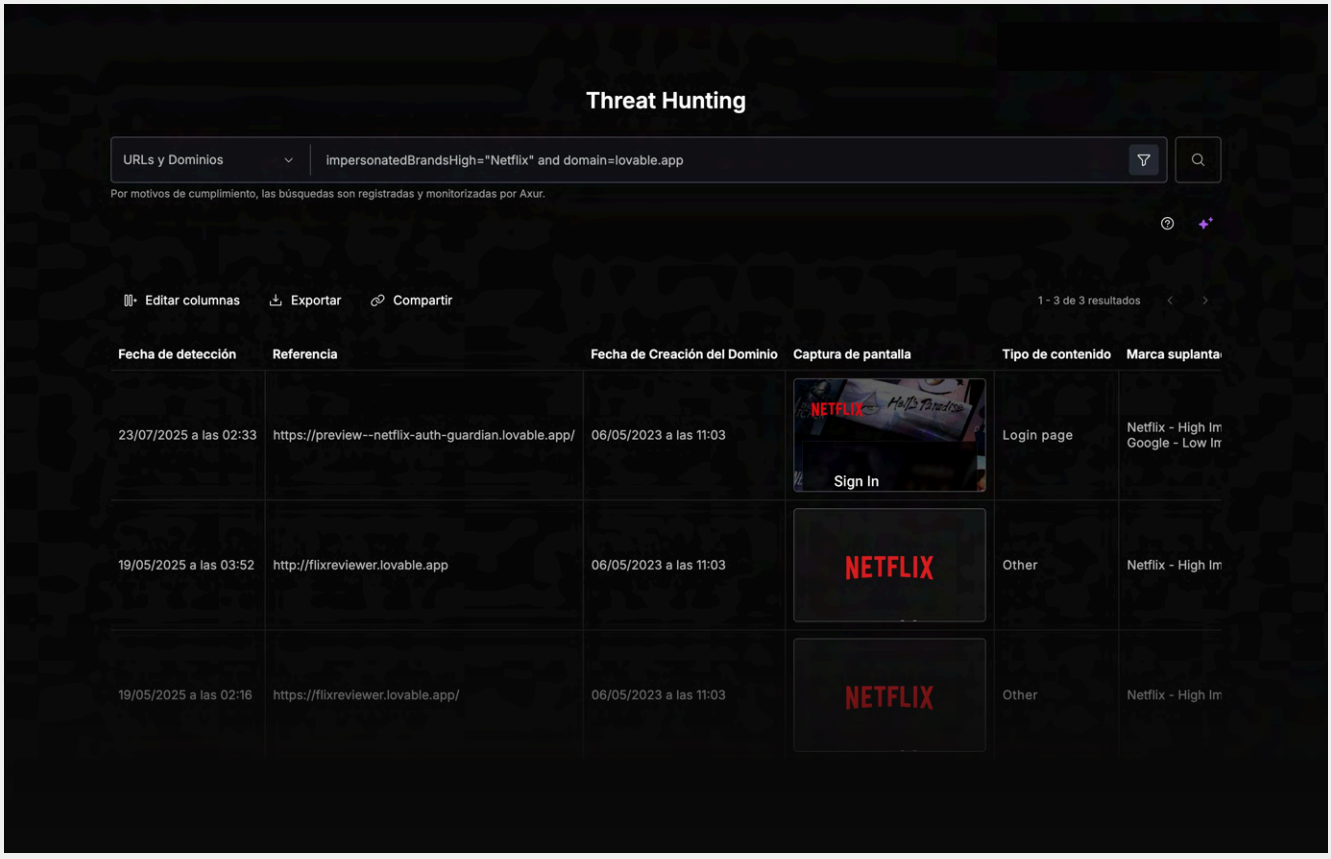
Evolución mensual de los principales vectores de ataque observados entre finales de 2024 y 2025.



IA acelera el phishing: páginas falsas creadas en minutos con herramientas como Lovable

Los grupos de fraude digital han incorporado herramientas de generación asistida por IA, como Lovable, para automatizar la creación de páginas de phishing con alta fidelidad visual. Estos constructores permiten replicar interfaces legítimas —bancos, proveedores de e-commerce, servicios de autenticación— en cuestión de minutos, sin exigir conocimientos técnicos avanzados.

El uso de modelos generativos para clonar flujos de inicio de sesión, ajustar textos persuasivos y adaptar el idioma al público objetivo acelera la producción y personalización de campañas, reduciendo el tiempo entre la concepción y la ejecución. Esta tendencia consolida el phishing como un vector de ataque altamente escalable y difícil de detectar, sobre todo cuando se combina con kits alojados en infraestructuras legítimas y dominios recién registrados.



Captura de pantalla de Threat Hunting de Axur muestra casos de phishing creados con la herramienta Lovable.

Uso de dominios de nivel superior

La lista de los dominios de nivel superior (TLDs) más utilizados por los delincuentes se mantuvo muy similar a la del año anterior. El creciente uso de .app evidencia que las plataformas de creación de sitios web con IA se han convertido en un recurso clave para los actores maliciosos. **Netlify, Vercel y Lovable representan el 75% de los casos de phishing que utilizan el TLD .app.**

Principales dominios (TLD) más utilizados entre 2024 y 2025

	2024	2025	
.com	26.612	20.921	↓ -21,4%
.online	9.147	4.861	↓ -46,9%
.site	5.062	6.392	↑ +26,3%
.shop	5.196	6.358	↑ +22,4%
.store	1.721	1.607	↓ -6,6%
.net	1.489	922	↓ -38,1%
.org	1.254	861	↓ -31,3%
.ru	1.017	552	↓ -45,7%
.de	928	895	↓ -3,6%
.xyz	997	494	↓ -50,5%
.app	-	1619	Nuevo
.top	-	952	Nuevo

Los TLD (dominios de nivel superior) son los sufijos de las direcciones web, como “.com” (que puede ser utilizado por cualquier persona u organización), “.gov” (exclusivo de sitios del gobierno de Estados Unidos) y “.uk” (sufijo de país).

La concesión de TLDs era bastante restringida en el pasado, ya que solo unas pocas instituciones estaban autorizadas a operarlos, normalmente para representar regiones o países (como “.br”, “.de”, “.jp”, “.ar”, entre otros).

Desde 2012, existe un procedimiento para solicitar la concesión de un generic top-level domain (gTLD), lo que flexibilizó la creación de nuevos sufijos. Cada TLD es operado por una entidad mantenedora (registry), que puede optar por vender subdominios para recuperar el costo de la infraestructura y de la solicitud.

Como el procedimiento para solicitar un gTLD es caro y bastante burocrático, los ciberdelincuentes necesitan elegir uno de los TLD existentes para registrar un dominio que sirva para ampliar el alcance de un fraude o hacerlo más convincente. Esta elección es especialmente importante en sitios de phishing, ya que la dirección de la página probablemente será verificada por las víctimas.

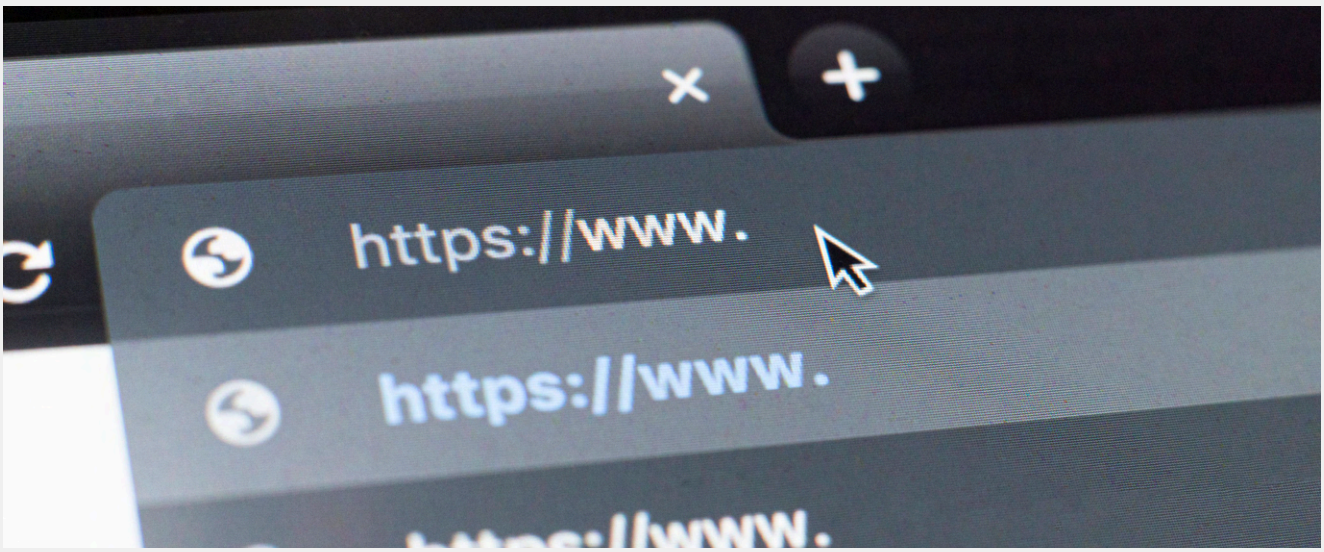
Para tomar esa decisión, el estafador suele considerar algunos elementos:

→ Disponibilidad del dominio:
como las direcciones cortas, palabras simples y marcas comerciales ya no están disponibles en TLD tradicionales, los delincuentes pueden intentar encontrar esos nombres en TLD genéricos más recientes o en alternativas similares.

→ Vínculo con el fraude:
muchos sufijos de gTLD son temáticos. Un criminal puede entender que alguno de ellos hará que la estafa parezca más creíble. Este es uno de los factores que puede explicar, por ejemplo, el aumento en el uso del TLD “.app”.

→ Costo:
algunos TLD son más caros que otros. En casos como “.edu” y “.gov”, que no pueden registrarse libremente, la única opción del ciberdelincuente es comprometer un sitio con esos sufijos para alojar el fraude.

→ Normas del registrador y combate al fraude:
existen reglas que todos los registradores de dominio deben seguir. Sin embargo, puede haber diferencias en el tratamiento de casos específicos que generen una preferencia por parte de los criminales, ya que esto afecta el tiempo que la estafa podrá permanecer en línea.



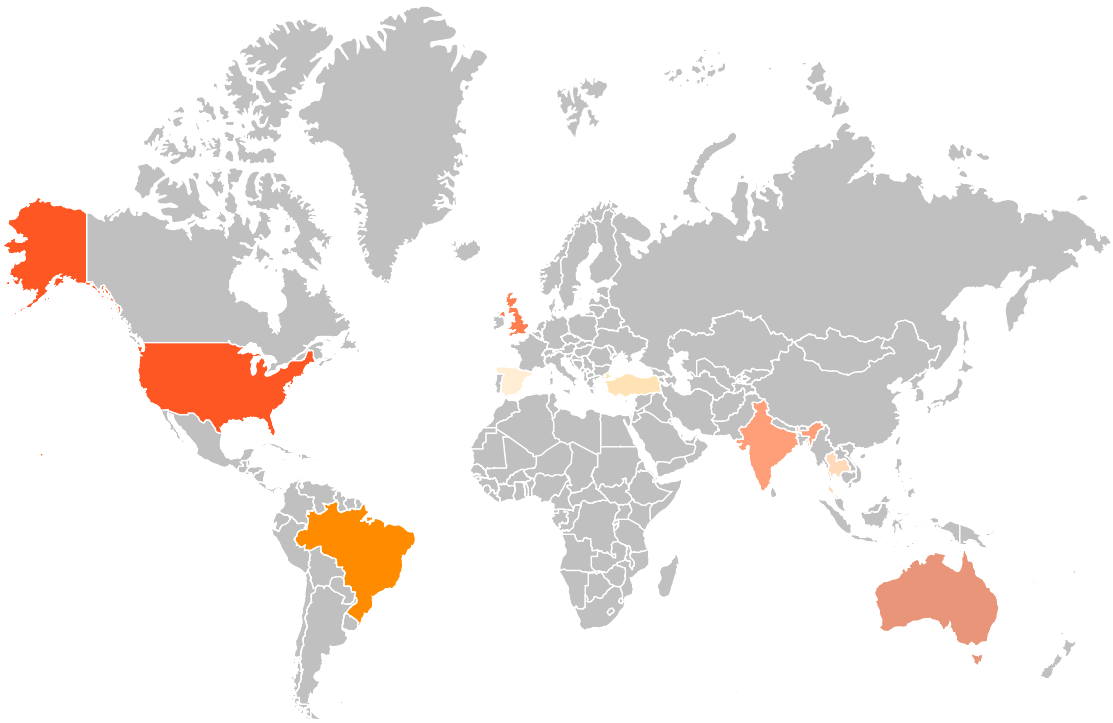
Tarjetas

> La Plataforma Axur detectó la filtración de datos de 395 millones de tarjetas de crédito y débito.

El número de detecciones de tarjetas filtradas en 2025 se mantuvo estable en relación con el período del informe anterior. Lamentablemente, la cantidad de tarjetas expuestas sigue siendo elevada y preocupante.

Gracias al BIN (Bank Identification Number), es posible identificar el origen de cada tarjeta.

Ranking global de países con tarjetas válidas expuestas en 2025



Estados Unidos: **56,16%** | Brasil: **5,36%** | Reino Unido: **2,24%** | Australia: **1,73%**
India: **1,67%** | Tailandia: **1,32%** | Turquía: **0,74%** | España: **0,71%** | Israel: **0,68%** | Otros: **6,49%**

En 2025, el liderazgo global en tarjetas filtradas sigue siendo de Estados Unidos, seguido de Brasil y UK.

El robo de tarjetas representa un riesgo significativo para las instituciones financieras y para el comercio electrónico. Después de que una tarjeta se utiliza de forma indebida, el consumidor normalmente inicia un proceso de chargeback, obligando a la tienda a devolver el importe cobrado.

Como la mercancía no siempre puede recuperarse, la tienda termina asumiendo una pérdida en esa operación.

Con los datos de Axur, los minoristas pueden detectar el uso de tarjetas filtradas y bloquear la compra o realizar las validaciones necesarias para garantizar su legitimidad.

La verificación también es especialmente importante para las instituciones de pago. Las exposiciones de tarjetas impactan directamente a las instituciones financieras y a los procesadores, que necesitan validar transacciones con rapidez y precisión para reducir pérdidas y mantener la confianza de las banderas (marcas de tarjeta).

Caso de uso real

150%
menos tiempo en la validación de tarjetas

En 2025, la fintech **Zoop**, que provee infraestructura tecnológica para el sector financiero, integró la base de tarjetas expuestas de Axur a su proceso de validación.

La verificación se realiza en milisegundos y bloquea de forma preventiva cerca del 30 % de los intentos de transacción con tarjetas comprometidas, reduciendo el tiempo de respuesta operativa en un 150 % y fortaleciendo la seguridad de las operaciones de pago.

