///AXUR

Threat Landscape

→ 2024/2025

Mensaje de Axur

Las amenazas evolucionan constantemente, pero el 2024 se destacó por desafíos singulares: la profunda integración de la Inteligencia Artificial (IA) en la ciberseguridad y la ampliación del alcance de los riesgos asociados.

Actores maliciosos han utilizado la IA generativa para diseñar campañas de phishing altamente convincentes y automatizar vectores de ataque a una escala sin precedentes. Al mismo tiempo, la IA se ha convertido en una aliada poderosa en la defensa, enfrentando amenazas con una cobertura, velocidad y priorización incomparables. Como se observará en los capítulos de este informe, la IA también desempeña un papel clave en la generación de insights, demostrando cómo la tecnología puede colaborar en la construcción de resiliencia frente a los retos actuales.

Por otra parte, el ransomware sigue siendo una amenaza persistente. Hemos presenciado la aparición de nuevos métodos de acceso, incluidos ataques cada vez más complejos a las cadenas de suministro, mientras los apagones digitales pusieron a prueba la solidez de nuestros sistemas. Sin embargo, en medio del caos, también hemos observado ejemplos notables de colaboración.

El 2024 nos exigió más que nunca. Fue un año para reflexionar no solo sobre las herramientas que utilizamos, sino también sobre la filosofía que guía nuestras estrategias de defensa ante las amenazas del futuro. En lo personal, este periodo reafirmó mi compromiso con nuestra misión: crear experiencias digitales más seguras, aprovechando el poder transformador de la tecnología para conectar, responder y adaptarse con mayor rapidez.

Le invito a explorar este informe, en el que analizamos estas amenazas en constante evolución, presentamos estrategias de respuesta y compartimos insights diseñados para fortalecer su equipo en este entorno complejo. No solo para comprender los desafíos, sino para identificar las oportunidades que estos generan. Para construir resiliencia y garantizar que, a medida que la tecnología avance, lo haga al servicio de un futuro digital más seguro y sólido.

Avancemos juntos.

Fábio F. Ramos
CEO de Axur

Índice

Resumen Ejecutivo

57,2 mil millones de credenciales detectadas, un aumento de 13 veces.

339 millones de tarjetas de crédito y débito identificadas, 26 veces más que en 2023.

Casos de phishing duplicados, con **72.455 páginas maliciosas detectadas.** Cabe destacar que el 70% de estas páginas fraudulentas no contenían palabras clave relacionadas en el dominio.

439.000 incidentes de fraude reportados, un aumento del 118%, incluyendo perfiles falsos, aplicaciones fraudulentas y suplantación de marcas.

Más de **2.3 mil millones de mensajes analizados** en la Deep & Dark Web, resultando en **+966.000 incidentes.**

El 32% de los incidentes en la Deep & Dark Web involucraron contenido audiovisual, como audios, videos e imágenes estáticas.

Más de 401.000 contenidos fraudulentos eliminados mediante flujos automatizados de Takedown.

Aumentaron los ataques a ejecutivos y VIPs, con más de **33.000 incidentes** relacionados con perfiles falsos y exposición de información.

→ Ransomware en salud:
Los ataques interrumpieron servicios críticos en EE. UU. y el Reino Unido.

→ El mayor de la historia:
Cloudflare bloquea un ataque DDoS récord de 3,8 Tbps.

→ Filtraciones en AT&T y Snowflake:
Millones de registros expuestos, revelando vulnerabilidades en telecomunicaciones.

→ Falla de Falcon:
Problemas en el sensor de CrowrdStrike causaron interrupciones y explotaron vulnerabilidades interconectadas.

→ Operación Cronos:
Iniciativa global debilitó al grupo LockBit, marcando avances en la lucha contra el ransomware.

Sectores más afectados

→ Retail/E-commerce

1º en phishing: 27.305 páginas fraudulentas detectadas
3º en incidentes en la Deep & Dark Web: 172.873 incidentes
3º en takedowns: 61.343 contenidos fraudulentos eliminados

→ Finanzas/Seguros

2º en phishing: 15.051 páginas fraudulentas detectadas
2º en incidentes en la Deep & Dark Web: 257.275 incidentes
1º en takedowns: 107.601 contenidos fraudulentos eliminados

→ Tecnología

3º en phishing: 9.502 páginas fraudulentas detectadas
1º en incidentes en la Deep & Dark Web: 418.806 incidentes

→ Telecomunicaciones

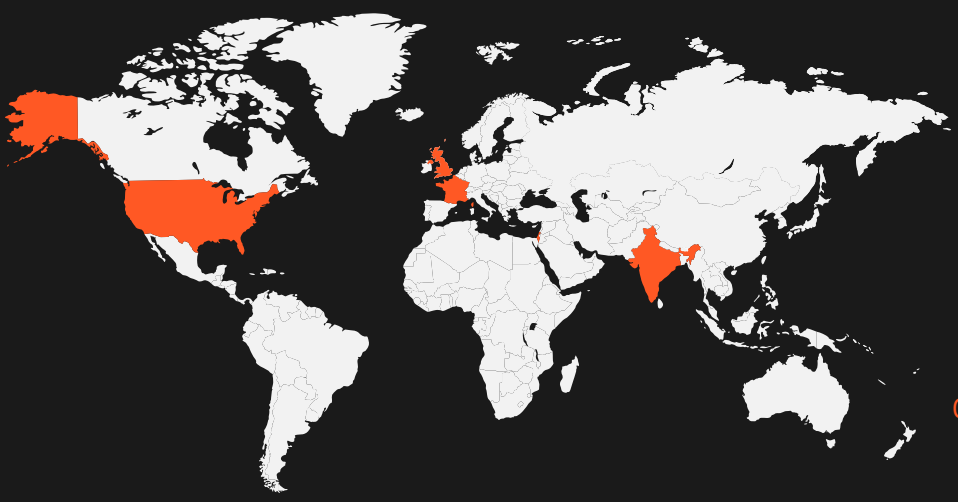
2º en takedowns: 93.287 contenidos fraudulentos eliminados
4º en incidentes en la Deep & Dark Web: 47.018 incidentes

→ Turismo y viajes

5º en takedowns: 45.060 contenidos fraudulentos neutralizados

Principales geolocalizaciones afectadas

EE.UU., India, Reino Unido, Francia e Israel fueron los países más atacados por ciberdelincuentes en 2024.



Tendencias emergentes de ataque

→ IA en cibercrimen: GenAI impulsa deepfakes y ataques personalizados.

→ Expansión de superficies de ataque: Los dispositivos IoT y políticas BYOD aumentan las vulnerabilidades.

→ Infostealers más sofisticados: El robo de credenciales y cookies se vuelve más versátil.

→ Ciberseguridad como prioridad nacional: Las tensiones geopolíticas refuerzan la necesidad de un enfoque robusto.

Recomendaciones

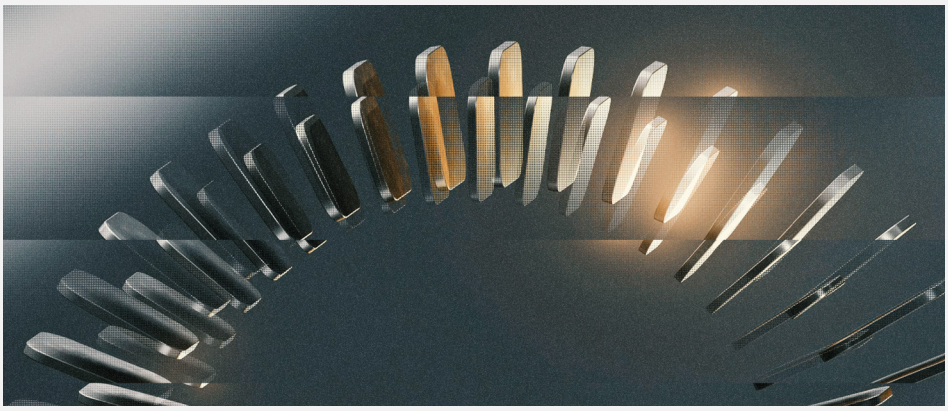
→ Gestión de identidades: Monitorear y revocar credenciales comprometidas, complementando MFA con análisis continuos.

→ EASM y vulnerabilidades: Priorizar vulnerabilidades críticas mediante insights de inteligencia de amenazas.

→ Planes de continuidad: Mapear dependencias críticas para garantizar la resiliencia operativa.

→ Concientización: Implementar programas educativos que fortalezcan la cultura de la seguridad dentro de las organizaciones.

Panorama de Amenazas y Exposición



El panorama de la ciberseguridad en 2024 se presenta como un campo de batalla dinámico y desafiante.

Los ataques de ransomware siguen siendo una preocupación central, con grupos perfeccionando sus tácticas y apuntando a sectores críticos como salud e infraestructura. Además, el auge de los ataques basados en identidad, impulsados por técnicas sofisticadas de phishing y ingeniería social, subraya la necesidad de una defensa robusta. Las vulnerabilidades en la nube también han aumentado, reflejando la creciente dependencia de este tipo de servicios.

El análisis de las CVEs más explotadas revela un aumento significativo en la explotación de vulnerabilidades críticas, donde los ciberdelincuentes aprovechan fallas en sistemas ampliamente utilizados. Los malwares muestran una capacidad creciente para comprometer datos sensibles, mientras que las tácticas más comunes incluyen ataques DDoS y phishing, ejecutados con mayor sofisticación y frecuencia.