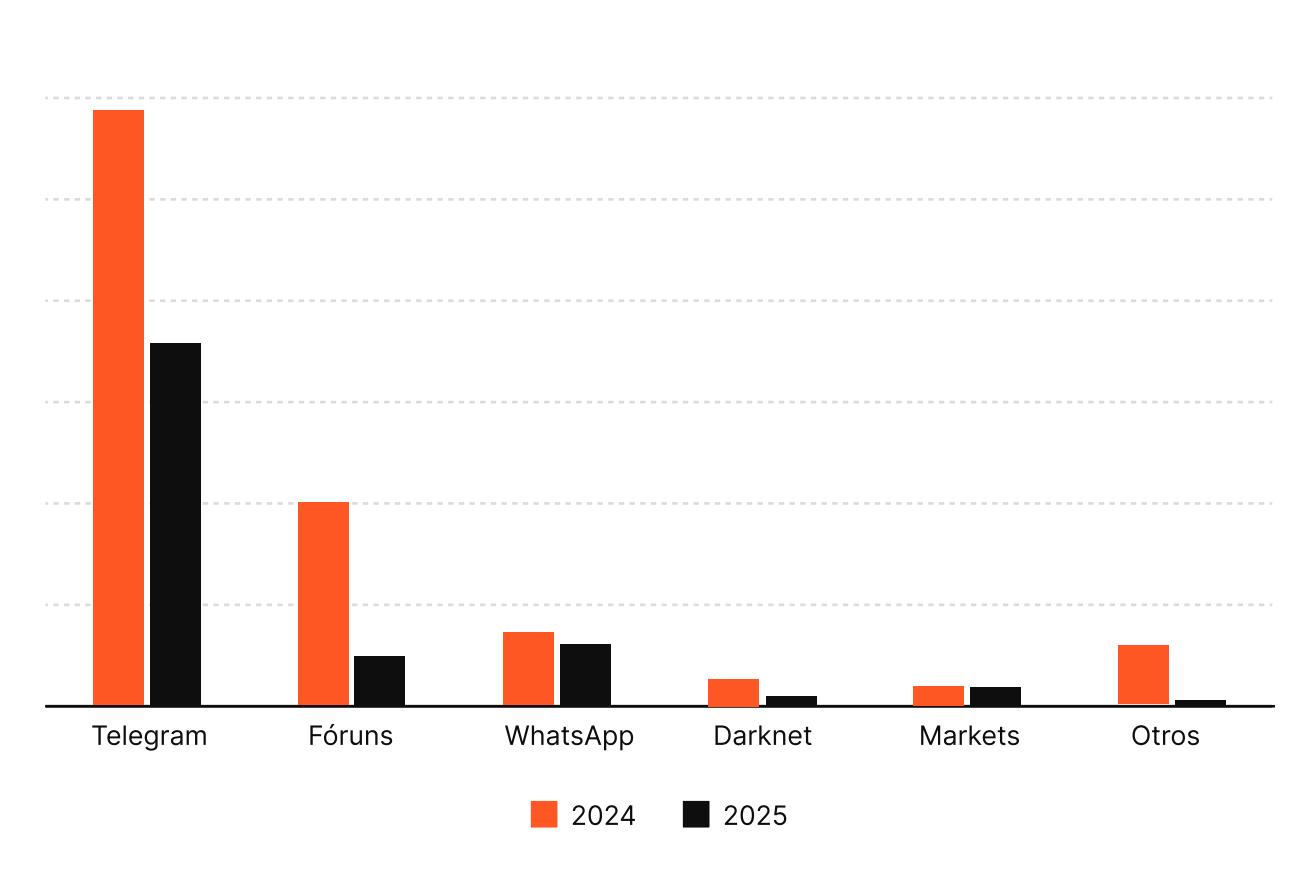
LEA EL CASO

Deep & Dark Web

> En 2025, identificamos 496.403 comunicaciones sospechosas en la Deep & Dark Web que fueron convertidas en incidentes para investigación y generación de inteligencia.

El ecosistema del cibercrimen cuenta con una serie de canales que normalmente quedan fuera de la web visible para la mayoría de las personas, ya que no aparecen en búsquedas simples en los motores de búsqueda y, muchas veces, el acceso a esos canales, grupos o foros es restringido.

Sin embargo, estos espacios de Deep & Dark Web utilizados por los delincuentes pueden ser monitoreados para generar inteligencia sobre las amenazas cibernéticas que se discuten en esos entornos.



Fuentes de incidentes en la Deep & Dark Web en 2025.

Sectores más afectados en la Deep & Dark Web

El sector financiero asumió el liderazgo, pasando de 26,1 % a 48,6 % de los casos, mientras que el retail cayó de 45 % a 18,1 %. Esta inversión refleja el crecimiento de las fraudes dirigidas al ecosistema bancario y de medios de pago, en especial las campañas que involucran ataques al Pix y a los prestadores de servicios de tecnología financiera (PSTI).

El aumento también sugiere una mayor sofisticación en las estrategias de los grupos criminales, que están explotando con más intensidad las vulnerabilidades estructurales, como integraciones de sistemas y credenciales de acceso en instituciones financieras.

El avance del sector de tecnología, de 16,8 % a 22,5 %, también refuerza este movimiento: proveedores de infraestructura, fintechs y plataformas SaaS pasaron a ocupar un papel central en la cadena de riesgo. Telecomunicaciones, por su parte, se mantuvo relativamente estable, con una ligera reducción, lo que puede indicar mayor madurez en los controles y una respuesta más ágil a los incidentes.

En conjunto, los datos confirman una tendencia de migración de las campañas de fraude hacia objetivos de mayor impacto sistémico, donde la explotación de credenciales, APIs e integraciones puede generar efectos en cascada sobre múltiples servicios financieros.

	2024	2025	
Varejo	45%	18,1%	↓ -59%
Financiero	26,1%	48,6%	↑ +86%
Tecnología	16,8%	22,5%	↑ +33%
Telecomunicaciones	4,8%	4,7%	↓ -2%

Axur tiene visibilidad sobre varios de esos canales y realiza un monitoreo que transforma las señales recopiladas en incidentes que pueden ser investigados. En algunas situaciones, esas señales incluso permiten bloquear una acción antes de que efectivamente ocurra.

Caso de uso real

Detección de insiders a partir de indicios en la dark web

En 2025, el Grupo Casas Bahia utilizó el monitoreo de deep & dark web de Axur para investigar indicios de filtración de información corporativa identificados en foros restringidos.

A partir de estas señales, el Axur Research Team llevó a cabo un análisis en profundidad que reveló la actuación de insiders involucrados en la extracción y comercialización de datos internos.

La investigación permitió mapear el origen de la filtración, contener al grupo responsable e implementar controles preventivos para evitar reincidencias y mitigar cualquier impacto reputacional.

LEA EL CASO

Perfiles falsos, aplicaciones ilegítimas y uso fraudulento de marca

Ninguna estafa se presenta a las víctimas como una estafa. En lugar de eso, recurre a marcas y personas conocidas, preferentemente en contextos plausibles, para que las víctimas crean en la narrativa del golpe.

El monitoreo de Axur rastrea la web para detectar situaciones en las que una marca se utiliza de forma indebida para promover contenidos y ofertas ilegítimas, aplicaciones maliciosas, perfiles fraudulentos y uso no autorizado de la marca en anuncios patrocinados de búsqueda.

En 2025, los casos de uso indebido de marcas registraron un aumento, con indicios de que prácticas relacionadas con typosquatting, cybersquatting o registro de dominios similares (+1000 %), así como el uso de marcas en anuncios pagados, contribuyeron a este movimiento.

El uso fraudulento de la marca sigue siendo el tipo de incidente más común, seguido por los perfiles falsos en redes sociales y las aplicaciones falsas.

Los perfiles falsos en redes sociales pueden utilizarse para engañar a los consumidores con ofertas o servicios que no existen.

El consumidor puede creer que está hablando con un representante real de la empresa y terminar adquiriendo productos o servicios que nunca serán entregados, creando una situación indeseable tanto para la empresa — que pierde un cliente— como para el propio consumidor, que pierde su dinero.

El uso de la marca en búsqueda pagada también aumentó, de 1.282 a 5.499 registros, lo que refuerza la tendencia observada por los investigadores de Axur de que los estafadores han buscado cada vez más utilizar la publicidad en línea para dar apariencia de legitimidad a las fraudes.

Las aplicaciones falsas para dispositivos móviles representan una amenaza grave, especialmente para empresas del sector financiero, ya que estos aplicativos pueden utilizar la marca de bancos y entidades financieras para solicitar los datos y credenciales de las víctimas.

En 2025, las aplicaciones móviles falsas parecen presentar una caída significativa. Sin embargo, como mostramos en el análisis de TLD, este movimiento puede estar relacionado con una migración táctica de los agentes de amenaza, que pasaron a explotar con más intensidad URLs alojadas en dominios .app.

	2024	2025	
Uso fraudulento de marca	204.060	262.302	↑ +28,5%
Perfil falso en red social	126.432	132.349	↑ +4,7%
Aplicación móvil falsa	17.621	11.561	↓ -34,4%
Nombre de dominio similar	248	2.954	↑ +1.091,1%
Uso de marca en búsqueda paga	1.282	5.499	↑ +328,9%

Ejecutivos & VIPs

> Detectamos más de 19 mil incidentes que involucraban la imagen y la información de Ejecutivos & VIPs.

Los delincuentes pueden aprovecharse de la imagen y de los datos de ejecutivos y otras personalidades conocidas en diversos contextos.

La información de los ejecutivos puede alimentar fraudes de Business Email Compromise (BEC), en los que el estafador envía correos falsos a otros colaboradores de la empresa o a socios comerciales. Si los destinatarios creen en el mensaje, pueden seguir instrucciones peligrosas e incluso realizar movimientos financieros indebidos.

Estos datos personales también pueden utilizarse para elaborar fraudes dirigidos a los propios ejecutivos, creando un riesgo para la organización y sus sistemas internos.

> Detectamos cerca de 2 mil incidentes que involucraban la exposición de credenciales de ejecutivos o de la alta dirección de las empresas.

A su vez, la imagen de los ejecutivos en perfiles y contenidos falsos en redes sociales puede utilizarse para aumentar la credibilidad de algún producto o servicio. En este punto, hemos observado una regionalización de las fraudes que involucran el supuesto respaldo a oportunidades de inversión, con el uso de la imagen de ejecutivos conocidos, como Elon Musk.

El perfeccionamiento de las herramientas de inteligencia artificial ha facilitado la creación de deepfakes convincentes, ya sea en imágenes estáticas o en videos. Con ello, muchas personas pueden tener dificultades para identificar que el contenido es falso. En ciertos incidentes, el contenido engañoso se encuentra solo en el pie de foto o en el texto que acompaña la imagen, distorsionando su contexto para inducir a la víctima al error.

Amenazas a ejecutivos	Cantidad
Perfil falso en red social	8.759
Exposición de información personal	8.572
Exposición de credencial	2.460
Exposición de tarjetas	27
Total	19.818

Takedown agéntico: una nueva etapa en la automatización de respuesta

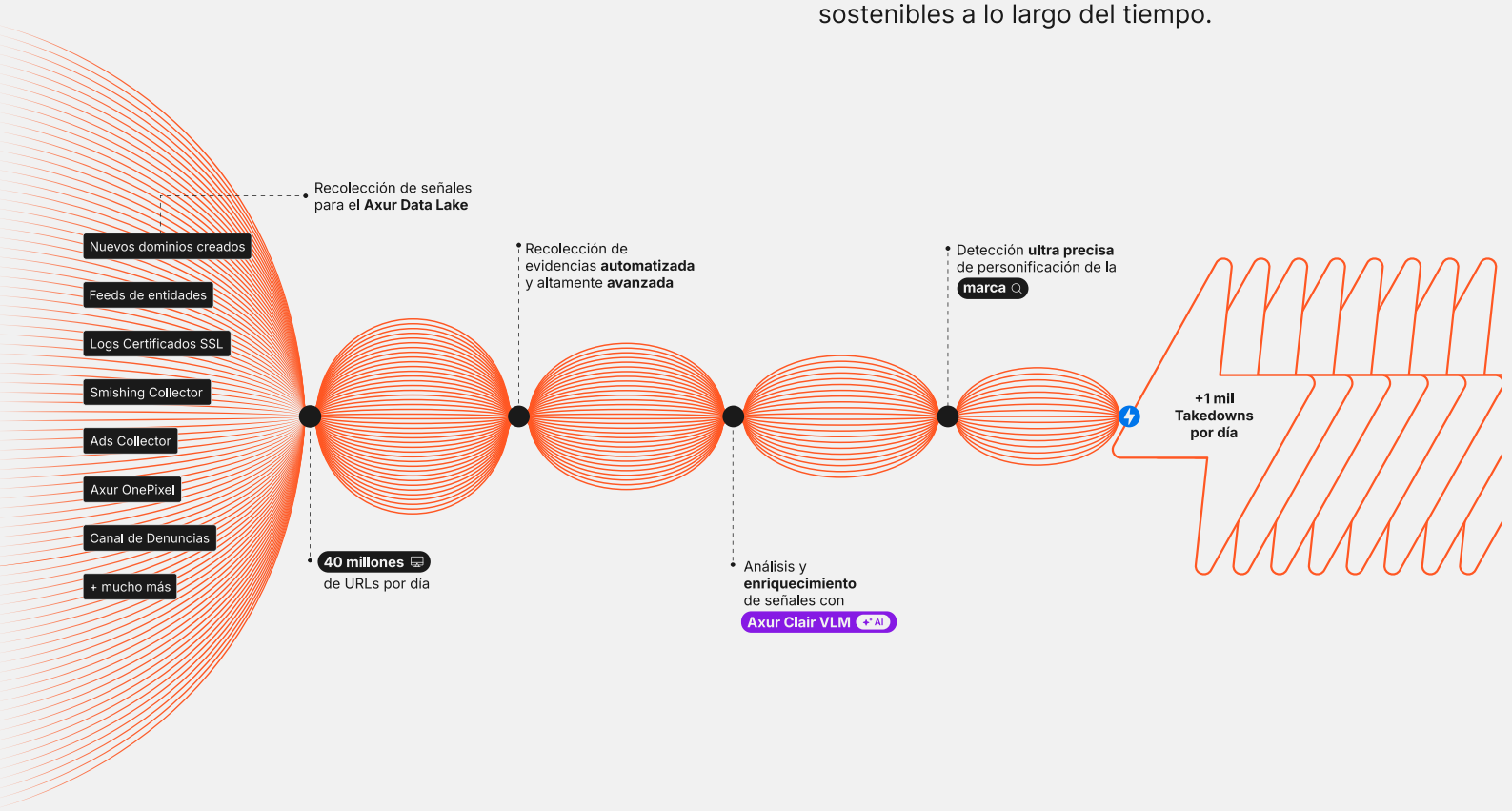
> Hasta octubre de 2025, ya se habían eliminado 343 mil casos de contenido fraudulento gracias a las notificaciones automatizadas de Axur.