Nuestra solución de IA, equipada con inteligencia de amenazas (CTI) integrada, procesa y resume miles de alertas y horas de análisis en información clave, entregando solo los insights más relevantes sobre superficies de ataque específicas o temas de interés previamente definidos.

Esta tecnología avanzada ha sido utilizada para elaborar el panorama de amenazas de este capítulo, con comentarios de Alisson Moretto, Head de Cyber Threat Intelligence de Axur.

44 mil
artículos analizados

6 mil horas
de análisis de amenazas

Revisado y comentado por:

Alisson Moretto

Head de Cyber Threat Intelligence en Axur

> Amplia experiencia en la investigación de crímenes digitales y soporte a incidentes.

> Profesor invitado en programas de posgrado y conferencista en eventos destacados del sector.

Principales insights de 2024

Haga clic en los títulos para ver el análisis completo

↗ Ciberataque a Change Healthcare interrumpe servicios de prescripción en EE. UU.:

Este incidente destaca la vulnerabilidad de los sistemas de salud a los ciberataques, afectando servicios críticos y generando preocupaciones sobre la seguridad de los pacientes y la integridad de los datos.

↗ Qilin Ransomware afecta los servicios de sangre del NHS en Londres:

Este ataque demuestra el potencial del ransomware para interrumpir servicios públicos esenciales, afectando la atención médica y los servicios de emergencia.

↗ Cloudflare detiene el mayor ataque DDoS de la historia:

Cloudflare mitigó un ataque DDoS récord de 3,8 Tbps, llevado a cabo con dispositivos IoT comprometidos y dirigido a diversos sectores, destacando la creciente sofisticación de las ciberamenazas globales.

↗ Filtración de datos de AT&T: Infiltración masiva en Snowflake expone registros de llamadas:

Este caso plantea serias preocupaciones de privacidad para millones de usuarios, evidenciando vulnerabilidades en la infraestructura de telecomunicaciones.

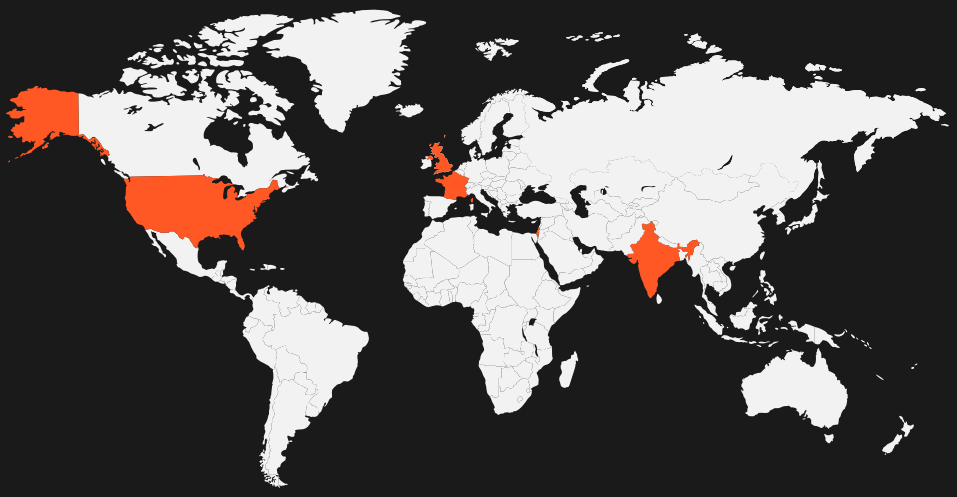
↗ Operación Cronos desmantela la red de ransomware LockBit:

Este esfuerzo de las autoridades refleja un avance significativo en la lucha contra el ransomware, apuntando a disuadir futuros ataques.

↗ Falla global en Falcon expone vulnerabilidades interconectadas:

Una actualización del sensor Falcon de CrowdStrike provocó errores críticos en sistemas, generando ataques de phishing y subrayando la necesidad de controles de calidad y resiliencia cibernética.

Ubicaciones más impactadas en 2024



Estados Unidos, India, Reino Unido, Francia e Israel han sido los principales objetivos de agentes de amenazas en 2024, debido a factores geopolíticos, vulnerabilidades tecnológicas y un incremento general en actividades cibernéticas maliciosas.

Las tensiones geopolíticas, especialmente en Medio Oriente, jugaron un papel crucial. Israel, por ejemplo, se convirtió en un blanco frecuente, en parte por su posición estratégica como aliado de EE. UU. y sus relaciones con países como Irán. En 2024, Israel recibió apoyo militar y cibernético de EE. UU., Reino Unido y Francia para contrarrestar ataques iraníes, atrayendo la atención de grupos hostiles como RipperSec.

Los sectores de gobierno, educación y salud en países como EE. UU. y Reino Unido han demostrado ser vulnerables, manejando datos sensibles y operando infraestructuras que los ciberdelincuentes pueden explotar.

Actores maliciosos más activos

El panorama cibernético en 2024 se caracteriza por la evolución constante de los actores de amenaza. Grupos como RansomHub y ShinyHunters están destacándose por sus operaciones agresivas y su impacto significativo.

Mientras tanto, otros grupos como LockBit enfrentan dificultades debido a la presión de las autoridades. Además, la colaboración entre grupos hacktivistas está aumentando, reflejando una nueva estrategia en el escenario de las amenazas cibernéticas.

Activo desde: 2020

Motivación: financiera

Sectores más afectados: organizaciones en Estados Unidos y Europa, con enfoque en infraestructura y otros sectores

País de origen: Rusia

RansomHub ↗

Reencarnación del ransomware Knight, se convirtió rápidamente en uno de los grupos más destacados tras el declive de LockBit3, con más de 210 víctimas nuevas en 2024.

Activo desde: 2020

Motivación: financiera

Sectores más afectados: financiero y otras empresas ricas en datos

País de origen: opera internacionalmente

ShinyHunters ↗

Este grupo capturó la atención tras atacar a Ticketmaster y exponer datos de 560 millones de usuarios, consolidando su capacidad para llevar a cabo ataques masivos.

Activo desde: 2023

Motivación: política

Sectores más afectados: gubernamentales o empresas de países contrarios a su ideología

País de origen: Malasia

RipperSec ↗

Este grupo sobresalió por sus ataques DDoS y campañas hacktivistas como #FreeDurov, destacando la creciente colaboración entre grupos antes aislados.

Activo desde: 2022

Motivación: financiera

Sectores más afectados: varios, incluyendo gobierno, telecomunicaciones, energía y otros

País de origen: Rusia

Intelbroker ↗

Aunque con poca información nueva, este agente sigue activo en foros, compartiendo accesos y datos sensibles.

Activo desde: 2019

Motivação: financiera

Sectores más afectados: varios, incluyendo industria, salud, educación y otros

País de origen: Rusia

LockBit ↗

Tras una serie de exitosas operaciones policiales contra LockBit3, el grupo experimentó un declive significativo en sus actividades. Este grupo fue responsable de más de 2,000 víctimas en todo el mundo y extorsionó más de 120 millones de dólares en pagos de rescate. En 2024, la cooperación entre 10 países permitió desmantelar su infraestructura.

CVEs destacados en 2024

Grupos de ransomware han comenzado a explotar esta vulnerabilidad para inyectar cargas maliciosas e instalar ransomware en servidores vulnerables.

Es necesario aplicar el parche actualizando a las versiones 8.1.29, 8.2.20 o 8.3.8. Además, se recomienda utilizar el Verificador de Susceptibilidad a Inyección de Argumentos, implementar un WAF, restringir el acceso a scripts PHP-CGI, validar entradas y realizar auditorías de seguridad regulares.

Se identificó una vulnerabilidad crítica de ejecución remota de código en el software Veeam Backup and Replication, que afecta a versiones 12.1.2.172 y anteriores, con una puntuación CVSS de 9,8. Se lanzaron dos parches para solucionar el problema, siendo el segundo una corrección completa. Esta vulnerabilidad está relacionada con ataques de deserialización en un mecanismo de comunicación antiguo, explotada ampliamente por grupos de ransomware.

Descubierto en SolarWinds Web Help Desk (WHD), permite a atacantes no autenticados acceder y modificar detalles de tickets, exponiendo datos sensibles como credenciales y solicitudes de restablecimiento de contraseña.
Se lanzó un hotfix para resolver el problema.

Una vulnerabilidad en libcurl ocurre cuando una aplicación permite HTTP/2 server push y los encabezados recibidos superan el límite de 1000. En este caso, libcurl aborta el push pero no libera toda la memoria asignada, causando una fuga de memoria silenciosa que dificulta su detección.
Esta vulnerabilidad puede causar una condición de denegación de servicio.

Identifica un problema en los métodos de verificación de direcciones IPv4 mapeadas en IPv6. Métodos como IsPrivate e IsLoopback devuelven resultados incorrectos para direcciones que serían válidas en sus formas tradicionales IPv4.

Se trata de una vulnerabilidad de deserialización de datos no confiables que puede permitir la ejecución remota de código (RCE) con una carga maliciosa, incluso sin autenticación.

Más insights sobre CVEs con Axur

Comience su prueba gratuita de nuestra solución Cyber Threat Intel con IA y descubra todo sobre las amenazas más relevantes de 2024.

Demo gratuita

Malware más activos en 2024

En 2024, el panorama de malware se caracterizó por un aumento en la sofisticación de los ataques y por la prevalencia del ransomware como servicio (RaaS). Grupos ampliamente conocidos siguen evolucionando sus estrategias para maximizar el impacto financiero sobre sus víctimas.

TTPs más utilizados

T1078 - Cuentas válidas

Esta técnica se refiere al uso de credenciales legítimas para obtener acceso a sistemas. Los atacantes frecuentemente explotan cuentas válidas para evitar la detección y mantener acceso a redes comprometidas, siendo particularmente eficaz en entornos donde las credenciales son reutilizadas o mal gestionadas.

T1190 - Explotación de aplicaciones públicas

Esta técnica abarca la explotación de aplicaciones web expuestas públicamente en internet. Los atacantes pueden aprovechar fallos para obtener acceso inicial a redes corporativas, especialmente en organizaciones que no aplican parches con rapidez.

T1071 - Protocolos de capa de aplicación

Implica el uso de protocolos de capa de aplicación para comunicarse con servidores de comando y control (C2). Los atacantes emplean esta técnica para extraer datos o recibir instrucciones sin levantar sospechas, utilizando protocolos comunes como HTTP o HTTPS.

T1059 - Interpretación de comandos y scripts

Involucra el uso de lenguajes como PowerShell, Bash o Python para ejecutar acciones maliciosas en sistemas objetivo. Es una técnica común en ataques que buscan automatización o ejecución remota, evitando controles de seguridad.

T1203 - Explotación de ejecución del cliente

Se refiere a la explotación de vulnerabilidades en software del cliente para ejecutar código malicioso. Esto puede ocurrir mediante la apertura de documentos o enlaces maliciosos en correos electrónicos, permitiendo la ejecución no autorizada. Es una técnica común en ataques dirigidos.

T1566 - Phishing

Comprende ataques de phishing donde los atacantes engañan a los usuarios para revelar información sensible como credenciales o datos financieros. Esta técnica sigue siendo de las más prevalentes debido a su eficacia y bajo costo.

1st	T1078	129 fuentes
2nd	T1071	125 fuentes
3rd	T1203	48 fuentes
4th	T1190	27 fuentes
5th	T1059	27 fuentes

2024 en números

Credenciales

La plataforma de Axur detectó 57,2 mil millones de credenciales filtradas a lo largo de 2024, evidenciando la necesidad de una gestión de identidad precisa y eficiente para proteger servicios en línea y redes corporativas.

Estas detecciones se basan en actividad de la Deep & Dark Web y en archivos compartidos en la web indexada, incluyendo foros frecuentados por ciberdelincuentes.

57.233.053.785

Total de credenciales recogidas de todas las fuentes

19.299.578.150

Credenciales de empresa

Por lo tanto, se puede afirmar que todas estas credenciales ya están en manos de actores maliciosos. Si estas credenciales no son revocadas y reemplazadas, las cuentas permanecerán en riesgo.

Además, casi todas las credenciales (98%) ya se encuentran sin ningún tipo de cifrado. Esto sugiere que los ciberdelincuentes están utilizando técnicas para identificar contraseñas asociadas a hashes filtrados (como MD5 y SHA) o accediendo a contraseñas sin cifrado a través de infostealers.

Según el Verizon Data Breach Investigations Report (DBIR) 2024, el 31% de todas las brechas de acceso en los últimos diez años se debieron al uso de credenciales robadas. En ciertas categorías de ataque, como la toma de control de cuentas en plataformas web, más del 70% de los accesos no autorizados ocurrieron debido al uso de credenciales débiles o previamente comprometidas.

La amenaza de los infostealers

En 2024, los infostealers fueron responsables de la obtención de 3.2 mil millones de credenciales.

Esta categoría de malware incluye códigos diseñados específicamente para robar credenciales. Las familias de infostealers están en constante evolución para evadir la detección por parte de soluciones antivirus.

A diferencia de los keyloggers tradicionales, que operan de manera pasiva esperando que el usuario acceda a un sistema para capturar contraseñas, los infostealers están programados para buscar y extraer información directamente del sistema.

Cuando es posible, acceden a contraseñas almacenadas en navegadores web, gestores de contraseñas y aplicaciones instaladas en el equipo (como billeteras digitales, plataformas de software y videojuegos, entre otros). Además, pueden robar cookies almacenadas en los navegadores.

El robo de cookies y tokens de acceso permite realizar ataques de secuestro de sesión (session hijacking). Utilizando sesiones previamente autenticadas, los atacantes pueden eludir la autenticación multifactor (MFA).

Los infostealers suelen propagarse mediante campañas de ingeniería social, softwares piratas y phishing. Las credenciales obtenidas se venden a otros ciberdelincuentes especializados. Por ejemplo, mientras que las contraseñas de bancos o billeteras digitales pueden usarse para fraudes financieros, las credenciales de VPN o servicios de acceso remoto suelen aprovecharse en ataques de ransomware.

Nuevas recomendaciones

Las contraseñas, además de ser robadas por infostealers, pueden comprometerse a través de ataques de fuerza bruta y ataques de credential stuffing, que reutilizan contraseñas expuestas en múltiples servicios.

Incluso contraseñas cifradas o representadas mediante algoritmos de hash pueden vulnerarse utilizando Rainbow Tables o mediante el aumento progresivo de la capacidad computacional.

Actualización de estándares

En septiembre de 2024, el National Institute of Standards and Technology (NIST) publicó una revisión de sus Password Guidelines. Este documento recomienda que las organizaciones adopten un enfoque proactivo, bloqueando credenciales comprometidas, en lugar de imponer reglas rígidas, como cambios periódicos de contraseñas.

☑ Recomendaciones actuales

→ **Revocar contraseñas comprometidas:**
Los sistemas deben revocar credenciales filtradas y prevenir su reutilización. También deben bloquear nuevos registros con contraseñas comprometidas.

→ **Uso de contraseñas largas:**
Se deben incentivar contraseñas de al menos 15 caracteres. Los sistemas no deben aceptar contraseñas menores a 8 caracteres.

→ **Permitir hasta 64 caracteres:**
Es importante permitir contraseñas largas, incluidas frases (passphrases).

☒ Prácticas no recomendadas

→ **Cambios periódicos de contraseña**:
Obligar a cambiar contraseñas puede llevar a la creación de claves más débiles. Es preferible enfocarse en la revocación de credenciales comprometidas y la adopción de MFA.

→ **Requisitos de caracteres especiales**:
Las contraseñas largas y bien construidas ofrecen mayor entropía que aquellas con caracteres especiales. Los sistemas deben aceptar cualquier carácter Unicode.

→ **Preguntas y pistas de seguridad**
Este método no es seguro, ya que los atacantes pueden usar estas herramientas para adivinar contraseñas.

Tarjetas

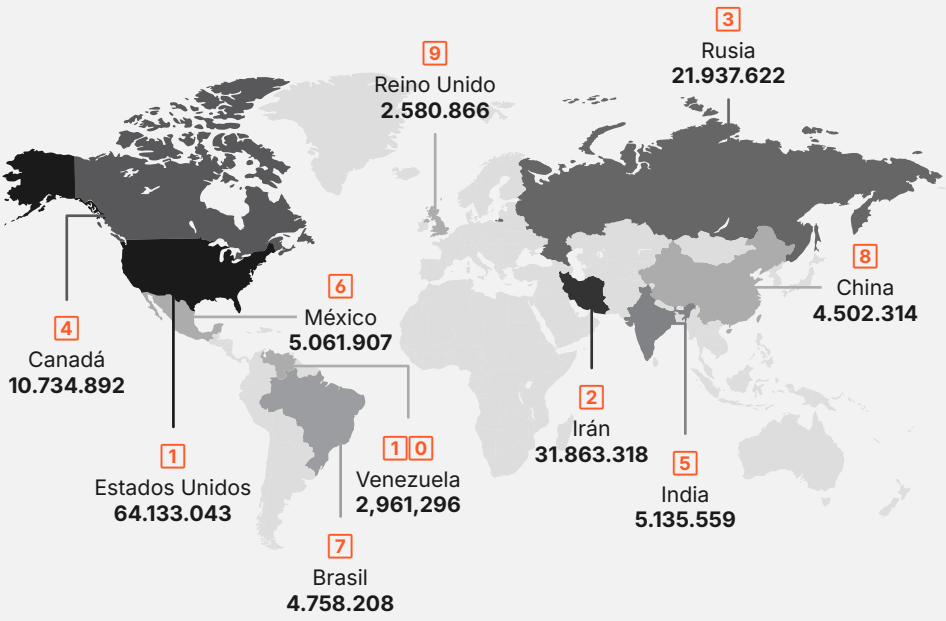
Los ciberdelincuentes compartieron 339 millones de tarjetas de crédito y débito en 2024.

Crecimiento de tarjetas expuestas

2023	**13.5 millones**
2024	**339 millones**

El volumen de tarjetas robadas se mantiene elevado. Gracias al BIN (Bank Identification Number), es posible estimar el origen de cada tarjeta filtrada.