El volumen, sostenido por flujos basados en IA y en la validación de evidencias, consolidó la madurez de un proceso que hoy evoluciona hacia un nuevo paradigma: el takedown agéntico.

A diferencia de la automatización tradicional, que ejecuta tareas preprogramadas con base en reglas fijas, el takedown agéntico introduce capacidad de decisión autónoma. El modelo Clair, Cyber Lens for Anomaly and Impersonation Recognition, basado en una arquitectura Vision Language Model (VLM), interpreta tanto el contenido textual como los elementos visuales de cada página, identificando patrones de fraude, indicios de suplantación de identidad y señales de phishing incluso cuando la marca no se menciona de forma explícita.

A partir de este análisis contextual, el sistema es capaz de definir la acción adecuada, notificar al proveedor responsable y acompañar las respuestas, operando de manera continua y con mínima intervención humana. Se trata de un modelo agéntico, en el cual la IA no solo detecta y reporta, sino que también decide y ejecuta.

El diferencial está en la integración entre el análisis multimodal y la toma de decisiones automatizada, lo que permite que Clair conduzca el ciclo completo de respuesta, desde la identificación de la amenaza hasta la ejecución del takedown, con trazabilidad y consistencia. Es una evolución que acerca la seguridad digital a un modelo verdaderamente orientado a la mitigación de riesgo, haciendo que los procesos sean más rápidos, precisos y sostenibles a lo largo del tiempo.

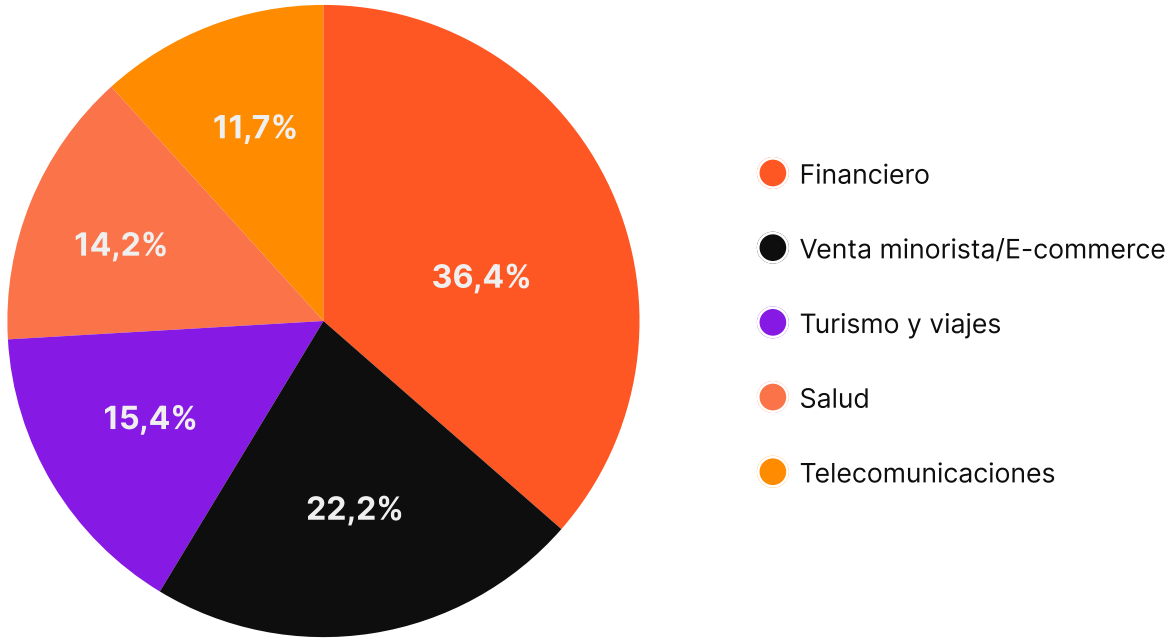


Takedowns por sector

La distribución de los takedowns por sector muestra que el segmento financiero concentra el 36,4 % de las remociones, manteniéndose como el principal objetivo, en línea con el aumento de fraudes observados en este mercado durante el período. A continuación aparecen retail y e-commerce (22,2 %), turismo y viajes (15,4 %), salud (14,2 %) y telecomunicaciones (11,7 %).

La predominancia del sector financiero refleja tanto la alta atractividad económica de las fraudes bancarias como la mayor capacidad de detección y respuesta de las instituciones, lo que se traduce en un mayor número de acciones de takedown ejecutadas en el período.

Distribución de los takedowns por sector entre octubre de 2024 y octubre de 2025



Plataformas más notificadas

En 2025, removimos más de 70 mil perfiles falsos mediante notificaciones enviadas a Meta, responsable de las redes Facebook, Instagram, WhatsApp y Threads.

Tiempo hasta la primera notificación

El tiempo hasta la primera notificación es uno de los indicadores más críticos en el ciclo de respuesta a incidentes, pues determina la rapidez con que una amenaza identificada avanza a la etapa de mitigación.

Los datos de la plataforma Axur muestran que, en promedio, la primera notificación se emite entre tres y cinco minutos después de la solicitud de takedown. El tiempo más corto se observó en los casos de nombre de dominio similar (3,05 minutos) y distribución no autorizada (3,02 minutos).

Reducir el intervalo entre la detección y la primera notificación significa disminuir la ventana de exposición, es decir, el período en que la amenaza permanece activa y potencialmente accesible a las víctimas.

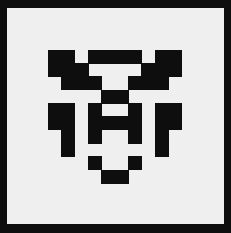
A escala, esa diferencia de pocos minutos puede representar miles de accesos evitados a páginas falsas o perfiles fraudulentos, lo que refuerza la importancia del monitoreo automatizado y de la priorización inteligente de alertas.

Tipo	1ª notificación
Phishing	5,07 minutos
Perfil falso	3,22 minutos
Nombre de dominio similar	3,05 minutos
Distribución no autorizada	3,02 minutos
Venta no autorizada	3,78 minutos

Cyber Threat Intelligence

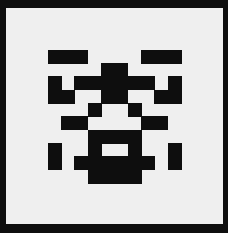
Por medio del módulo de Cyber Threat Intelligence de Axur, es posible acompañar las amenazas más relevantes y comprender el panorama de amenazas de un período específico, como el recorte de 2025.

Actores Maliciosos



Scattered Spider

Scattered Spider es un grupo occidental que ganó mucha atención en 2025 tras diversos ataques exitosos contra empresas en el Reino Unido. El grupo es conocido por utilizar credenciales expuestas y ataques de phishing (principalmente con voz) para obtener esas credenciales o debilitar la autenticación multifactor. Después de formar una supuesta alianza con ShinyHunters y LAPSUS$, el grupo también realizó una campaña exitosa de ataque a ambientes Salesforce, combinando phishing y la explotación de integraciones con terceros.



Qilin

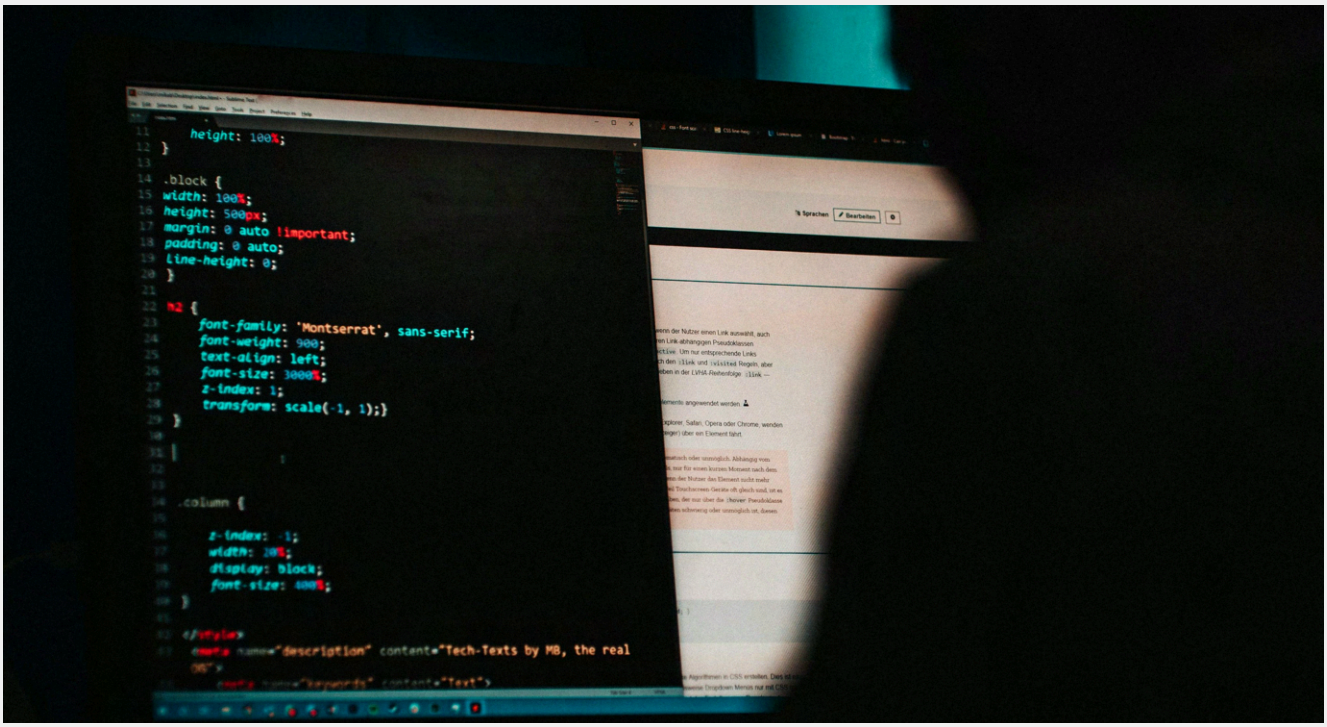
Qilin es una organización que opera en la modalidad de ransomware como servicio (RaaS). Cada afiliado puede elegir su propio método para obtener el acceso inicial a los objetivos, lo que significa que hay una diversidad considerable en las técnicas utilizadas. El grupo aparentemente concentró actividades que antes eran de otros grupos, convirtiéndolo posiblemente en el nombre más activo en la categoría de ransomware al final de 2025.

RansomHub

Este grupo de ransomware es considerado una reencarnación del ransomware Knight. Rápidamente, se convirtió en uno de los grupos más prominentes, especialmente tras acciones policiales contra LockBit3, que resultaron en una caída significativa en su actividad. También fue responsable de un aumento notable de víctimas en 2024. El grupo hizo más de 210 nuevas víctimas, de acuerdo con el FBI, entre ellas empresas como la fabricante de automóviles Kawasaki y el proveedor de comunicaciones estadounidense Frontier Communications, además de filtrar datos de Change HealthCare tras el ataque de BlackCat/ALPHV. El grupo redujo sus actividades en abril.

Salt Typhoon

Muchos especialistas consideran que Salt Typhoon está asociado al gobierno chino. Se destacó en 2025 debido a una serie de ataques que comenzaron aún en 2024, cuando la prensa notició que varias empresas de telecomunicación en Estados Unidos habrían sido invadidas por Salt Typhoon. Este grupo es notorio por atacar objetivos de infraestructura crítica (como telecomunicaciones y energía) y órganos gubernamentales, generalmente con la finalidad de obtener información sobre terceros.



CVEs en destaque

Las principales vulnerabilidades de 2025 prácticamente cuentan una historia: son fallas que comienzan en dispositivos de borde de red y migran hacia los endpoints, donde el invasor entonces obtiene el acceso administrativo para consolidar su presencia en la red corporativa.

CVE-2024-21762

EPSS 0.9291 | Actively exploited | NVD

9.8

Este CVE se refiere a una de las diversas vulnerabilidades explotadas en dispositivos de borde a lo largo de 2025. Esta falla estaba presente en algunas versiones del FortiOS y permite la ejecución de comandos a partir de solicitudes específicas.

CVE-2024-55591

EPSS 0.94152 | Actively exploited | NVD

9.8

Este CVE se refiere a una vulnerabilidad más en FortiOS. Cuando se realiza con éxito, el ataque burla el proceso de autenticación y concede permisos administrativos al invasor.

CVE-2025-53770

EPSS 0.87044 | Actively exploited | NVD

9.8

Información técnica respecto de una vulnerabilidad en SharePoint se filtró para algunos atacantes que explotaron la brecha en la modalidad de día cero, es decir, antes de que la corrección fuera distribuida por Microsoft. Diversas empresas fueron atacadas por grupos de hackers asociados a China.

CVE-2025-29824

EPSS 0.00696 | Actively exploited | NVD

7.8

Este CVE trata de una vulnerabilidad en Windows con impacto de elevación de privilegio. Puede ser utilizada por invasores para facilitar el movimiento lateral dentro de una red corporativa tras la invasión y para instalar software malicioso más difícil de detectar y remover.

CVE-2023-46805

EPSS 0.94377 | Actively exploited | NVD

8.2

Otra vulnerabilidad que burla el proceso de autenticación en dispositivos de borde. El sistema afectado es Ivanti Connect Secure (ICS), una solución para acceso remoto (VPN). Esta vulnerabilidad puede conceder un acceso inicial a la red corporativa.

CVE-2024-21887

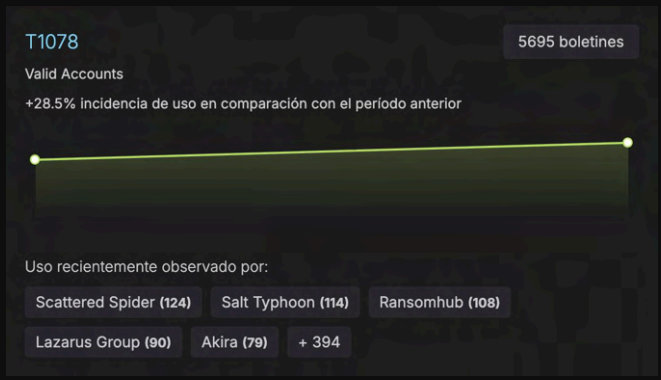
EPSS 0.9442 | Actively exploited | NVD

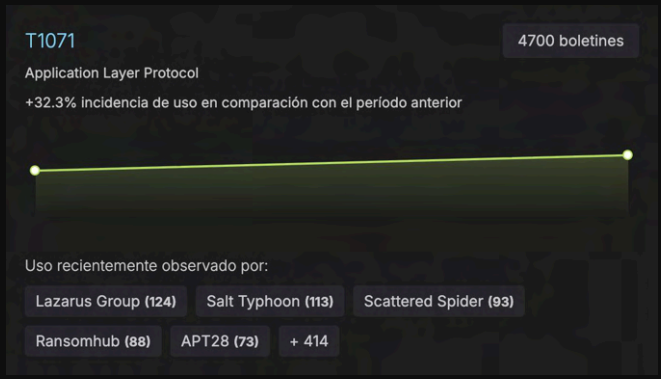
9.1

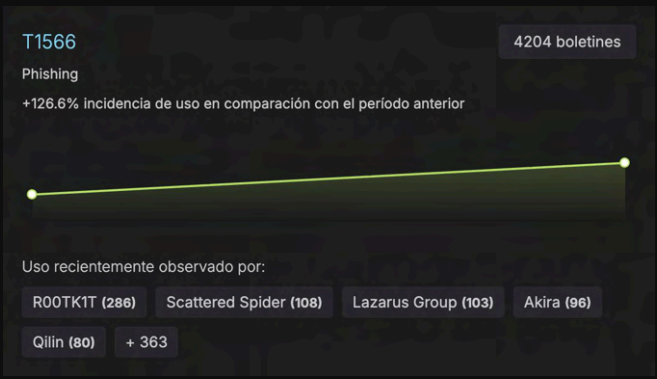
Una vulnerabilidad más en Ivanti Connect Secure. En este caso, la falla está en el procesamiento de solicitudes específicas, permitiendo que el invasor ejecute códigos arbitrarios en el sistema.