Las tarjetas estadounidenses, con alto poder adquisitivo, continúan liderando esta lista.



El robo de tarjetas afecta tanto a las instituciones financieras como al comercio electrónico, que en muchos casos asumen las pérdidas relacionadas con productos y servicios adquiridos mediante tarjetas robadas. Axur monitorea estas filtraciones para ayudar a las empresas a bloquear el uso fraudulento de dichas tarjetas.

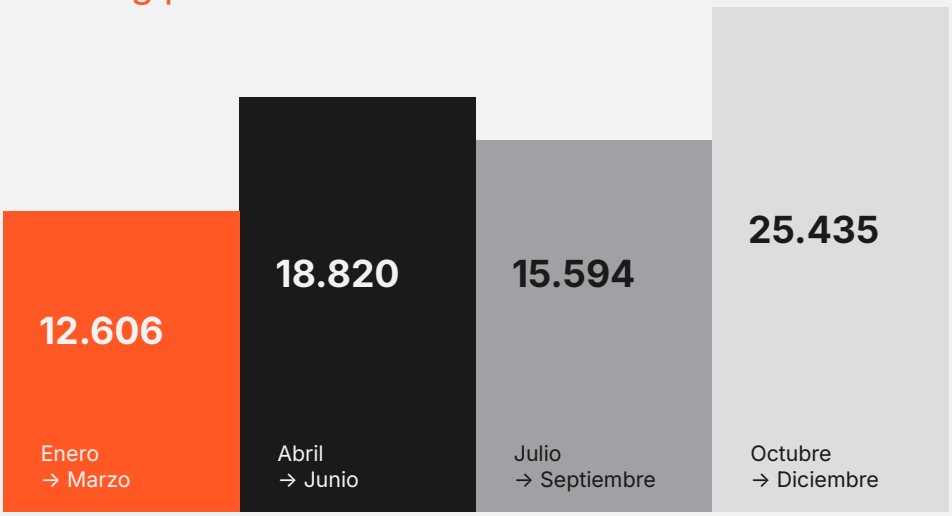
Phishing

El volumen de páginas de phishing detectadas se duplicó en 2024, alcanzando las 72.455.

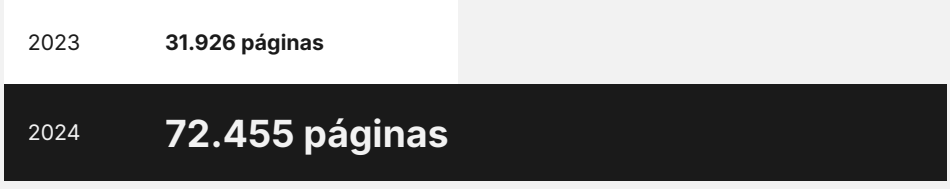
Detectar páginas de phishing es una etapa crucial en la lucha contra el fraude en línea. El monitoreo de Axur se centra en identificar páginas donde las víctimas podrían ser inducidas a proporcionar información sensible.

Este enfoque resulta especialmente relevante en el entorno móvil, donde los ataques suelen explotar marcas conocidas a través de publicidad en aplicaciones o SMS. En este contexto, identificar y eliminar estas páginas es esencial para mitigar riesgos y proteger a los usuarios en un espacio que concentra gran parte de las actividades de consumo y operaciones financieras.

Phishing por trimestre



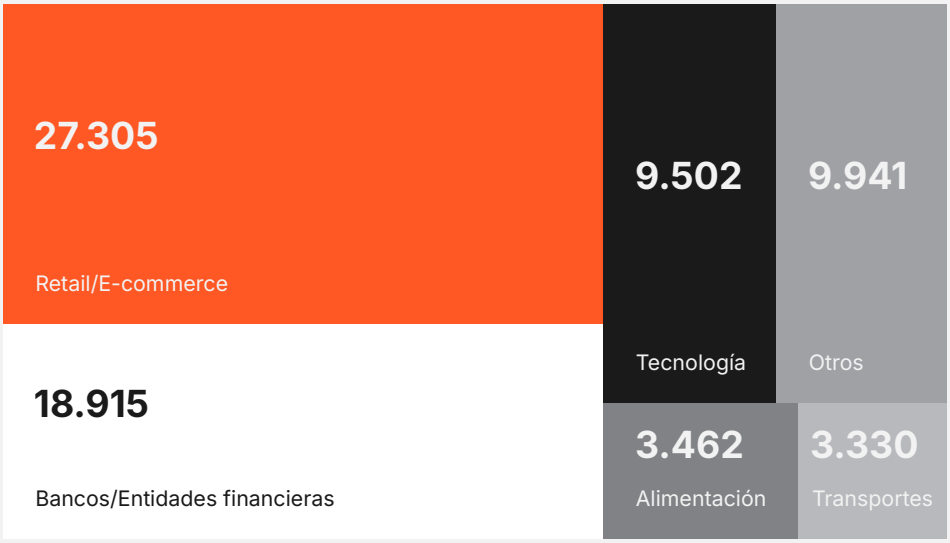
El crecimiento de las páginas de phishing



El sector minorista y el comercio electrónico siguen siendo los más afectados por ataques de phishing, seguidos de cerca por las instituciones financieras. Los estafadores suelen utilizar cuentas comprometidas para realizar compras fraudulentas o acceder a información personal.

Además, las marcas de retail se emplean con frecuencia como vehículo para robar datos de tarjetas de crédito, que posteriormente se usan para adquirir productos o servicios.

Phishing por sector



70% de los ataques de phishing no contienen una palabra clave en el dominio

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

Cómo los LLM están redefiniendo la detección de amenazas

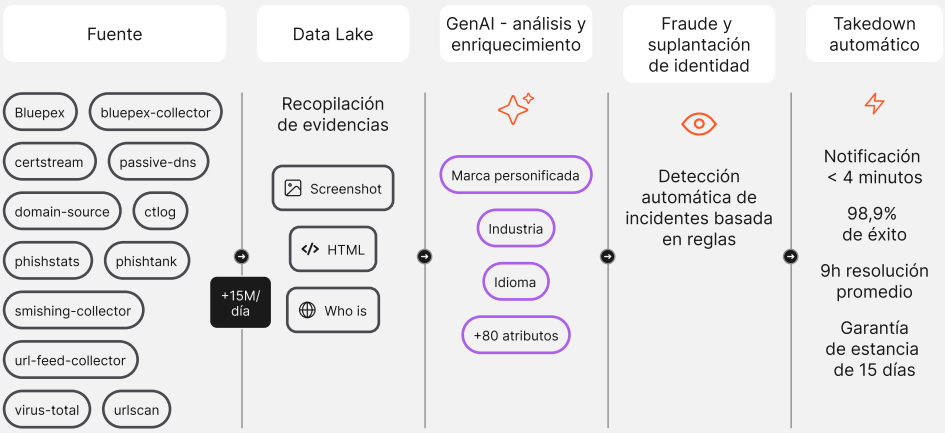
Axur ha dado un paso adelante en la identificación de amenazas digitales con el desarrollo de Clair LLM (Cyber Lens for Anomaly and Impersonation Recognition), un modelo propietario basado en IA generativa. A diferencia de las soluciones tradicionales, Clair utiliza Vision Language Models (VLMs) diseñados internamente y entrenados con más de 15 años de datos y experiencia en la detección de contenido fraudulento. Esta tecnología combina análisis textual y visual para inspeccionar más de 15 millones de sitios diarios, aumentando significativamente la capacidad de detectar fraudes sofisticados.

El modelo procesa URLs, analiza el contenido de las páginas y genera descripciones detalladas. Identifica marcas presentes, detecta solicitudes de credenciales, pagos o contraseñas, y evalúa si hay intentos de suplantar a una marca específica.

Todo esto ocurre de manera automática, sin necesidad de intervención humana. La precisión se debe a la integración de datos enriquecidos y análisis avanzados que van más allá de la detección basada en palabras clave. Además, el uso de modelos propios garantiza que todos los datos procesados permanezcan dentro de la infraestructura de Axur, asegurando la privacidad de la información analizada.

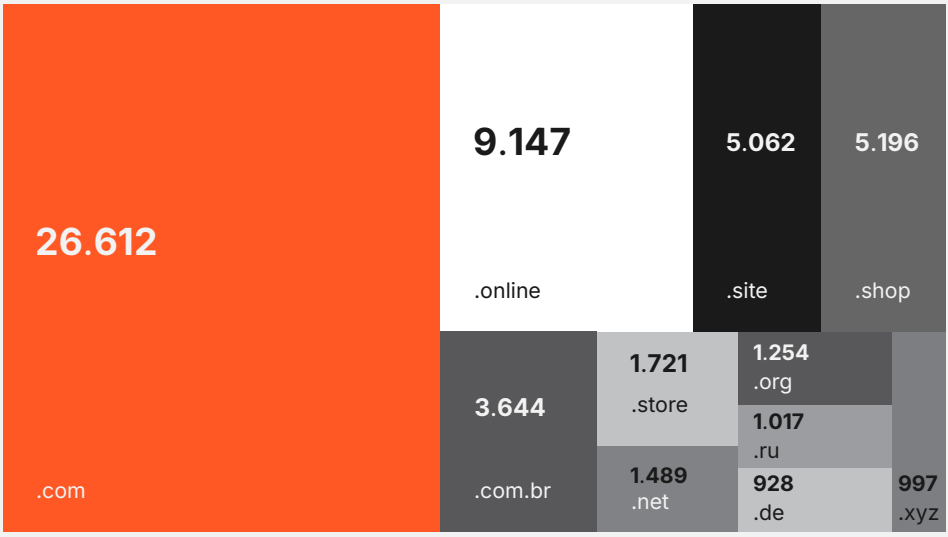
Con la herramienta de Threat Hunting, los equipos de ciberseguridad y antifraude utilizan el modelo Clair para profundizar en la investigación de campañas de phishing. Aplican filtros personalizados que mejoran la visibilidad sobre los ataques, manteniendo la eficiencia de las detecciones automatizadas.

Una nueva era en la protección de marcas



Uso de dominios de nivel superior

En el 2024, se observó un aumento en la proporción de fraudes realizados en dominios de nivel superior (TLDs) como ".shop" y ".store", reflejando la prevalencia de estafas de phishing relacionadas con el comercio minorista y el e-commerce.



Los dominios de nivel superior (TLDs) son los sufijos de las direcciones web, como ".com" (que puede ser utilizado por cualquier persona u organización), ".gov" (reservado para sitios gubernamentales) y ".uk" (sufijo de país). En el pasado, la concesión de TLDs era bastante limitada, y solo unas pocas instituciones estaban autorizadas a operarlos, principalmente para representar regiones o países (como ".br", ".de", ".jp", ".ar", entre otros).

Desde 2012, se ha implementado un procedimiento para solicitar un dominio genérico de nivel superior (gTLD), lo que ha flexibilizado la creación de nuevos sufijos. Cada TLD es gestionado por una organización (registry), que puede optar por vender subdominios para recuperar los costos de infraestructura y del proceso de solicitud.

Dado que el procedimiento para obtener un gTLD es costoso y burocrático, los ciberdelincuentes deben elegir entre los TLDs existentes para registrar un dominio que les permita ampliar el alcance de su estafa o hacerla más creíble.
Esta elección es crucial para sitios de phishing, ya que la dirección de la página será probablemente verificada por las víctimas.

Factores considerados por los ciberdelincuentes al elegir un dominio:

→ Familiaridad del dominio

La mayoría de los usuarios de internet están acostumbrados a visitar sitios terminados en ".com". Sin embargo, los sufijos más populares suelen tener pocas opciones disponibles.

→ Disponibilidad del dominio

Como los dominios cortos, palabras simples y marcas registradas ya no están disponibles en TLDs tradicionales, los delincuentes recurren a TLDs genéricos más recientes o a alternativas similares.

→ Relevancia temática

Muchos sufijos de gTLDs tienen temáticas específicas. Un delincuente puede optar por un dominio que haga la estafa más convincente.

→ Costo

Algunos TLDs son más costosos que otros. En casos como ".edu" y ".gov", que no están disponibles para registro, los ciberdelincuentes solo pueden utilizarlos si logran comprometer un sitio legítimo.

→ Políticas del registry y respuesta a fraudes

Aunque todas las registradoras deben cumplir ciertas normas, el tratamiento de casos específicos varía. Esto puede influir en la preferencia de los ciberdelincuentes, ya que afecta cuánto tiempo permanecerá activa la estafa.

Análisis de TLDs		
DPN	2023	2024
.com	32,9%	36,65% ↑
.online	19,6%	12,6% ↓
.shop	16,9%	7,16% ↓
.site	7,3%	6,97% ↓
.com.br	5,6%	5,02% ↓
.store	5,1%	2,37% ↓

Takedowns realizados

401.000 casos de contenido fraudulento fueron eliminados gracias a las notificaciones de Axur.

A medida que el phishing se vuelve más sofisticado y explora nuevos canales como SMS y publicidad en aplicaciones, el tiempo de respuesta para eliminar contenido malicioso se vuelve un factor crítico. Detectar una página de phishing es solo el primer paso para mitigar los riesgos: una notificación rápida y estructurada para su eliminación es esencial para reducir el tiempo de exposición al ataque.

En 2024, Axur llevó a cabo más de 401.000 takedowns mediante notificaciones dirigidas a proveedores de infraestructura, redes sociales o servicios de alojamiento utilizados por los ciberdelincuentes. Esto fue posible gracias a un proceso altamente automatizado respaldado por inteligencia artificial, que acelera el envío de notificaciones y recopila las pruebas necesarias para garantizar un mayor éxito.

La eficacia de las solicitudes depende de un enfoque técnico y preciso: identificar al proveedor correcto, presentar pruebas claras y cumplir con los formatos requeridos. Sin embargo, el éxito también está vinculado a la credibilidad construida a lo largo de los años, lo que mejora la confiabilidad de las notificaciones y reduce los retrasos en su cumplimiento.

Además, durante el intervalo entre la notificación y la eliminación, medidas proactivas como alertas a navegadores y proveedores de seguridad ayudan a limitar el impacto del fraude, protegiendo a posibles víctimas. Este conjunto de estrategias es clave para garantizar una alta tasa de éxito en las solicitudes realizadas.

Takedowns

401 mil	98,9%	4 minutos	9 horas
Takedowns solicitados	Tasa de éxito	Tiempo medio de 1ª notificación	Resolución promedio

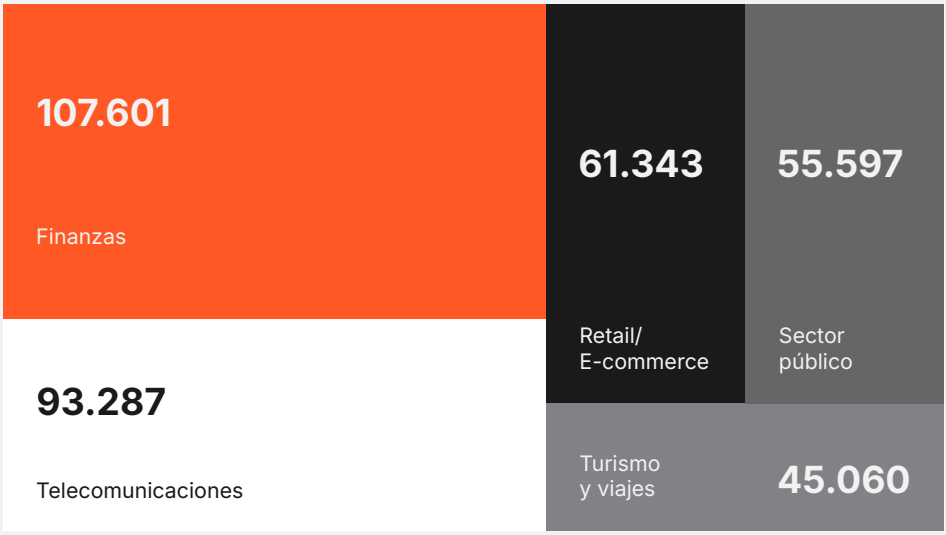
Detecte, analice y elimine las amenazas más rápido que nunca

- Takedowns con un clic o 100% automáticos
- Notificación en <4min
- 98,9% de éxito
- 9h tiempo promedio de actividad
- Garantía de estancia de 15 días
- Web Safe Reporting
- Siga todo el proceso
- Pague sólo por takedowns exitosos

Sectores más afectados

En 2024, el sector financiero lideró con el 29,8% de los casos, lo que resultó en más de 107.000 notificaciones. Telecomunicaciones y retail/e-commerce representaron juntos el 42% de los incidentes, sumando aproximadamente 154.000 páginas eliminadas.

Sectores como turismo y el sector público también enfrentaron desafíos, con más de 100.000 páginas fraudulentas neutralizadas.



Deep & Dark Web

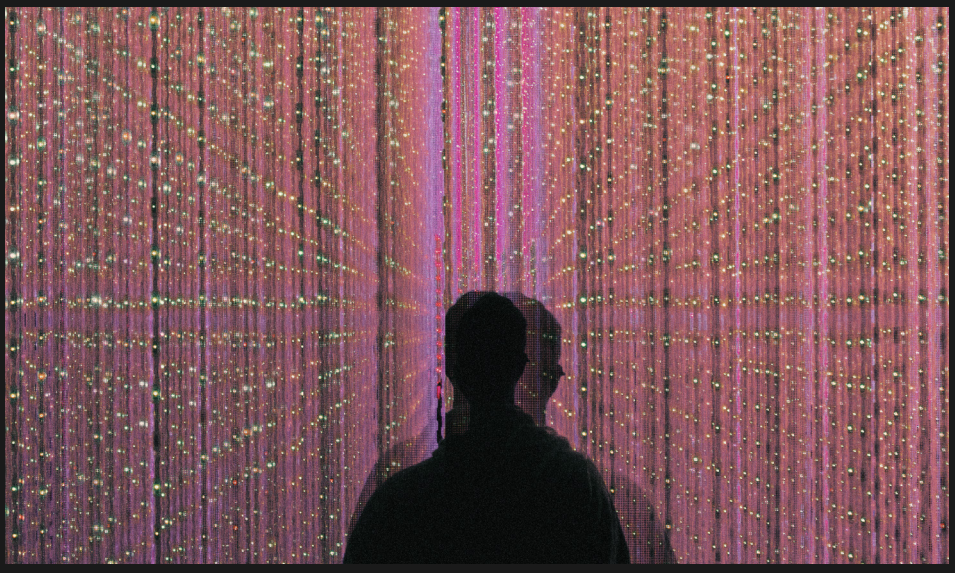
Analizamos 2.3 mil millones de mensajes en entornos de la Deep & Dark Web para proveer inteligencia sobre ciberamenazas e incidentes.