TTPs en destaque

Las técnicas más recurrentes en 2025 reflejan la creciente sofisticación de los ataques: explotan vulnerabilidades en aplicaciones expuestas o de cliente para obtener ejecución de código y acceso inicial (T1190, T1203), avanzan mediante el uso de credenciales válidas (T1078) para mantener la persistencia y escalar privilegios, y se consolidan con comunicaciones disfrazadas (T1071) y campañas de phishing dirigidas (T1566) que garantizan el control y el movimiento lateral dentro de la red corporativa.







Malware en destaque

Los grupos de ransomware más activos de 2025 refuerzan la consolidación del modelo “as a service”. Akira y LockBit mantienen un alto volumen de ataques con doble extorsión, explotando credenciales válidas para el acceso inicial, mientras que Ransomhub surge como sucesor de operaciones anteriores, ampliando su enfoque hacia la filtración de datos de alto valor.

Qilin se destaca por la sofisticación y personalización de su código, lo que dificulta el análisis defensivo, mientras que Lumma Stealer, que opera bajo el modelo MaaS, se centra en el robo y la reventa de credenciales, alimentando el ecosistema de acceso inicial.

Insight de la plataforma Axur

Cyber Threat Intelligence

La complejidad actual de la ciberseguridad exige que los equipos filtren, correlacionen y prioricen información en medio de volúmenes masivos de datos. El CTI de Axur fue desarrollado justamente para resolver ese desafío, combinando algoritmos de IA y un modelo de lenguaje entrenado en amenazas cibernéticas para transformar datos fragmentados en alertas curadas y contextuales.

Diariamente, el sistema analiza cientos de fuentes, como reportes, feeds, grupos especializados y noticias, e identifica lo que realmente es relevante para cada ambiente, mapeando amenazas y vulnerabilidades conforme a la superficie de ataque de cada cliente.

Escenario geopolítico

Visión general del escenario geopolítico

Acuerdos y asociaciones internacionales fueron fragilizados en 2025 por una sumatoria de dificultades.

De un lado, tenemos las barreras regulatorias: tarifas comerciales, restricciones en exportaciones, sanciones financieras, realineamiento de prioridades y nuevas legislaciones que entraron en vigor.

Del otro, tenemos los desafíos concretos que motivaron esas medidas: los ataques cibernéticos contra la infraestructura crítica, recelos respecto al dominio de China como proveedora de piezas, equipos y productos en sectores estratégicos, la disputa sobre el liderazgo tecnológico en inteligencia artificial, la guerra entre Rusia y Ucrania y la escalada de conflictos e incertidumbres en el Medio Oriente.

Estos factores contribuyeron para la visión de que no basta con proteger empresas o sectores específicos, una vez que ellos dependen de toda una cadena de proveedores. Diversidad y redundancia no serían soluciones viables, una vez que todos se ven interconectados por un número limitado de desarrolladores de software y plataformas de TI.

Esta perspectiva despertó el debate sobre soberanía digital, dando forma a una nueva ola de ideas e inversiones en infraestructura de TI.

unque las consecuencias sean más tangibles en el sector gubernamental y terceros que trabajan con infraestructura crítica, es posible que los efectos se esparzan hacia otros sectores de la economía.

La política y las tensiones globales siempre impactaron los negocios, sobre todo en las empresas cuya actuación no se limita a las fronteras de un único país. Con internet y los servicios digitales, tenemos un escenario en que casi todos dependen de software, de equipos y de servicios de tecnología viabilizados por una compleja red de proveedores globales.

En esas circunstancias, la relación entre las tensiones geopolíticas y los desafíos en el área de ciberseguridad tiende a ampliarse.

> Una evidencia de esto apareció en una investigación del Foro Económico Mundial publicada al inicio de 2025 en que el 60% de las empresas dijeron creer que las tensiones geopolíticas impactaron su estrategia de ciberseguridad.

La relevancia de esas tensiones varía para cada empresa. Por eso, conviene enumerar los temas ligados a la ciberseguridad que se destacaron a lo largo del año y analizar qué consecuencias trajeron para los diferentes sectores de la economía.

Ataques a infraestructura crítica

La preocupación con la resiliencia cibernética en elementos críticos de infraestructura (energía, telecomunicaciones, agua y logística) no es nueva, pero los métodos utilizados para evaluar la madurez del sector y las propuestas de perfeccionamiento han avanzado de forma significativa.

En 2024, el gobierno de Biden dio inicio a una revisión de las grúas usadas en puertos estadounidenses con el objetivo de sustituir los modelos fabricados en China. Reguladores posteriormente citaron la presencia de componentes electrónicos no documentados con conectividad externa como una de las justificaciones para esa medida.

En paralelo, agentes de seguridad del gobierno indicaron que invasores chinos estaban infiltrados en los sistemas de TI de varias empresas en sectores críticos, sin dar ejemplos específicos.

En septiembre de 2024, la prensa, inicialmente a través del Wall Street Journal, divulgó que hackers chinos vinculados a Salt Typhoon obtuvieron acceso a varias operadoras de telecomunicación. A pesar de la gravedad del incidente, lo que marcó ese ataque fue el interés de los invasores: los clientes de las operadoras.

En 2025, presenciamos los desdoblamientos de esa campaña. Otros países comenzaron a publicar notas y boletines alertando sobre la actividad de Salt Typhoon en las operadoras de telecomunicación en su territorio, muchas veces explotando fallas en los llamados dispositivos de borde (edge devices) de marcas como Cisco, Ivanti y Palo Alto Networks.

> En agosto, el FBI alertó que más de 80 países fueron atacados por Salt Typhoon.

En el mismo mes, el órgano alertó sobre la actividad de otro grupo de hackers, esta vez asociado a Rusia, que también estaría enfocado en operadores de infraestructura crítica.

Tanto China como Rusia niegan involucramiento con los ataques.
Estén los países directamente involucrados o no, las invasiones generan tensiones y recelos con consecuencias claras para las empresas involucradas. Un ejemplo se dio tras un reportaje del sitio ProPublica denunciar el involucramiento de ingenieros chinos en contratos del Departamento de Defensa, obligando a Microsoft a prometer que no más utilizaría esos equipos.

La idea de "nacionalizar" servicios en pro de la seguridad nacional acabó llegando también en propuestas al legislativo norteamericano. Congresistas se enfocaron sobre reglas para la compra de equipos e incluso para call centers, todas con potencial de imponer barreras a la tercerización.

Al mismo tiempo, órganos de gobierno en varios países vienen estructurando evaluaciones de ciberseguridad. En diciembre de 2024, la Agencia de Ciberseguridad de la Unión Europea (ENISA) lanzó su primer reporte sobre el "estado de la ciberseguridad" en el bloque.

El foco de esas medidas tiende a ser la infraestructura crítica y algunos órganos gubernamentales. Sin embargo, ellas ya están siendo extendidas a las empresas que prestan servicios a los sectores protegidos.

Comentario del especialista

Sérgio Costa

Investigador del
Axur Research Team.

Al analizar los grupos hacktivistas, en el contexto del conflicto involucrando a Israel, Hamas e Irán, los grupos están cada vez más unidos por una causa común y posiblemente realizando acciones coordinadas, con una tendencia creciente a visar infraestructuras críticas.

A pesar de eso, ataques DDoS clásicos aún son prevalentes. Algunos grupos están citando el desarrollo de ransomwares, que pueden servir como fuente de soporte financiero para sus acciones. La línea entre hacktivismo y actividades patrocinadas por estados-nación se está volviendo cada vez más tenue, levantando dudas sobre las verdaderas motivaciones de ciertos grupos.

Conflictos regionales

La guerra entre Rusia y Ucrania crea una situación singular para los ataques cibernéticos. Acciones exitosas son hasta celebradas por los canales que distribuyen noticias del conflicto, eliminando buena parte de la duda sobre su origen.

Ataques notorios fueron realizados contra operadoras de telecomunicación de Ucrania (Kyivstar) y de Rusia (Nodex, Lovit, Beeline, Rostelecom). Muchos de los incidentes involucran DDoS y son realizados por hackers dichos "voluntarios".

Otro escenario específico es el del Medio Oriente, con tensiones involucrando principalmente a Israel, Hamas e Irán.

El Ministro de Inteligencia de Irán llegó a anunciar que agentes del país se habían infiltrado en el programa nuclear israelí. De manera general, admisiones de esa naturaleza son raras, y la duda no está más en el origen del ataque (como ocurre en las operaciones de espionaje que no son reconocidas), sino en la veracidad de los hechos narrados por el atacante.

Hubo también una escalada en las tensiones entre India y Pakistán, con cuatro días de conflicto armado en mayo. En ese período, Pakistán anunció una campaña de ataques cibernéticos contra India para derribar servicios y destruir archivos. Las hostilidades terminaron con un acuerdo de cese al fuego.

Desafíos de supply chain

Ataques ligados a tensiones geopolíticas no siempre son los únicos que utilizan una determinada estrategia, pero es común que ellos adopten esas estrategias conocidas con una finalidad diferente o con más sofisticación.

Esto no es diferente para los ataques a cadenas de proveedores (supply chain). Mientras las campañas de ataques a terceros realizados por criminales buscan datos corporativos y procuran por una chance de extorsionar a las víctimas, los ataques a operadoras de telecomunicación tienen la finalidad de colectar información sobre objetivos de interés geopolítico.

Además de los ataques a operadoras de telecomunicación en decenas de países, hay relatos de que proveedores de internet en Moscú también habrían sido atacados para facilitar el espionaje de las embajadas instaladas en la capital rusa.

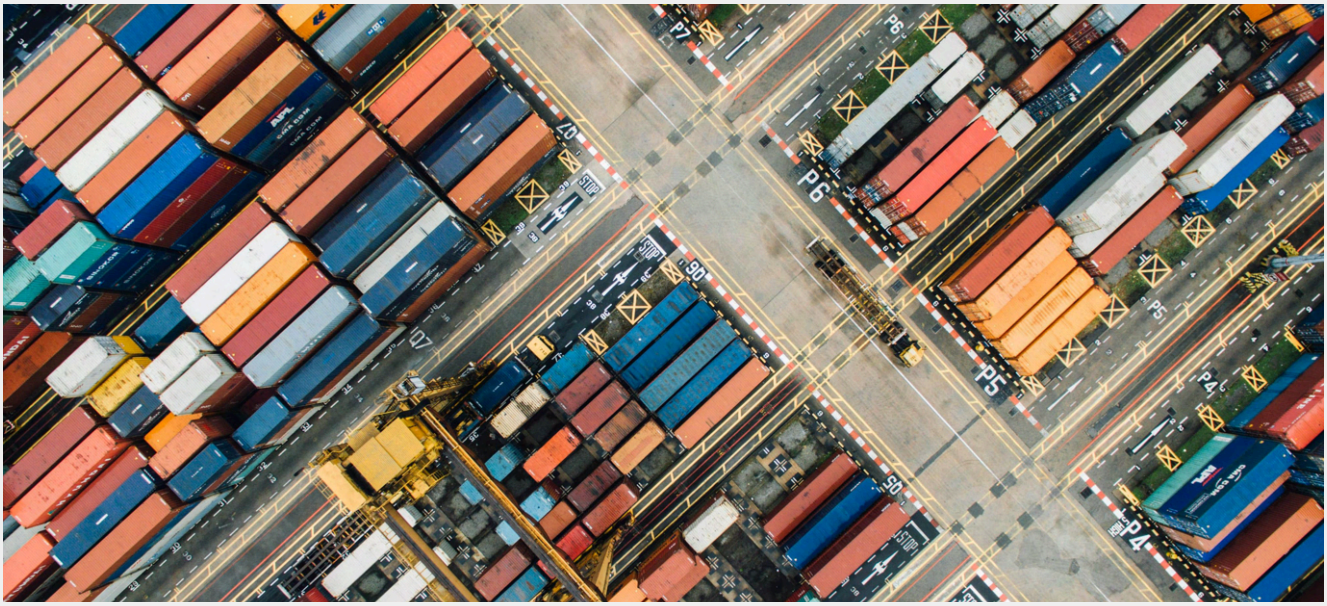
Al contrario de los criminales, que buscan los objetivos más rentables y vulnerables, ataques para fines de espionaje patrocinados por gobiernos pueden estudiar con más calma un objetivo y encontrar brechas menos expuestas.

Operadores de infraestructura crítica son un objetivo valioso y actúan como un "proveedor" para una gran parcela de las empresas e individuos, lo que ayuda a explicar esas acciones. Sin embargo, vale recordar que el incidente de SolarWinds también fue atribuido a un grupo patrocinado por un gobierno (Rusia).

> Por eso, es justo concluir que cualquier empresa particular que preste servicio para objetivos de interés geopolítico puede convertirse en objetivo de esos ataques.

La idea es evitar un escenario en que las autoridades de esos países decidan distribuir software comprometido o hardware saboteado. La operación de los pagers explosivos del Medio Oriente ya había demostrado ese riesgo en 2024.

Más recientemente, hemos visto casos como los impedimentos a ingenieros chinos en contratos gubernamentales de Estados Unidos y la decisión de Microsoft de reducir el acceso chino a información del Microsoft Active Protections Program (MAPP), una plataforma que trae información previa sobre vulnerabilidades que pronto serán corregidas.



La decisión de Microsoft de limitar el acceso chino ocurrió tras una vulnerabilidad de SharePoint compartida a través del MAPP ser explotada antes de la distribución del patch. Con la falla sin corrección, hackers (que serían chinos, según los análisis de los incidentes) consiguieron acceso fácil a cientos de empresas.

China es el principal objetivo de esas medidas, pero el país asiático también trabaja para no depender más de software y hardware estadounidense. El gobierno chino inclusive recomendó que empresas de tecnología locales no adquirieran los chips H20 de Nvidia, que fueron desarrollados para contornar las restricciones de exportaciones de hardware de IA.

Hay, sin embargo, una serie de medidas más neutras visando aumentar la resiliencia cibernética, como la adopción de Software Bill of Materials (SBOMs) y otras metodologías de gestión de riesgo de terceros.

Al mismo tiempo, acciones en la Justicia vienen intentando derribar la idea de que es posible tercerizar el riesgo, responsabilizando al contratante por no fiscalizar el trabajo realizado en su nombre.

Esas medidas visan la creación de un escenario en que las propias empresas demandan una preocupación mayor de seguridad por parte de sus proveedores, lo que contribuye para la resiliencia cibernética de sectores enteros de la economía.

El robo de US$ 1,5 mil millones

Muchos de los ataques patrocinados por gobiernos son realizados para fines de espionaje. Sin embargo, los hackers de Corea del Norte divergen de ese patrón, actuando principalmente para obtener recursos y financiar el régimen.

En marzo, la casa de cambio de criptomonedas ByBit sufrió un ataque cibernético de Lazarus, un notorio grupo norcoreano. La acción, que fue considerada el mayor robo de la historia, resultó en el desvío de US$ 1,5 mil millones de fondos de la casa de cambio.

El ataque fue posible porque los invasores comprometieron un proveedor de ByBit, Safe {Wallet}. El primer objetivo del ataque fue un ingeniero de Safe que, según algunas evidencias, puede haber sido víctima de phishing.

Con acceso al sistema de ese ingeniero, los invasores entonces obtuvieron una clave del almacenamiento en nube de Safe para adulterar un código JavaScript en su plataforma. El código comprometió una cartera de ByBit.

Este incidente ilustra las complejidades técnicas de los ataques de supply chain, la persistencia de los hackers patrocinados por gobiernos y la forma como los riesgos de tercerización muchas veces extrapolan los límites imaginados por las metodologías de gestión de riesgo.

Soberanía digital y resiliencia

El concepto de "soberanía digital" no es exactamente nuevo, pero no fue por mera coincidencia que inversiones en datacenters nacionales y soberanos fueron anunciados en el mismo año en que el gobierno de Estados Unidos decidió adquirir parte de Intel.

Esencialmente, la idea de soberanía digital defiende que un país tenga independencia para cuidar de sus necesidades de TI, tanto en términos de infraestructura como en la gestión y regulación.

Países que tienen alguna capacidad de fabricación de semiconductores de punta están tomando medidas para fortalecer la cadena productiva del sector o atraer nuevas inversiones. En Estados Unidos, eso comenzó aún en 2023 con la ley CHIPS.

Ya en 2025, la fabricante de memorias japonesa Kioxia anunció que desconectaría terceros que no consiguieran una puntuación satisfactoria en una evaluación de seguridad, posiblemente reflejando nuevas demandas de clientes y reguladores.

Mientras tanto, Estados Unidos asumió el control del 10% de la fabricante de procesadores Intel – una rara intervención directa del gobierno norteamericano que ayudó a estabilizar el valor de mercado de la empresa.

Pero, teniendo en vista la complejidad de la fabricación de semiconductores, muchos países no tienen condiciones de replicar la cadena de producción de la infraestructura de TI, aun contando con aliados estratégicos. Siendo así, una alternativa es garantizar la presencia de activos en territorio nacional y la capacidad de gestión y regulación.

Con la aprobación del CLOUD Act en 2018, críticos cuestionaron la independencia de los proveedores norteamericanos, señalando que ellos serían obligados a cumplir órdenes y entregar información en desacuerdo con la legislación local. Con la migración hacia la nube, la influencia norteamericana dejó de limitarse a servicios puntuales como e-mail o chat y colocó toda la infraestructura de TI bajo una jurisdicción externa.

Durante la pandemia del coronavirus, la nube fue el camino natural para que las empresas pudieran continuar funcionando con trabajo remoto y evitaran la adquisición de hardware, que estaba con precio elevado en consecuencia de la suspensión del funcionamiento de las fábricas y la demanda por equipos.

Esa consolidación reforzó las preocupaciones asociadas al CLOUD Act. Sin embargo, el avance de la inteligencia artificial, con sus elevados requisitos computacionales, trajo un elemento aún más urgente al tema.

Un hecho notable en 2025 fue la suspensión temporal de la dirección de correo electrónico de un procurador del Tribunal Penal Internacional en respuesta a una sanción del gobierno de Estados Unidos. Como el e-mail era un servicio de nube de Microsoft, el episodio levantó cuestiones sobre la privacidad y sobre cómo proveedores de nube extranjeros respetarían las leyes europeas.

Los proveedores norteamericanos reaccionaron y se comprometieron con una infraestructura soberana, pero no pudieron negar que estaban sujetos a las decisiones del gobierno y de los tribunales de Estados Unidos. Eso significa que ellos tendrían, sí, que entregar datos a las cortes estadounidenses, aun que los datos estuvieran almacenados en territorio europeo.

Con ese recado, algunas empresas anunciaron nuevas inversiones en infraestructura soberana en Europa, de ojo en el mercado gubernamental y en la demanda por más seguridad jurídica.

Ese movimiento no se restringe a Europa. China tiene iniciativas semejantes para reducir la dependencia en hardware y software norteamericano, mientras Brasil está invirtiendo en una Nube de Gobierno, en infraestructura de computación para inteligencia artificial y en investigaciones en el área de semiconductores.

Consecuencias para la ciberseguridad

Visto de forma aislada, la soberanía digital parece ser una cuestión política y abstracta. Sin embargo, ese tema está ligado a cuestiones de gobernanza, seguridad nacional y resiliencia cibernética.

Del punto de vista de resiliencia, la consolidación de la infraestructura de TI en apenas algunos proveedores trae riesgos significativos, ya que todos los servicios atados a esos proveedores pueden sufrir interrupciones o violaciones simultáneamente. La gestión de riesgo también es dificultada, una vez que los mecanismos para compensar ese riesgo sistémico serán más complejos.

Dependiendo de las prioridades y de los métodos, la mitigación de los riesgos de un apagón cibernético generalizado puede ser más cara que el costeo de una infraestructura distribuida.

El tema de riesgo sistémico está vinculado a otro asunto más próximo del día a día de las empresas: la cadena de proveedores y terceros (supply chain). ra confiable.

Además de computadoras y software, datacenters necesitan de proveedores para servicios de enfriamiento, energía y conectividad – y todo eso debe entrar en la cuenta para una infraestructura confiable.

En ese sentido, incidentes de supply chain pueden acalorar la discusión de soberanía digital en la misma medida en que la regulación de ese tema puede traer impacto para la gestión de riesgos atados a proveedores.

Infelizmente, no hay cómo prever el futuro, especialmente ante la inestabilidad geopolítica actual. Es posible, por ejemplo, que el tema de soberanía digital siga por un rumbo más político, con acuerdos multilaterales y mecanismos de colaboración internacional para proteger la jurisdicción de cada país.

Por otro lado, también es posible que ella se desdoble en acciones con impacto directo en los negocios y en la estrategia de ciberseguridad. Un ejemplo es la creación de incentivos para adopción de software, hardware e infraestructura dedicados al perfeccionamiento de la gobernanza cibernética.

Tendencias

Agentes de IA

La idea de que la inteligencia artificial pudiera llevar a cabo acciones por cuenta propia siempre estuvo presente. Sin embargo, los primeros productos con ese concepto tenían un carácter algo experimental, tanto por la utilidad limitada como por los riesgos de dejar a la IA a cargo de tomar acciones críticas.

Los agentes de IA maduraron a lo largo de 2025 con la disponibilidad y el perfeccionamiento de productos dinámicos orientados a todos los segmentos del mercado. Algunos de los avances más rápidos se observaron en tareas de desarrollo de software, donde IAs empezaron a encontrar bugs y vulnerabilidades junto con los informes correspondientes para comunicarlos a los desarrolladores.

> La popularización del término “vibe coding” es un reflejo de esta tendencia.

Como era de esperarse, innovaciones similares surgieron en las técnicas de ataque. Investigadores han demostrado formas de explotar la interpretación de la IA combinando inyecciones de prompts maliciosos y APIs para producir resultados indeseados.

Los riesgos incluyen vulnerabilidades mapeadas poco después del lanzamiento de navegadores como Perplexity Comet y ChatGPT Atlas, de OpenAI. Uno de los ataques divulgados contra Comet utilizaba esteganografía, texto invisible incrustado en páginas web, que es leído por el motor de OCR del navegador y enviado directamente al sistema de IA sin validación.

Esto permite que los atacantes ejecuten acciones no autorizadas, como robo de datos, acceso a cuentas y compromiso de sistemas corporativos.

El navegador de OpenAI, por su parte, era vulnerable a la inyección persistente de comandos maliciosos en la memoria del asistente, lo que posibilitaba la ejecución arbitraria de código y el escalamiento de privilegios. Ambos casos muestran que los agentes también se convierten en una superficie de ataque crítica para las empresas.

> Debido al potencial de los agentes de IA, muchas compañías pueden empezar a buscar maneras de integrarlos en sus flujos, llevando toda la discusión técnica sobre estos agentes al entorno corporativo y, por lo tanto, crear desafíos para proteger dichos sistemas.

La adopción de agentic AI dentro de las organizaciones no se limita a la experimentación, representa un cambio de paradigma operativo. AI evolucionar de copilotos a sistemas autónomos con capacidad de decisión y ejecución, estos agentes pasan a integrar directamente el ciclo de respuesta: detectar, decidir y actuar.

Esta autonomía exige una arquitectura de gobernanza sólida, basada en restricciones, aprobaciones, aislamiento y trazas de auditoría que aseguren rastreabilidad y reversibilidad de las acciones.

Las empresas que pretendan incorporar agentes autónomos necesitan alinear identidades de máquina, políticas de mínimo privilegio y mecanismos de supervisión humana para evitar ejecuciones indebidas o escaladas no autorizadas. El riesgo no reside solo en las alucinaciones de los modelos, sino en la ejecución de comandos válidos en contextos erróneos, lo que demanda métricas de observabilidad y auditoría en tiempo real.

Además, la proliferación de agentes fuera del control corporativo, impulsada por el shadow IT, amplía la superficie de exposición. Incluso sin integración oficial, esos agentes pueden interactuar con sistemas críticos o datos sensibles, por lo que se vuelve indispensable

> el uso de controles de identidad dinámicos, aislamiento de entornos y monitoreo continuo de las interacciones entre agentes y APIs corporativas.

En 2026, la madurez en seguridad estará definida por la capacidad de equilibrar autonomía y control, permitiendo que la IA actúe con agilidad, pero dentro de límites verificables, auditables y reversibles.

Los equipos de ciberseguridad deberán estar atentos a estos movimientos para brindar el apoyo necesario, con el objetivo de un uso consciente y seguro de estos agentes que fortalezca el negocio.

Uso por actores maliciosos

Si existe el “vibe coding”, también existe el “vibe hacking”. Los modelos de IA pueden detectar vulnerabilidades para hacer el software más robusto, pero los delincuentes pueden valerse de la misma idea para encontrar nuevas vulnerabilidades con el fin de explotarlas.

Del mismo modo, los criminales pueden utilizar IAs para facilitar el desarrollo y la adaptación de código malicioso, o para reestructurar artefactos con el objetivo de evadir la detección por herramientas de seguridad, como EDR, XDR, filtros de spam e IDS.

Agentes de IA y sus identidades también pueden ser explotados por delincuentes que obtuvieron acceso a la red corporativa, creando un canal para la movimentación lateral que no estará necesariamente limitada por la segmentación de red tradicional.

A medida que el uso de la IA crece entre los atacantes y dentro de las empresas, la necesidad de adoptar la IA como aliada en la ciberseguridad se vuelve cada vez más evidente.

> Existen muchas tareas de ciberseguridad que hoy no reciben la debida atención, principalmente por la dificultad de priorizar alertas y auditar eventos.

Esto provoca que muchas alertas sean ignoradas o analizadas solo de manera superficial, incluso en entornos de SOC.

Solo el 9% de las organizaciones monitorea el 100% de su superficie de ataque (IBM), y el 28% de los profesionales de ciberseguridad usa IA para reducir los falsos positivos.

(ISC2 2024 Cybersecurity Workforce Study).

Por esta razón, es probable que muchos comiencen a explorar agentes de IA como medio para mejorar la comprensión de los eventos en su infraestructura, acelerando la detección y la respuesta a incidentes.

La capacidad de la IA para vincular alertas internas con bases de datos enriquecidas con inteligencia de amenazas tiene el potencial de ampliar significativamente la calidad de las alertas que llegan a los equipos de ciberseguridad.

Adoptar agentes de IA en la ciberseguridad también es una oportunidad para entender los requisitos de esta tecnología y las soluciones para integrarla de forma segura en la infraestructura de TI. Ese aprendizaje puede compartirse con las demás áreas del negocio y guiar la adopción de IA en los más variados procesos.