El cibercrimen es hoy un ecosistema complejo que conecta a todos los individuos y grupos involucrados en ataques cibernéticos. Estos canales de comunicación existen para agilizar el crimen y maximizar las ganancias ilícitas de sus actividades.

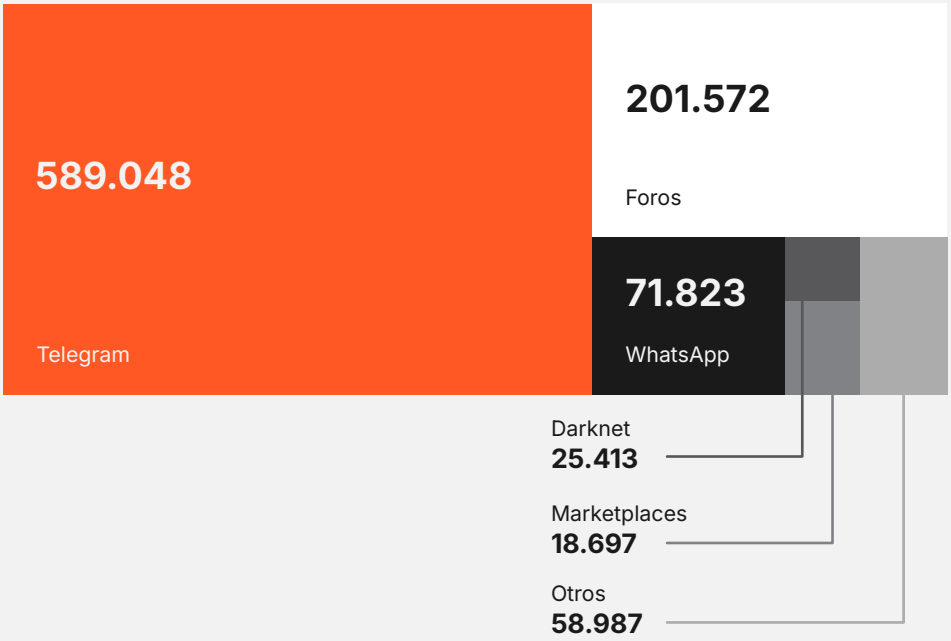
No obstante, estos espacios en la Deep & Dark Web representan una oportunidad para recolectar inteligencia y rastrear los movimientos de cada actor.

Axur monitorea estas plataformas y analiza las comunicaciones de los ciberdelincuentes para identificar indicios de incidentes de exposición de datos, vulnerabilidades o campañas de fraude.

Esta información se traduce en 966.170 incidentes detectados: la clave está en filtrar e interpretar el material recopilado en forma de alertas.



Fuentes de Deep & Dark Web



Tipos de detección

Análisis por sectores

Sectores	2023	2024
Retail	45%	18% ↓
Banca	26,1%	25% ↓
Tecnología	16,8%	44% ↑
Telecomunicaciones	4,8%	5% ↑
Turismo	3,6%	2% ↓
Otros	3,7%	6% ↑

Contenido audiovisual

En 2023, cerca del 25% de los incidentes en la Deep & Dark Web se detectaron en contenido audiovisual. Esta tendencia fue aún más relevante en 2024, donde casi la mitad de las comunicaciones analizadas correspondieron a audios, videos o imágenes, gracias al uso de inteligencia artificial para transcribir audio y convertir imágenes en texto.

68%

Texto

32%

Audio, video e imagen

Perfiles falsos, aplicaciones móviles ilegítimas y el uso fraudulento de marca

Hemos detectado casi medio millón de fraudes digitales con sofisticadas estrategias para engañar a los consumidores

En 2024, Axur identificó más de 439.000 casos de fraudes digitales, incluyendo perfiles falsos, aplicaciones móviles ilegítimas, uso indebido de marcas en búsquedas pagadas, dominios similares a los originales y otras asociaciones fraudulentas. Estos incidentes reflejan las múltiples estrategias utilizadas por los ciberdelincuentes para engañar a los consumidores y dañar la reputación de las empresas.

151.119 perfiles falsos en plataformas de redes sociales

262.575 casos de uso fraudulento de marca

20.934 aplicaciones móviles ilegítimas

Los perfiles falsos en redes sociales, que sumaron 151.000 casos, suelen emplearse para promover páginas de phishing o engañar a seguidores de cuentas legítimas, solicitándoles información sensible o pagos fraudulentos.

De los perfiles falsos reportados por Axur en 2024, más del 80% fueron eliminados en colaboración con Meta Ads, responsable de Facebook e Instagram, sumando más de 57 mil takedowns a través de los flujos automatizados de Axur.

Con los cambios implementados por Mark Zuckerberg en las políticas de moderación de las redes sociales, será crucial monitorear los impactos en futuras eliminaciones.

Más información ↗

En cuanto a las 20.000 aplicaciones móviles ilegítimas detectadas, estas se aprovechan del entorno móvil para exigir interacciones adicionales tras su instalación, como la concesión de permisos para acceder a datos o monitorear actividades en los dispositivos, ampliando así el alcance y el impacto de los fraudes.

Ejecutivos y VIPs

Los ejecutivos suelen ser los principales objetivos de los ataques digitales debido a su posición de influencia y acceso a información confidencial. Los delincuentes emplean ingeniería social para explotar sus redes de contactos, ya sea mediante perfiles falsos en redes sociales o intentos de engañar a empleados y socios

Estas tácticas buscan obtener datos confidenciales como credenciales de acceso, tarjetas corporativas e información estratégica que pueda ser utilizada en ataques dirigidos.

→ Uso indebido de imagen: Las herramientas de edición de imágenes han permitido desde hace tiempo la superposición de rostros en fotografías. Sin embargo, la posibilidad de alcanzar una amplia audiencia a través de publicidad económica en internet ha facilitado el uso sistemático y fraudulento de la imagen de personalidades públicas.

Los deepfakes, creados mediante inteligencia artificial, han ampliado las posibilidades para este tipo de actividades fraudulentas.

Este uso indebido de la imagen y semejanza de figuras reconocidas puede emplearse en campañas de phishing contra empresas, pero también para promocionar productos y servicios de manera irregular. Esto genera una asociación engañosa entre un individuo y un producto o evento, confundiendo a los consumidores.

→ Datos confidenciales: Otro riesgo significativo es la exposición de datos confidenciales, como credenciales corporativas e información de tarjetas de crédito, frecuentemente encontrados en filtraciones de la deep y dark web.

Estos datos pueden ser utilizados para acceder a sistemas internos, realizar transacciones financieras o planificar ataques dirigidos.

Detectamos más de 33.000 incidentes relacionados con Ejecutivos y VIPs.

Tendenciαs

↗ La Inteligencia Artificial (IA) sigue liderando las тendencias

↗ Ransoмware: nuevos actores y regulación

↗ Nuevos мétodos de autenticación y adaptación de atacantes

↗ Phisнing: fronteras nuevas y tácтicas sofisticadas

↗ Ciвerseguridad como seguridad nacional

↗ Expansión de las superficies de ataque

La Inteligencia Artificial (IA) sigue liderando las тendencias

El potencial de la IA generativa se consolida tanto en la defensa de redes corporativas –a través de productos de Cyber Threat Intelligence (CTI)– como en fraudes digitales que emplean deepfakes y contenido personalizado para sus víctimas. Sin embargo, la GenAI no es la única forma de aprovechar los algoritmos de Deep Learning.

Por esta razón, la IA continúa siendo una fuente de innovación y riesgos que deben monitorearse de cerca. Actualmente, ya existen soluciones de ciberseguridad que utilizan IA para generar análisis avanzados, y es probable que esta misma capacidad sea aprovechada por ciberdelincuentes para crear mercados de curaduría de datos filtrados.

Podemos prever que los algoritmos de GenAI se perfeccionarán, facilitando fraudes más sofisticados mediante identidades falsas. Además, podrían surgir vulnerabilidades en las plataformas de IA mismas, como la descubierta por analistas de Wiz, que permitía ejecutar comandos y acceder a datos de otros clientes en una plataforma de "IA como servicio".

El ransomware también evolucionará gracias a la IA, permitiendo ejecuciones más rápidas, precisas y dirigidas. Con algoritmos avanzados, los ataques serán más difíciles de detectar y contener.

Ransoмware: nuevos actores y regulación

Operaciones policiales y conflictos internos han impactado significativamente a grupos de ransomware como LockBit y BlackCat en 2024. Sin embargo, otros grupos han ocupado rápidamente su lugar, demostrando la resiliencia del modelo de "ransomware como servicio" (RaaS) y el continuo interés de los atacantes en este modelo de fraude.

Desde mediados de 2024, las autoridades están considerando regulaciones que dificulten o incluso prohíban el pago de rescates. Además, crece la presión para que las aseguradoras dejen de cubrir estos pagos, ya que algunos analistas consideran que pagar incentiva a los delincuentes.

Es esencial que las empresas sigan de cerca estos desarrollos para estar preparadas, tanto en la prevención de incidentes como en la recuperación de sistemas. También deben evitar sorpresas por cambios en las pólizas de seguros cibernéticos o la legislación.

Nuevos métodos de autenticación y adaptación de atacantes

Mientras muchas empresas todavía enfrentan dificultades para implementar un segundo factor de autenticación (2FA), la tecnología avanza hacia el uso de passkeys. Sin embargo, no parece que estemos cerca de una solución definitiva de autenticación.

Por lo general, nuevos métodos de autenticación logran mitigar los ataques existentes, forzando a los atacantes a adaptarse. Sin embargo, los infostealers, que han ganado popularidad desde la adopción del MFA, son mucho más versátiles que el phishing tradicional, ya que pueden robar cookies y burlar el MFA. Esta versatilidad significa que los atacantes se adaptan rápidamente.

En 2025, es probable que los hackers perfeccionen aún más los infostealers.

Además, ciertos vectores de ataque, como OAuth y aplicaciones en la nube, podrían volverse más comunes incluso entre atacantes menos sofisticados.

Phisнing: fronteras nuevas y tácтicas sofisticadas

Muchos ataques están evolucionando hacia nuevas modalidades de phishing o ingeniería social, utilizando deepfakes, amenazas físicas o fraudes publicitarios en redes sociales. Las narrativas de los ataques cambian constantemente, dificultando los esfuerzos de concientización.

En 2025, el phishing seguirá siendo una amenaza importante. Actualmente, el 70% de los sitios maliciosos no mencionan la marca en sus dominios, y el 18% tampoco lo hace en sus textos. Esto requiere monitoreo avanzado que pueda detectar abusos de marca mediante imágenes u otros elementos sutiles.

El comercio electrónico, las instituciones financieras y los proveedores de tecnología seguirán siendo las principales marcas implicadas en estos ataques, aunque empresas de todos los sectores están en riesgo de ataques dirigidos a sus empleados.

Ciвerseguridad como seguridad nacional

Las tensiones en el escenario geopolítico han acercado el tema de la ciberseguridad al concepto de seguridad nacional. En 2024, muchos legisladores mostraron interés en analizar toda la cadena de proveedores de tecnología y las empresas que ofrecen estos servicios. La directora de la Agencia de Seguridad Cibernética e Infraestructura de los Estados Unidos llegó a declarar que el problema de la ciberseguridad es un "problema de la calidad del software".

Dado que muchas organizaciones desarrollan software o soluciones digitales personalizadas, es posible que el rigor técnico en los procesos de desarrollo y las medidas de seguridad de la información se conviertan en un diferenciador clave en el mercado en los próximos años. De este modo, una postura sólida en ciberseguridad podría transformarse en una ventaja comercial y un requisito indispensable para cerrar contratos.

Aunque esto no llegue a concretarse, el vínculo entre la ciberseguridad y la geopolítica también plantea otro tipo de preocupaciones, como la actuación de grupos de hacktivismo.

El posicionamiento de las empresas en medio de estas tensiones y la visibilidad sobre las filtraciones de datos realizadas por hacktivistas pueden llegar a ser aspectos valiosos en este contexto. Sin embargo, es esencial seguir de cerca lo que suceda a continuación, especialmente en regiones como América Latina, donde el tema aún no tiene la misma relevancia.

Expansión de las superficies de ataque

La proliferación de dispositivos IoT (Internet of Things) y la adopción de políticas de BYOD (Bring Your Own Device) amplían significativamente las superficies de ataque de las organizaciones. Cada dispositivo conectado, ya sea personal o corporativo, puede convertirse en un punto de entrada vulnerable para los ciberataques. Este desafío se ve agravado por la falta de estándares de seguridad consistentes en dispositivos IoT y por el aumento de endpoints fuera de las redes corporativas tradicionales.

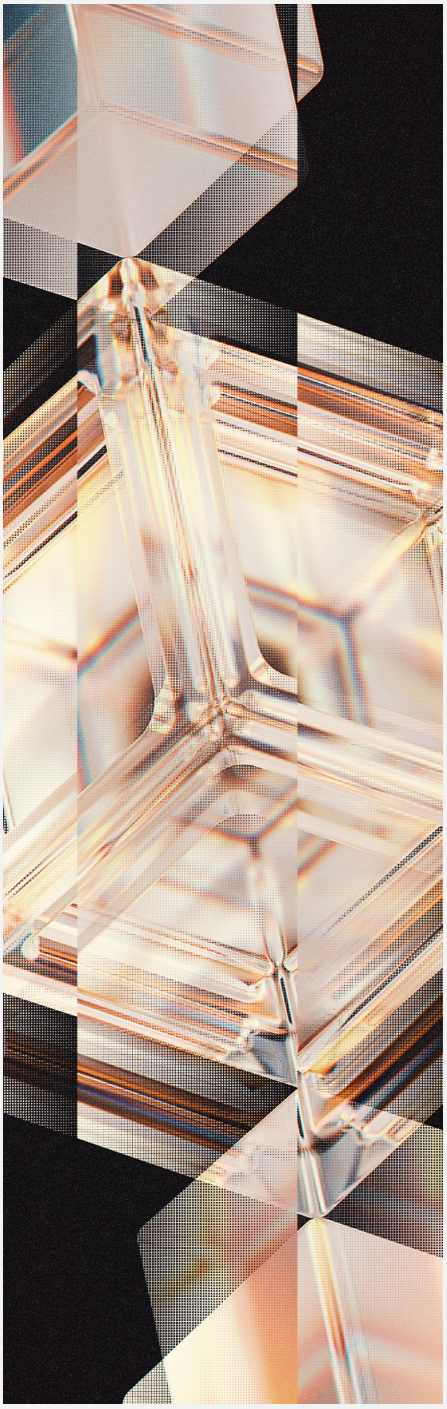
Será necesario implementar medidas de seguridad robustas, como la gestión centralizada de dispositivos, la segmentación de redes para aislar dispositivos menos seguros y la aplicación frecuente de parches y actualizaciones. Además, políticas claras sobre el uso de dispositivos personales y soluciones de monitoreo continuo serán fundamentales para identificar y responder rápidamente a posibles actividades maliciosas.

Recomendaciones

Gestión de identidades

La gestión inadecuada de identidades y credenciales se ha revelado como una de las principales vulnerabilidades de las empresas en 2024. Muchas organizaciones aún están en proceso de implementar autenticación multifactor (MFA) en todos sus puntos de acceso, pero las políticas de Identity and Access Management (IAM) ya deben considerar aplicaciones en la nube, claves API y otros mecanismos de acceso que suelen ser incompatibles con soluciones diseñadas para credenciales de usuarios humanos. Migrar estos sistemas a otro paradigma de autenticación a corto plazo puede no ser una tarea trivial.

El monitoreo de credenciales filtradas es una de las herramientas más importantes para mantener a las empresas un paso adelante de los atacantes, permitiendo bloquear credenciales antes de que sean usadas en ataques. Esta estrategia es especialmente útil para complementar soluciones basadas en MFA o proteger sistemas en proceso de migración.



Gestión de vulnerabilidades

La explotación de vulnerabilidades sigue siendo uno de los vectores de ataque más comunes para acceder a redes corporativas, evidenciando deficiencias en la gestión de vulnerabilidades.
La expansión de la infraestructura de TI y su descentralización hacia áreas específicas del negocio explican parte de este problema, pero incluso la aplicación de parches puede ser ineficaz cuando se corrigen vulnerabilidades menos críticas antes que las más urgentes.

Por ello, las empresas deben adoptar nuevos métodos para mejorar la visibilidad de su infraestructura de TI. Una solución que combine External Attack Surface Management (EASM) con alertas basadas en Inteligencia Artificial proporciona insights de alta relevancia sobre las vulnerabilidades más críticas, mejorando tanto la visibilidad como la priorización de los parches.

Plan de continuidad de negocios

Cuando las operaciones de una empresa dependen directamente de su infraestructura de TI, el impacto de los incidentes cibernéticos tiende a ser mayor. Ya existen casos emblemáticos de empresas que han entrado en procesos de reestructuración financiera o han cerrado sus operaciones tras ataques de gran magnitud. En 2024, por ejemplo, MediSecure inició un proceso de voluntary administration en Australia tras un ciberataque, y National Public Data declaró bancarrota tras la filtración de 2,9 mil millones de registros. El año anterior, Rackspace tuvo que cerrar su servicio de correo electrónico debido a un ataque de ransomware.

Este escenario crítico está alineado con la creciente preocupación de las empresas: según el informe Hiscox Cyber Readiness Report, contar con un Plan de Continuidad de Negocios es esencial para mantener la resiliencia organizacional frente a condiciones adversas.

La elaboración de este plan exige mapear sistemas críticos y evaluar la dependencia de terceros o proveedores, que también pueden ser blancos de ataques. Herramientas como el Threat Hunting de Axur, que cuenta con una base de datos de más de 42 mil millones de credenciales, son una opción para mapear riesgos asociados a plataformas y sistemas externos.

35% de las organizaciones considera los ciberataques como uno de los cinco mayores riesgos para su negocio.