Insight de la plataforma:
Axur Command

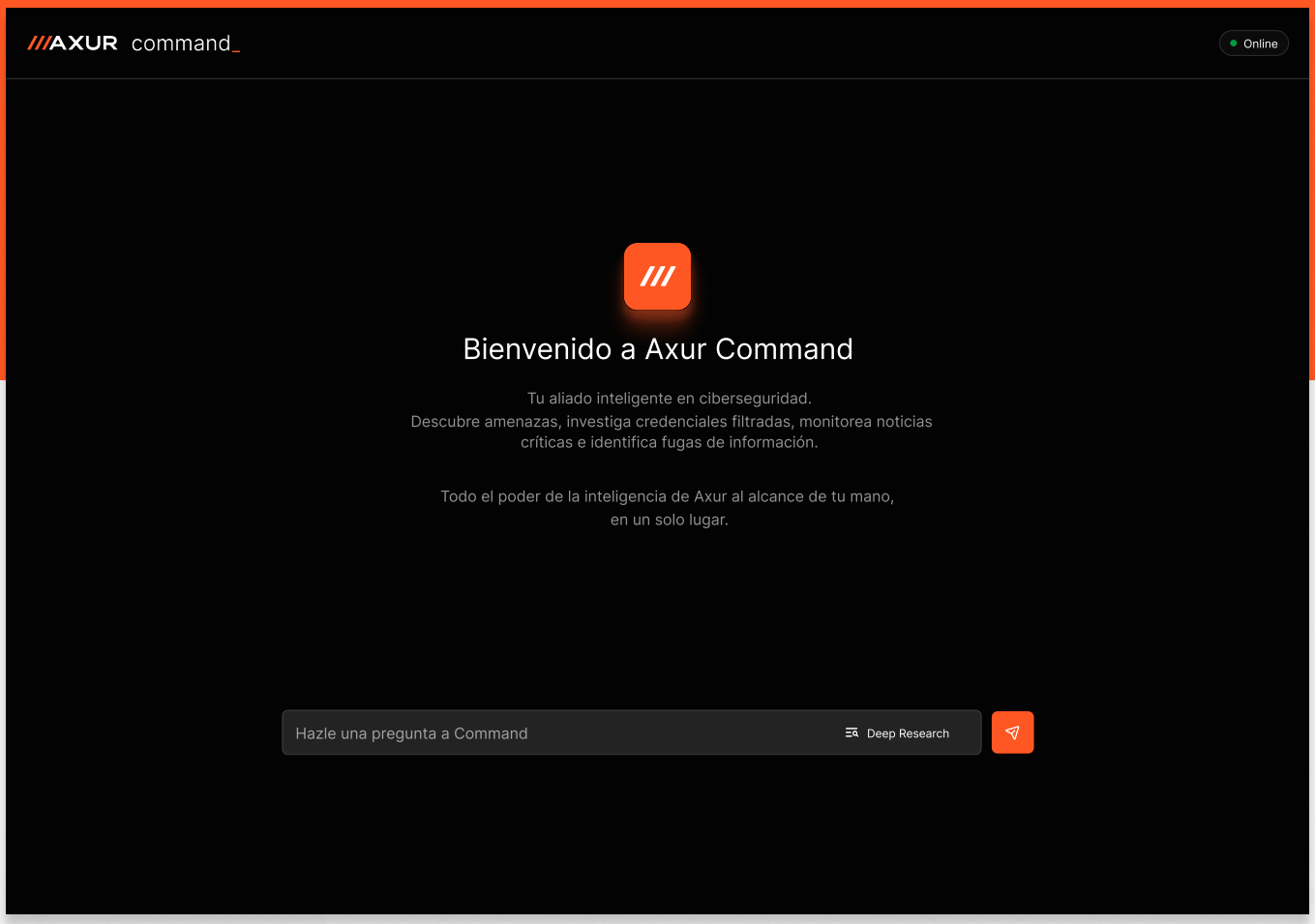
Axur Command introduce un nuevo paradigma de automatización en ciberseguridad, un centro de comando que orquesta agentes de IA especializados para correlacionar alertas, eliminar falsos positivos y ejecutar respuestas coordinadas en tiempo real.

La solución conecta distintas fuentes, como SIEM, EDR, CTI y EASM, en un flujo único de detección y respuesta, reduciendo el tiempo de análisis y la sobrecarga de los equipos.

Entre sus principales capacidades se encuentran:

Automatización de tareas de Tier-1, con agentes que triagean alertas y priorizan incidentes.

Correlación en tiempo real entre múltiples orígenes de datos, revelando el contexto completo de las amenazas.



Reglamentación

Cuando algo tiene impactos sociales significativos, es natural que diversas fuerzas de la sociedad civil se movilicen para establecer reglas. Ese encuadre puede materializarse en una ley, en iniciativas voluntarias o en organismos de autorregulación establecidos por los interesados.

Esa dinámica también aplica a la tecnología. La rápida evolución de la inteligencia artificial atravesó la burbuja del mundo tecnológico y atrajo la atención del mundo político. Varias leyes ya fueron aprobadas o están en discusión, y no es fácil prever qué nuevos debates pueden surgir en 2026.

A pesar del protagonismo de la IA, no solo ella está siendo examinada por los reguladores. La presencia creciente de las aseguradoras en el mercado de ciberseguridad viene promoviendo un debate más amplio sobre la responsabilidad por los daños derivados de incidentes de seguridad. Pagar el rescate en ataques de ransomware puede volverse más complicado.

El cambio de reglas dentro del propio sector también es algo esperado para 2026. Un ejemplo es el plan de Google para limitar el sideloading de aplicaciones de Android con un registro obligatorio para todos los desarrolladores. Brasil debería ser uno de los primeros países sometidos a la nueva regla, cuyo objetivo es reducir el volumen de ataques con aplicaciones falsas.

Cualquier cambio abarcador en la forma en que usamos la tecnología tiene el potencial de transformar también las amenazas.

Soberanía digital y de datos

El tema de la soberanía digital ganó bastante relevancia a lo largo de 2025, dado que el clima geopolítico viene dejando a muchos países preocupados por la independencia de su infraestructura tecnológica y la capacidad de mantener el control sobre datos almacenados en nubes de escala global.

> Los objetivos de la soberanía digital pueden impactar la infraestructura de TI y crear desafíos de gobernanza y cumplimiento. Estos cambios tienen un impacto cierto en la ciberseguridad, que deberá estar involucrada en todo el proceso.

En parte, este debate puede entenderse como un desdoblamiento del impacto que la logística internacional y el comercio mundial sufrieron a partir de la pandemia de Covid-19.

Al final de la pandemia, observamos en este informe que el trabajo remoto y la presión sobre los proveedores de semiconductores llevaron las cadenas de suministro de equipos de TI al límite, aumentando la demanda por la nube y reduciendo el control que las empresas tenían sobre su propio hardware.

La soberanía digital reúne debates sobre el mercado, el acceso a la tecnología y la seguridad nacional. Las consecuencias para las empresas aparecen en el diseño de la infraestructura de TI, que posiblemente tendrá que segregarse para clientes de distintos países, dependiendo de cómo avancen las conversaciones sobre soberanía.

Por otro lado, las inversiones en infraestructura que ya comenzaron en 2025 deberían empezar a mostrar resultados en 2026, creando oportunidades para las empresas que estén preparadas y seguras para este desafío.

Internet de las cosas y tecnología operativa (OT/IoT)

El Internet de las Cosas (IoT) y la Tecnología Operativa (OT) crean desafíos constantes para los equipos de ciberseguridad. Estos equipos no siempre cuentan con un software robusto, y a veces son abandonados por los fabricantes muchos años antes de ser sustituidos.

> Lamentablemente, ese legado viene empeorando, ya que los equipos están envejeciendo.

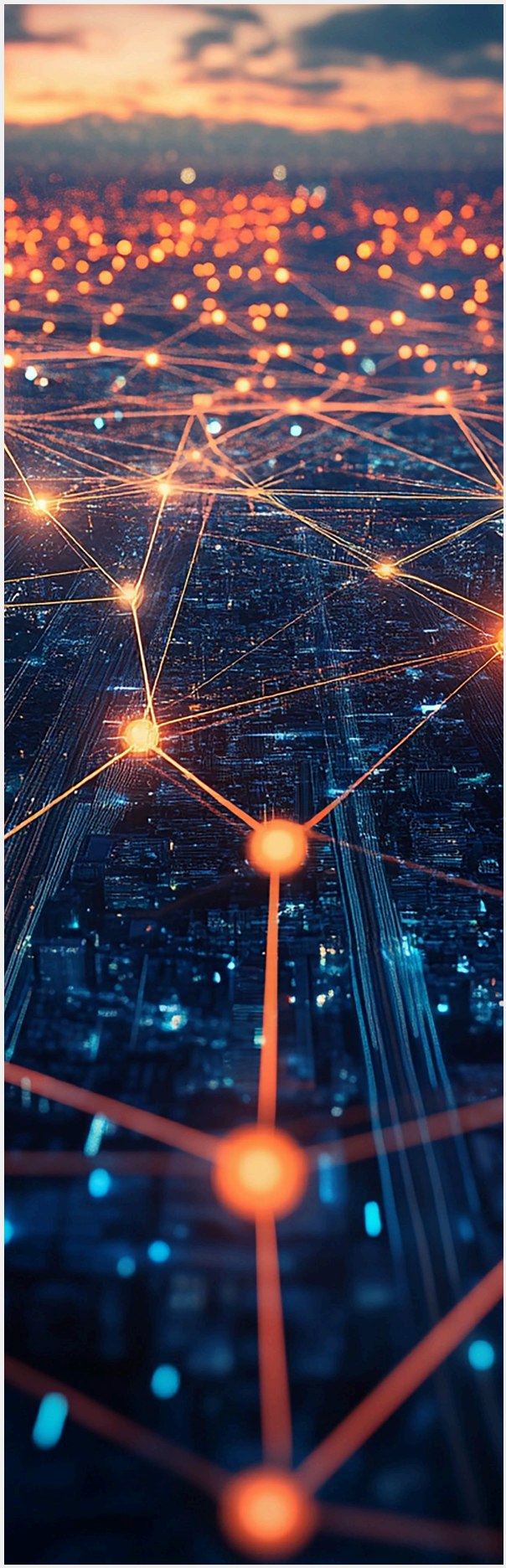
Aunque los fabricantes han asumido un compromiso mucho mayor con la seguridad de los productos en los últimos años, tomará tiempo hasta que todos los equipos sean reemplazados.

> En 2025, botnets antiguas fueron resucitadas con nuevas vulnerabilidades en equipos de red.

Los sectores de telecomunicaciones, energía y salud son especialmente vulnerables a fallas en esta categoría de activos, pero también están presentes en el comercio minorista y en hoteles. Algunas líneas de productos, como las cámaras de seguridad, son utilizadas por negocios de todos los sectores.

Además de la aplicación de parches de seguridad, la principal recomendación para la protección de estos dispositivos es el uso de firewalls o configuraciones de red que impidan cualquier tipo de acceso externo.

Una buena solución es el External Attack Surface Management (EASM) que puede utilizarse para detectar dispositivos accesibles externamente y vulnerabilidades en la infraestructura expuesta.



Insight de la plataforma:
External Attack Surface Management (EASM)

El EASM de Axur fue diseñado para mapear, monitorear y proteger esa superficie de ataque externa, ofreciendo una visión completa de todos los activos accesibles y de las vulnerabilidades asociadas.

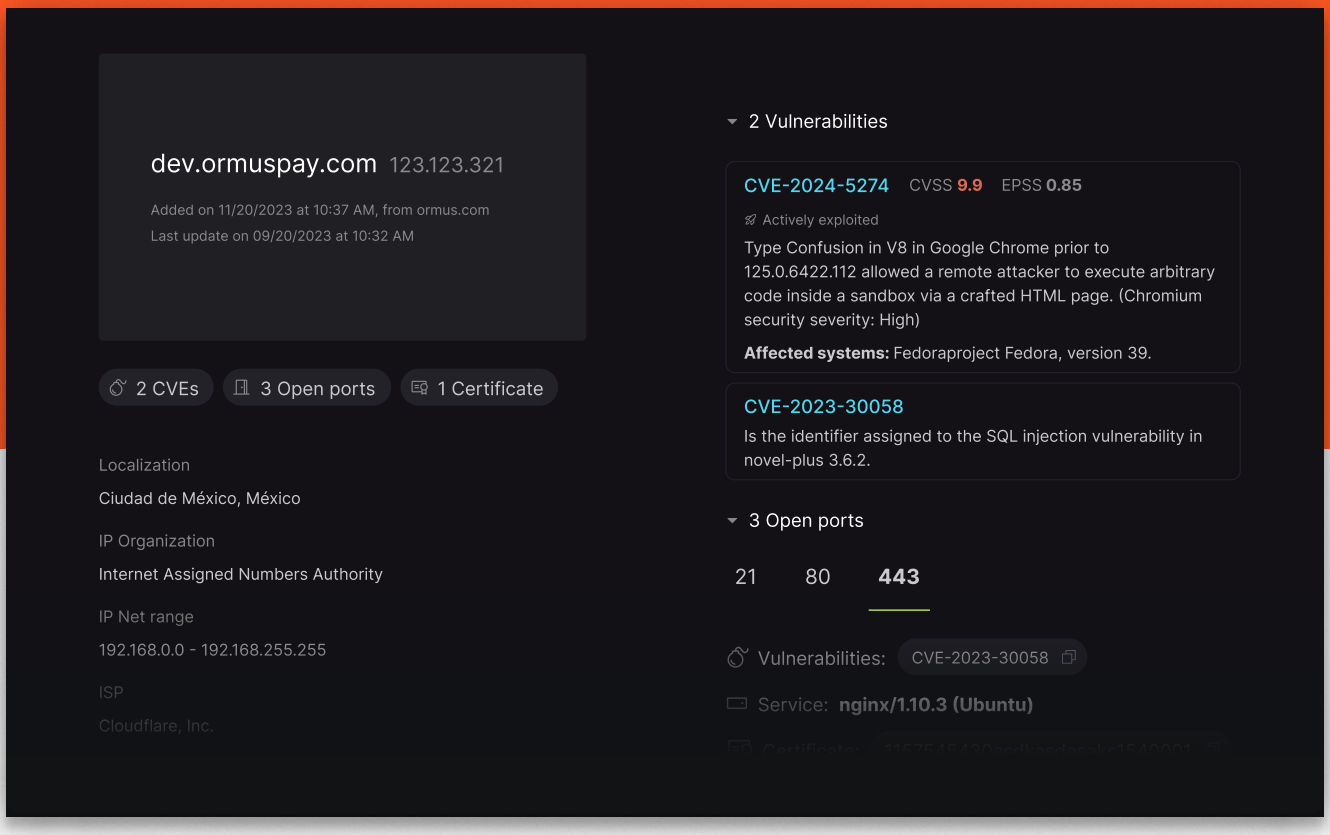
La solución identifica dominios, subdominios, IPs y servicios en ejecución, correlacionando esos datos con bases de vulnerabilidades conocidas (CVEs) y verificando certificados digitales, puertos abiertos y protocolos en uso.

Este análisis continuo permite que los equipos:

Descubran activos desconocidos u olvidados, reduciendo riesgos de shadow IT y exposición accidental.

Anticipen riesgos emergentes por medio de la integración directa con el módulo de Cyber Threat Intelligence (CTI) de Axur.

Clasifiquen vulnerabilidades críticas con base en contexto, gravedad y potencial de explotación.



Desarrolladores en la mira del phishing y de los stealers

Los objetivos tradicionales del phishing son los consumidores y los usuarios de servicios de tecnología. Los ataques de ransomware llevaron el phishing a diversos departamentos de las empresas, que ahora pueden recibir mensajes altamente contextualizados y relevantes para sus respectivas funciones.

> Ahora, sin embargo, estamos observando el crecimiento de un nuevo tipo de phishing dirigido a los desarrolladores de software.

El entorno de desarrollo de software adoptó grandes repositorios de bibliotecas y componentes, como npm (Node.js) y PyPI (Python), además de automatizaciones de múltiples tareas, muchas veces basadas en código de terceros, por ejemplo con GitHub Actions. Estos puntos que conectan varios proyectos de software se convirtieron en objetivos intermedios de hackers interesados en alcanzar a las empresas y usuarios que los utilizan.

En 2025, se observaron ataques de typosquatting dirigidos a los sitios de estos repositorios, así como a paquetes individuales que pueden comprometer a los desarrolladores que los utilicen. Credenciales robadas fueron empleadas para alterar paquetes oficiales y populares, y el incidente de tj-actions en GitHub consiguió propagar código malicioso a varios proyectos.

Integraciones con herramientas de IA pueden crear situaciones indeseadas por fallas de inyección de prompts, como ya mencionamos. Pero no podemos olvidar que, además de las vulnerabilidades técnicas, todos estos procesos involucran a personas susceptibles a la ingeniería social.

Una táctica usada con frecuencia contra programadores en 2025 fue la del empleo falso, en la que la víctima es contactada por un supuesto reclutador para realizar una entrevista. El reclutador solicita que la víctima instale programas o ejecute un código específico para participar en el supuesto proceso selectivo. Si la víctima sigue las instrucciones, el sistema será contaminado con un malware.

Los ataques de malware contra programadores son preocupantes, ya que los infostealers pueden robar tokens con permisos de acceso a repositorios. Resulta algo sorprendente que no haya registro de más casos que involucren el uso indebido de claves de API, pero tal vez eso cambie en 2026.

Insight de la plataforma Axur:
Monitoreo de filtración de datos

El Monitoreo de filtración de datos de Axur identifica credenciales, claves de API, tokens de acceso y secreto en código publicados en entornos públicos como GitHub.

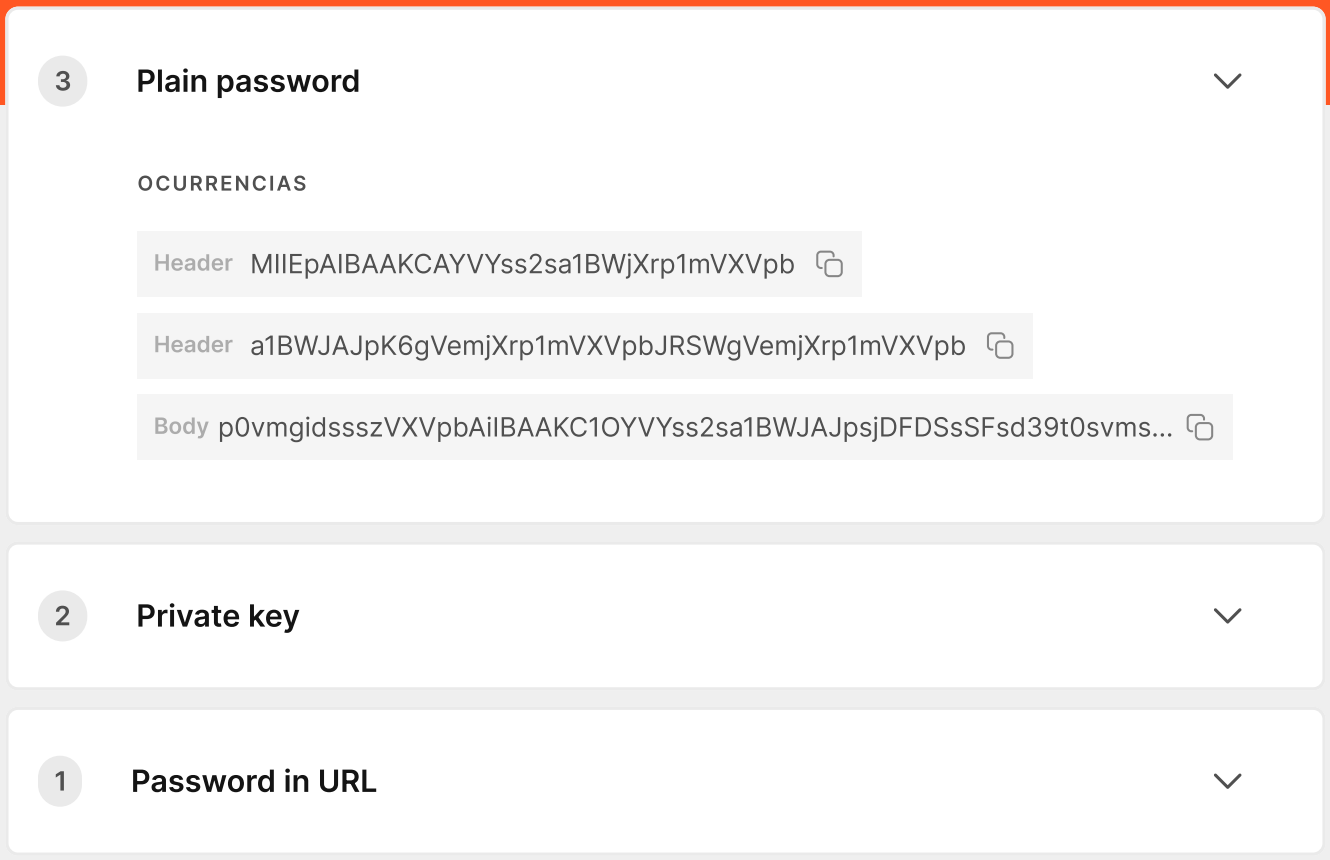
La solución prioriza las alertas según el riesgo y la relevancia para cada organización, ayudando a los equipos a actuar antes de que una exposición se convierta en incidente.

Entre las principales aplicaciones se encuentran:

Localización de credenciales y secretos incrustados en código y en pipelines de automatización, como GitHub Actions.

Identificación de claves reutilizadas o activas, reduciendo la probabilidad de uso indebido.

Exposición de secreto en código



Acciones de ciberseguridad para 2026

Crear políticas para la adopción de IA

En síntesis:

- Los permisos de los agentes de IA deben aprovechar la granularidad que ofrecen la gestión de acceso en APIs y otras integraciones.
- Los agentes de IA pueden automatizar múltiples procesos de análisis, detección y respuesta en ciberseguridad.
- Si el negocio demanda el uso de agentes, los equipos de seguridad tendrán que estar preparados para validar su uso, con políticas y tecnologías para su implementación y auditoría.

La creación de políticas para la adopción de agentes de IA debe estructurarse sobre frameworks graduales de autonomía, en los que cada etapa define la latitud operativa del agente, desde la mera observación hasta la ejecución con políticas y auditoría integradas.

Para cada nivel, la organización debe determinar reglas explícitas de alcance, reversión y observabilidad, garantizando que las acciones automatizadas sean siempre rastreables y reversibles.

El modelo RAIL, Restricciones, Aprobaciones, Aislamiento y Logs auditables, proporciona el cimiento técnico de esas políticas, alineándose con prácticas como NIST CSF 2.0 y CTEM, Continuous Threat Exposure Management. Esto implica definir identidad digital propia para cada agente, permisos basados en el principio de mínimo privilegio y validación humana obligatoria en acciones críticas.

La implementación también debe incorporar métricas de confianza operativa, midiendo la precisión, la reversibilidad y el tiempo medio de respuesta de los agentes, además de prever sandboxing y auditoría continua, de modo que la autonomía venga acompañada de una gobernanza verificable. Este enfoque posiciona las políticas de adopción de IA no solo como directrices éticas, sino como arquitectura de seguridad aplicada, fundamental para sostener la defensa autónoma de forma segura y escalable.

Los equipos de ciberseguridad que se mantengan como pioneros en la adopción de agentes para automatizar sus propias funciones deberían tener mayor facilidad para identificar amenazas emergentes.

Establecer una gobernanza efectiva y alineada al negocio

En síntesis:

- El cumplimiento no debe ser una etapa formal y aislada del proceso de ciberseguridad.
- Siempre que sea posible, las nuevas soluciones de ciberseguridad deben contribuir con las metas de gobernanza establecidas.
- Evaluar cómo medidas técnicas de peritaje, Threat Hunting y CTI pueden perfeccionar procesos de cumplimiento.

El concepto de gobernanza adquiere una nueva dimensión cuando se incorpora a la lógica del Continuous Threat Exposure Management, CTEM. En lugar de tratar cumplimiento y seguridad como ciclos aislados, el CTEM propone una visión continua y orientada por el contexto, donde la gobernanza se sustenta en visibilidad técnica y alineamiento estratégico. Cada etapa se convierte en un mecanismo de gobernanza en sí mismo, conectando datos de riesgo, priorización y respuesta con decisiones de negocio.

Este enfoque complementa la función GOVERN del NIST CSF 2.0 al introducir un modelo operativo que mantiene el control en tiempo real sobre la exposición, no solo sobre políticas estáticas. En lugar de identificar simplemente vulnerabilidades, los equipos de seguridad pasan a definir prioridades con base en el valor del activo, el impacto operativo y el contexto de la amenaza, acercando la gestión de riesgos a la gestión corporativa.

El CTEM también refuerza que la gobernanza necesita ser observable y medible, métricas como cobertura de alcance, tiempo medio de validación y proporción entre exposiciones detectadas y resueltas se convierten en indicadores de madurez.

En la práctica, se refuerza la idea de que la ciberseguridad es responsable por la capacidad de gestión de los activos de TI, así como por sus políticas y procesos que garantizan su cumplimiento.

El trabajo de cumplimiento muchas veces se reduce a procesos formales y lentos, con poco impacto en la resiliencia del negocio. Esto no es sostenible ni responde al interés real de los buenos reguladores, especialmente a la luz de las preocupaciones por la seguridad nacional que han motivado reformas regulatorias en el área de tecnología.

Transformar la capacidad de gobernanza en ganancias reales de resiliencia será una ventaja competitiva para las empresas. Esto se vuelve más fácil cuando la ciberseguridad se alinea al negocio, entendiendo las necesidades de la empresa también en sus necesidades de mercado, en el combate al fraude, en la protección de marca y reputación.

Combatir el fraude contra los consumidores y proteger la reputación de la empresa también son formas de evitar desgastes derivados de acciones judiciales y de la asociación indebida con la actividad ilícita que explota la marca.

La capacidad de investigar incidentes por medio de Threat Hunting y buenas fuentes de Cyber Threat Intelligence también es determinante para alcanzar objetivos reales de cumplimiento. Idealmente, todas las medidas de seguridad que recomendamos, como la automatización por IA, el monitoreo de credenciales y de fugas, y la visibilidad sobre la cadena de suministro, deben ser pensadas también desde la óptica del cumplimiento, convirtiéndolo en parte del proceso de seguridad y no en una etapa formal desvinculada de las medidas técnicas.

Cuanto más robustos sean los controles existentes con fines de gobernanza, más fácil será también la adopción de agentes de IA. Es importante recordar que puede ser difícil prever de qué forma las regulaciones o las necesidades del mercado pueden impactar el negocio. Flexibilidad y capacidad de reacción serán valores importantes en 2026.

Implementar el monitoreo de datos y credenciales

En síntesis:

- Las estafas de extorsión que amenazan con exponer datos corporativos, sustituyendo al ransomware en algunos casos, exigen monitoreo externo de fugas.
- Monitorear credenciales filtradas ayuda a evitar que delincuentes obtengan acceso a datos almacenados en la nube y en plataformas SaaS.
- Monitorear fugas de datos facilita la gobernanza y permite que la empresa adopte una postura más firme con sus socios.

El ransomware tradicional viene cediendo espacio a ataques cibernéticos de extorsión en los que los delincuentes amenazan a las empresas con la exposición de los datos que robaron de los activos a los que accedieron, incluidos aquellos ubicados en la nube, fuera de la red corporativa.

No existen formas de impedir que los datos se expongan si no se paga el rescate y, incluso si la empresa paga, tampoco hay forma de tener certeza de que los datos fueron descartados. Es posible que desavenencias entre los estafadores resulten en una nueva amenaza o que los criminales decidan comercializar la información robada en algún momento, incluso si se pagó el rescate.

Hay dos acciones importantes para aumentar la resiliencia frente a estas amenazas. La primera es proteger todos los activos de la infraestructura de TI, incluidos los externos. El monitoreo de credenciales expuestas es especialmente relevante, siempre considerando también las credenciales corporativas usadas en plataformas de terceros.

Todo lugar que almacene datos corporativos debe ser monitoreado y protegido. En muchos casos, la credencial de un usuario es la única barrera que impide que invasores accedan a datos almacenados en la nube o en soluciones SaaS. Como esas credenciales no se utilizan en los propios sistemas de la empresa, el monitoreo externo es la mejor alternativa.

La segunda acción es el monitoreo de fugas y datos corporativos. Monitorear la exposición de los datos de la empresa tiene beneficios para la gobernanza y para el inicio rápido de gestiones de mitigación de incidentes.

En el caso de datos compartidos con socios o proveedores, ese monitoreo también señala la preocupación por la protección de datos, sirviendo como herramienta para detectar indirectamente las violaciones de seguridad en terceros que resulten en una fuga.

Buscar visibilidad sobre la cadena de suministro

En síntesis:

- Los hackers están buscando vulnerabilidades en toda la cadena de suministro de un objetivo.
- Ciertas soluciones de ciberseguridad pueden utilizarse para ampliar la visibilidad sobre la cadena de suministro.
- La inteligencia de amenazas y las integraciones de IA pueden pensarse de manera cooperativa con los socios.

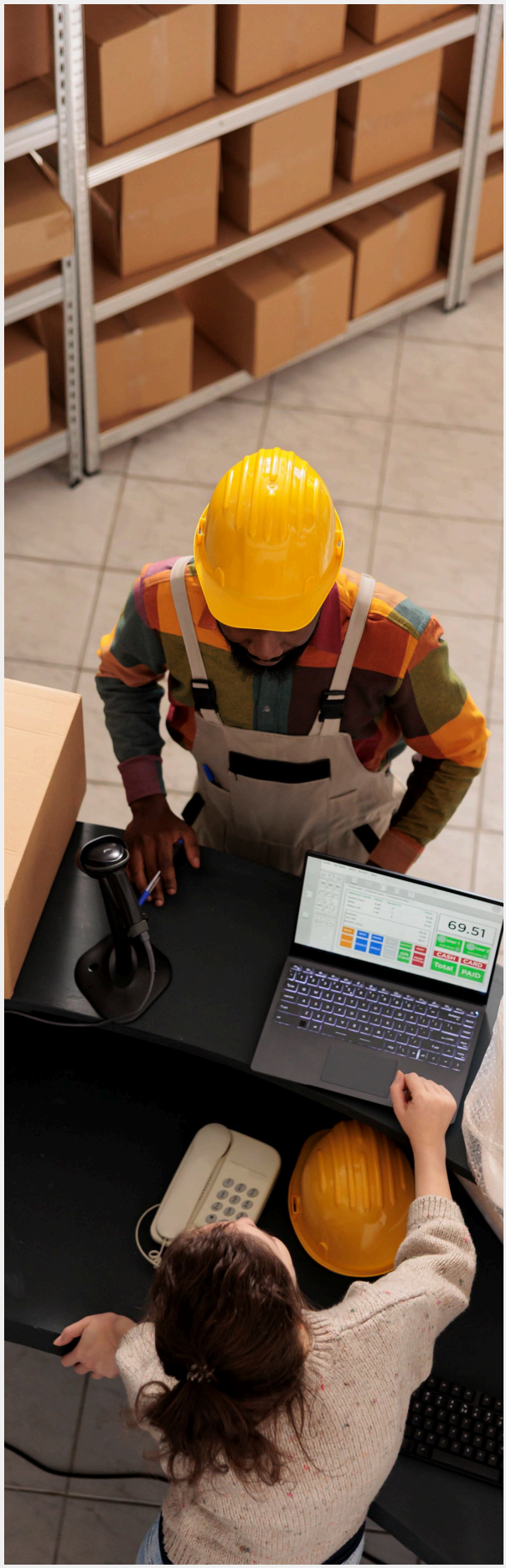
Los actores maliciosos vienen demostrando la capacidad de localizar vulnerabilidades en terceros para alcanzar a sus objetivos. Por ello, es importante buscar medios para ampliar la visibilidad sobre toda la cadena de proveedores y terceros, la supply chain.

Conviene mencionar que los objetivos pueden ser de oportunidad y no necesariamente predefinidos, a partir de un proveedor vulnerable, se puede entender qué resulta más interesante para los atacantes.

Algunas soluciones de seguridad ya existentes pueden refinarse para incluir la infraestructura de terceros. El Cyber Threat Intelligence de Axur puede configurarse para buscar información sobre las categorías de activos usados por terceros críticos, alertando sobre eventos que puedan indicar un aumento del riesgo en el entorno de los proveedores.

Herramientas como Threat Hunting y los monitoreos de datos expuestos y de credenciales también pueden utilizarse para brindar visibilidad sobre la cadena de suministro.

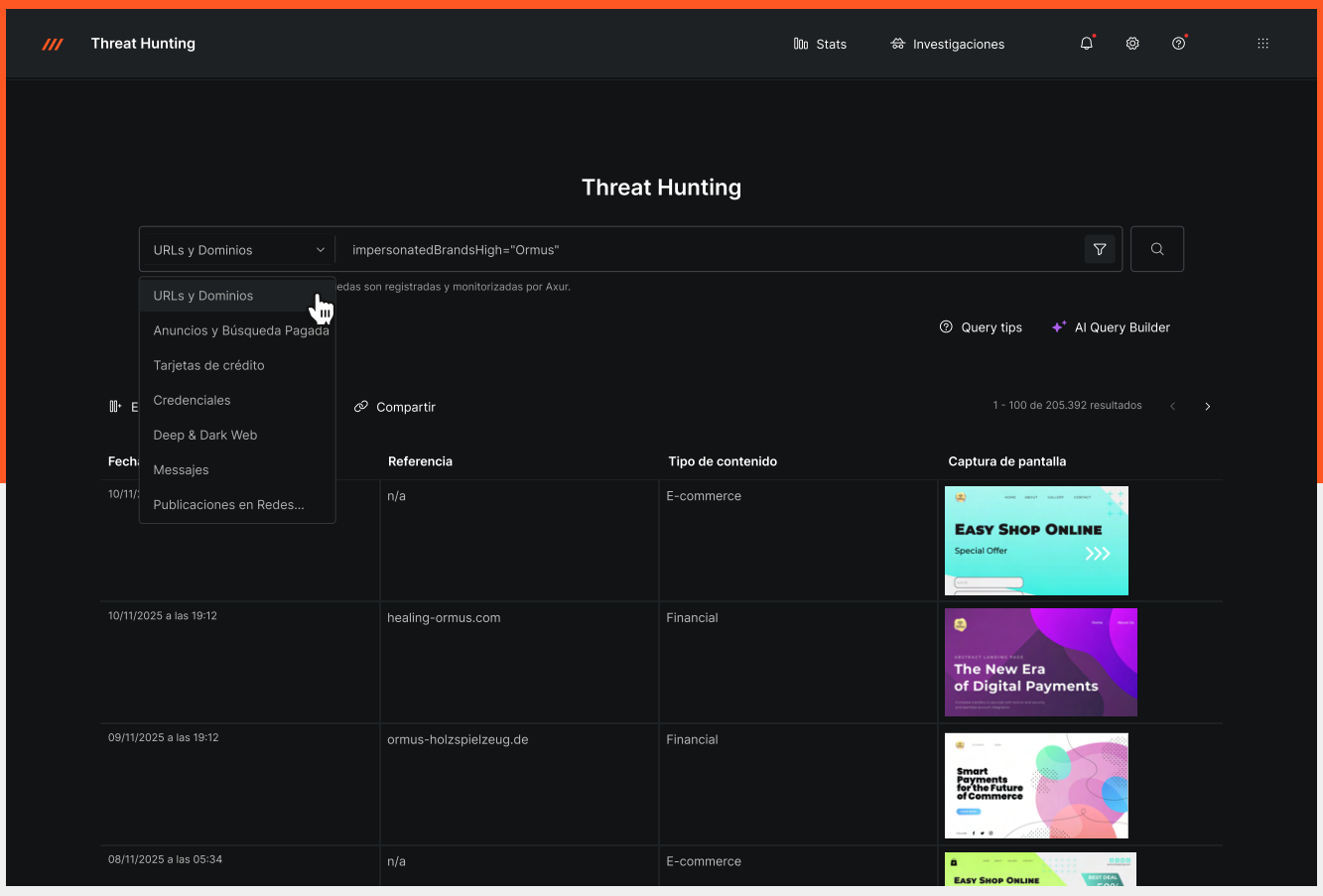
De la misma forma, agentes y otras herramientas de IA pueden emplearse para facilitar la comunicación con terceros y agilizar el tratamiento de incidentes.



Insight de la plataforma Axur:
Threat Hunting

El Threat Hunting de Axur permite realizar búsquedas avanzadas en la base de amenazas externas para identificar exposiciones de credenciales, tarjetas, dominios, mensajes en la deep y dark web, además de URLs maliciosas y perfiles en redes sociales. Además de investigar incidentes internos, la herramienta posibilita localizar credenciales y activos comprometidos de proveedores estratégicos, mapear campañas de phishing dirigidas a socios y anticipar riesgos compartidos en la cadena de suministro.

DESCUBRA 101 CASOS DE THREAT HUNTING



Concienciar a usuarios y socios

En síntesis:

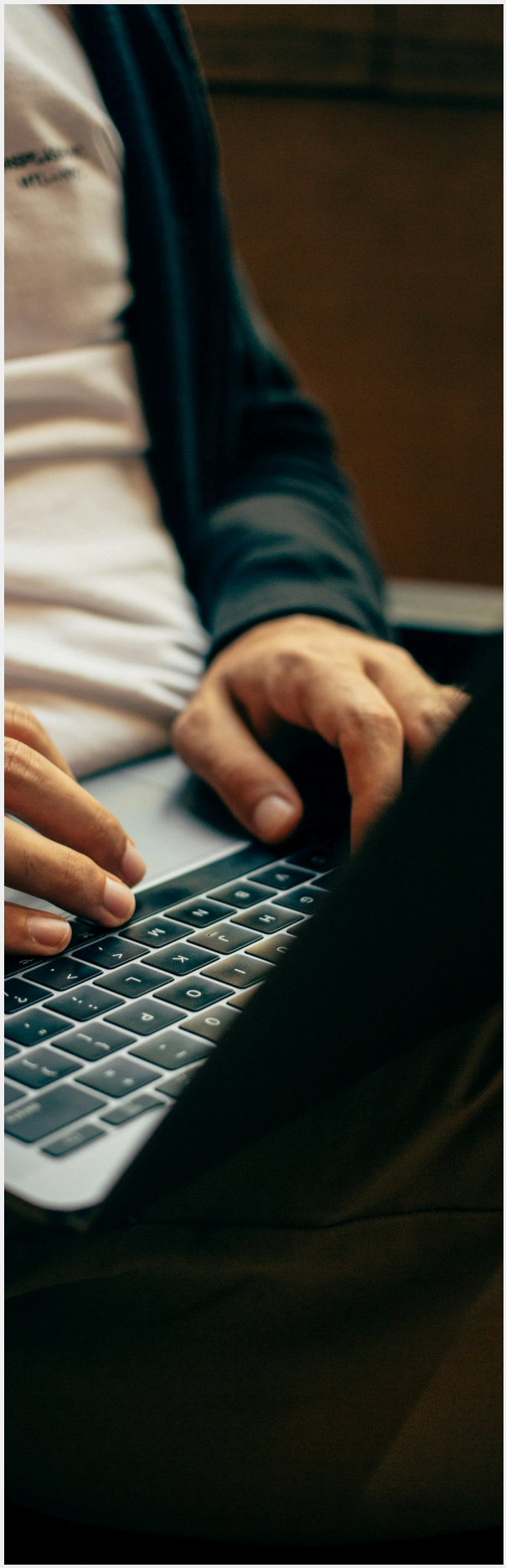
- Los ataques de phishing continúan evolucionando, incluso con nuevos objetivos primarios en algunas campañas.
- Ingenieros de software y equipos de soporte técnico se han convertido en objetivos frecuentes de phishing.
- Es necesario apostar por medidas técnicas, concienciación y capacitación.

Es comprensible que muchos vean el phishing como un problema mayoritariamente centrado en usuarios finales de departamentos sin vínculo con TI. Históricamente, el departamento de Recursos Humanos es uno de los más afectados, ya que criminales pueden hacerse pasar por candidatos para aplicar estafas.

Las fraudes en 2025 cambiaron ese escenario. Ingenieros de software fueron alcanzados por medio de typosquatting, explotación de errores de tipeo, en paquetes y sus repositorios. En otra situación, los delincuentes envían ofertas de empleo falsas y distribuyen un software malicioso bajo la justificación de que sería necesario para realizar la prueba técnica durante la selección.

Si la víctima cree en la estafa, el resultado suele ser la ejecución de un infostealer, que robará credenciales del desarrollador, incluidas las corporativas si estuvieran disponibles.

Estos escenarios, sumados a los ataques de phishing por teléfono que apuntaron a centrales de help desk y soporte técnico, exigen una posible ampliación de las campañas de capacitación y concienciación en seguridad.



Threat Landscape
Producido por el Axur Research Team

El Axur Research Team, ART, es el núcleo de inteligencia e investigación de Axur, responsable de transformar los datos recopilados por la plataforma en conocimiento accionable sobre amenazas digitales.

El equipo combina pericia técnica y visión analítica para mapear tendencias, correlacionar indicadores e identificar comportamientos emergentes en entornos no indexados.

A lo largo del año, el ART conduce investigaciones continuas sobre fraudes digitales, fugas de datos, amenazas externas y exposición de credenciales, entre otros vectores que impactan la seguridad de las organizaciones.

Los hallazgos resultan tanto en informes para clientes de Axur como en insights estratégicos que contribuyen a la comprensión del panorama global de amenazas.

Sobre Axur

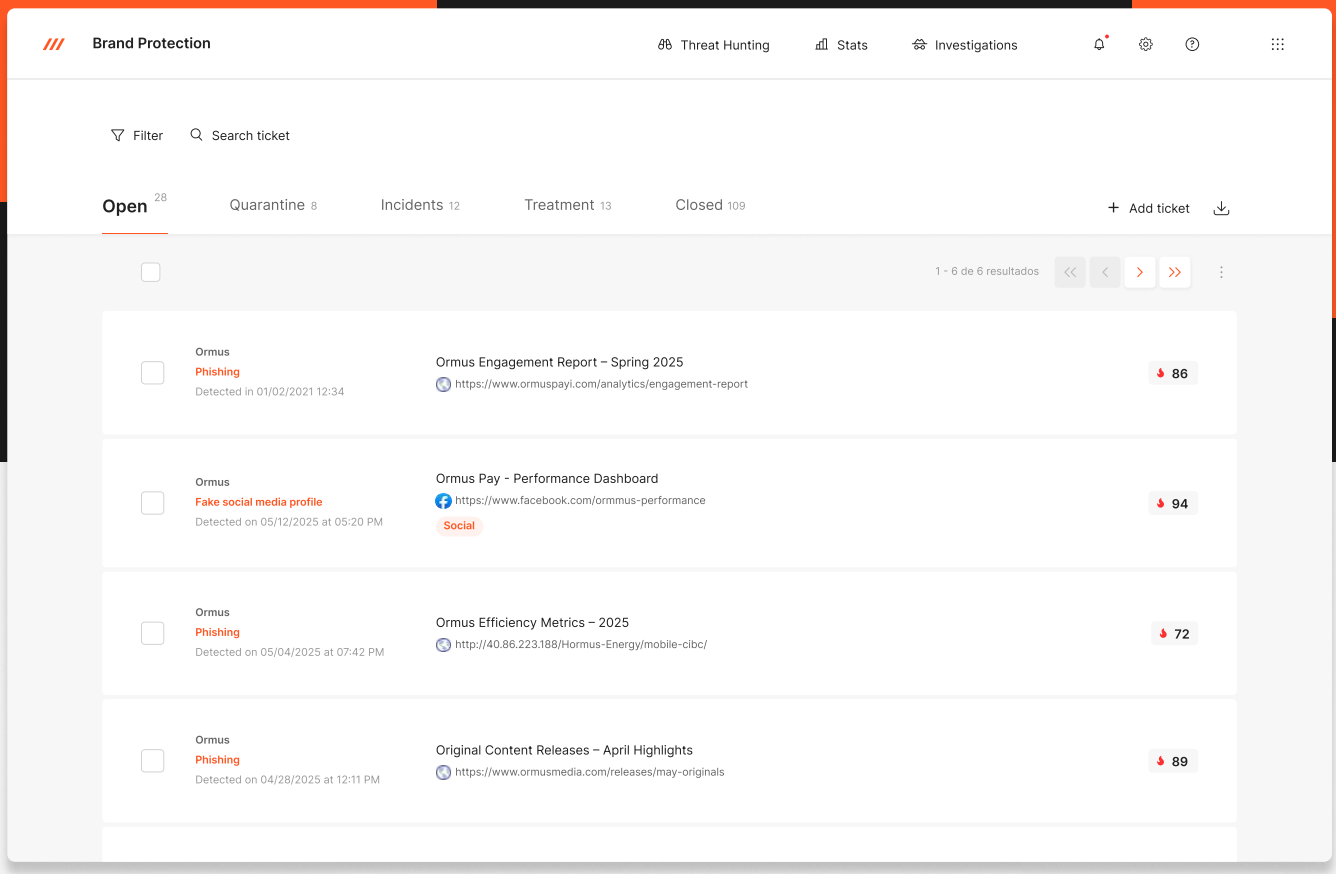
Axur es la empresa líder de ciberseguridad externa que empodera a los equipos de seguridad de la información para gestionar amenazas más allá del perímetro.

Nuestra plataforma detecta, inspecciona y responde a la suplantación de marca, estafas de phishing, menciones en la deep & dark web, vulnerabilidades, exposiciones y más.

Con flujos automatizados y el mejor takedown del mercado funcionando 24/7, Axur elimina contenido malicioso de manera rápida y eficiente, gestionando el 86% de las detecciones automáticamente.

Nuestras herramientas potenciadas por IA escalan la inteligencia de amenazas x180 veces, liberando a su equipo para que se concentre en iniciativas estratégicas.

AGENDE UNA DEMO




THREAT LANDSCAPE
2025 → 2026
AXUR