Combata al phishing con monitoreo y takedown

El phishing, como ataque basado en ingeniería social, rara vez enfrenta barreras técnicas para adaptarse a nuevos entornos y paradigmas de trabajo. Es una amenaza que afecta a clientes, proveedores y empleados.

Entender cómo el phishing impacta en el negocio trae grandes beneficios, ya que el combate a esta amenaza, especialmente a través de un takedown ágil y efectivo, tiende a reducir la exposición de la marca en una amplia gama de fraudes digitales. Las credenciales e información robadas mediante phishing representan un riesgo significativo para las redes corporativas, y la falta de visibilidad sobre esta amenaza puede complicar la gestión de identidades.

Cultura de seguridad

Las normas son poco efectivas si las personas no entienden su valor. La "TI invisible" causada por el aprovisionamiento irregular de sistemas y los errores en la gestión de identidades, como mantener activas las credenciales de empleados desvinculados, son señales comunes de que la cultura de seguridad de una empresa necesita mejoras.

Es más fácil implementar políticas de seguridad exitosas cuando los empleados y los tomadores de decisiones son conscientes de los riesgos y comprenden la importancia de seguir las directrices establecidas. Esta cultura puede fortalecerse mediante programas de concienciación en seguridad.

9 avances de la IA que están redefiniendo la detección y respuesta a amenazas

1 Sistemas autónomos de seguridad: Operaciones sin intervención humana.

→ La IA crea sistemas que detectan amenazas y corrigen vulnerabilidades en tiempo real.

2 Análisis conductuales mejorados: Monitoreo continuo y aprendizaje.

→ La IA identifica anomalías basándose en patrones de comportamiento, aumentando su precisión con el tiempo.

3 Inteligencia de amenazas predictiva: Predicción de amenazas futuras.

→ Algoritmos predicen ataques emergentes utilizando datos históricos, lo que permite defensas proactivas.

4 Automatización y análisis de datos: Caza de amenazas eficiente.

→ La IA automatiza el análisis de registros y eventos, permitiendo a los equipos enfocarse en investigaciones complejas.

5 Detección avanzada de anomalías: Identificación de patrones sofisticados.

→ El deep learning detecta amenazas desconocidas o complejas que los métodos tradicionales no pueden identificar.

6 Integración de NLP: Interacciones intuitivas.

→ La IA facilita consultas en lenguaje natural, haciendo más accesible el análisis de amenazas.

7 Respuesta rápida a incidentes: Mitigación automatizada.

→ La IA reduce los tiempos de respuesta, conteniendo incidentes rápidamente para minimizar daños.

8 Colaboración con intercambio de inteligencia: Defensa colectiva.

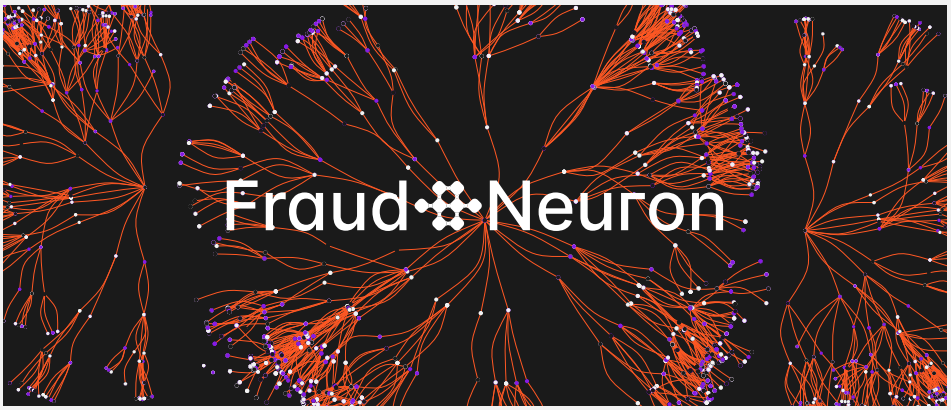
→ Los sistemas de IA comparten inteligencia en tiempo real, fortaleciendo la seguridad global.

9 Enfoque en amenazas emergentes: Identificación proactiva.

→ La IA rastrea señales de amenazas en plataformas como redes sociales y foros en la dark web.

Fraud Neuron

Framework para la gestión de fraudes



Para generar inteligencia de amenazas cibernéticas, estas deben ser descritas, modeladas y categorizadas.

El framework ATT&CK, creado y gestionado por la MITRE Corporation, es la metodología más reconocida para esta tarea, al describir un número creciente de Tácticas, Técnicas y Procedimientos (TTPs) utilizados por los agentes maliciosos.

Este framework funciona como un lenguaje común que los profesionales de ciberseguridad emplean para sintetizar y comprender rápidamente las acciones de un atacante, destacando la información esencial que un equipo de defensa necesita para detectar o prevenir una amenaza.

Para formar parte del framework, cada técnica se cataloga de manera individual. De esta forma, ATT&CK se convierte prácticamente en una base de datos de inteligencia sobre las estrategias usadas por los atacantes.

Fraud Neuron (F.N.), desarrollado por Axur, tiene como objetivo cumplir un papel similar en el campo de los fraudes digitales, facilitando el intercambio de información y creando un lenguaje común para los profesionales del área.

Un framework de ciberseguridad alineado con el negocio

A través de la categorización de tácticas específicas de fraudes y sus impactos en el negocio, incluidos activos intangibles como la marca, la reputación y el riesgo legal, Fraud Neuron complementa otras metodologías de modelado y ofrece una perspectiva innovadora para comprender el cibercrimen.

Los fraudes en canales digitales combinan elementos comunes de los ataques cibernéticos con atributos específicos del sector en el que opera la empresa, como el comercio electrónico o los servicios financieros. Al describir cómo ocurren estas combinaciones, Fraud Neuron reduce la distancia entre los equipos de ciberseguridad y los de prevención de fraudes, promoviendo una colaboración más efectiva.

Esta visión es especialmente valiosa para el mercado latinoamericano, donde la conexión entre los fraudes digitales y las técnicas de ataque cibernético es particularmente fuerte.

Disponible para la comunidad

Fraud Neuron ha sido desarrollado con base en la experiencia de Axur en la lucha contra los fraudes digitales y se encuentra abierto para su uso por parte de toda la comunidad de ciberseguridad. Este enfoque abierto facilita la adopción amplia, eliminando barreras para el intercambio de información y permitiendo que Fraud Neuron se consolide como un lenguaje común entre los profesionales para describir los incidentes.

En los canales del proyecto, profesionales de cualquier organización pueden enviar sugerencias de mejora o nuevas tácticas que puedan incorporarse al modelo.

El modelado y categorización de fraudes también puede emplearse para recopilar información sobre distintos grupos criminales, realizar análisis cuantitativos (como identificar las técnicas más comunes) y servir como una base de datos de los métodos utilizados por los delincuentes.

La inteligencia generada con la metodología de Fraud Neuron puede ser utilizada para priorizar la mitigación, desarrollar campañas de concientización y preparar a las organizaciones para los fraudes que afectan a cada sector en particular.

Contribuya a Fraud Neuron

github.com/axur/FraudNeuron

Pilares principales de Fraud Neuron

→ Identificación del objetivo
Tipo de objetivo (individuo u organización)

→ Temática
Categoría general de la fraude, incluyendo elementos de ingeniería social

→ Reconocimiento
Técnicas utilizadas para recopilar datos de las víctimas

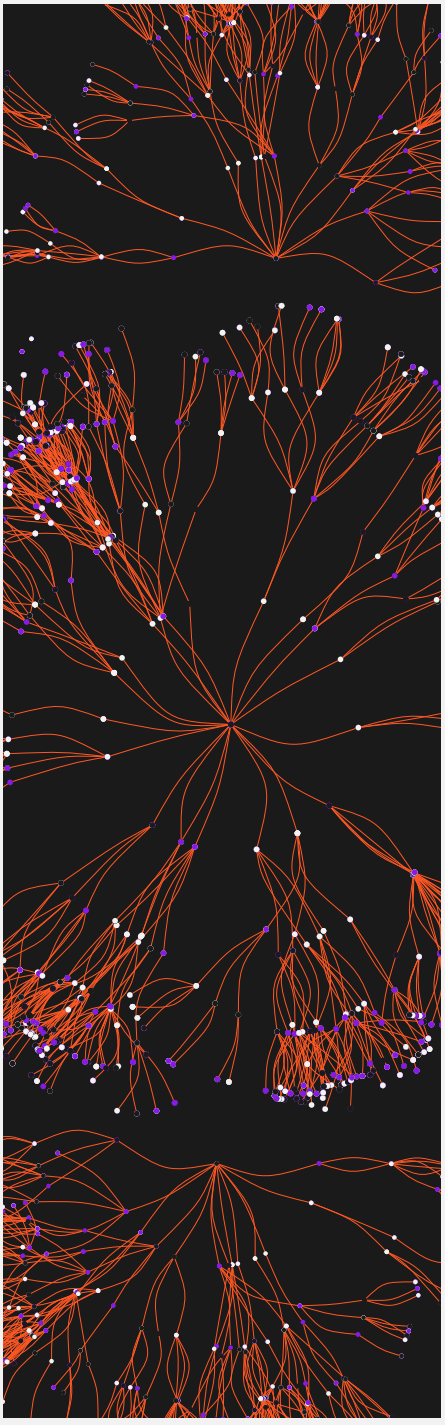
→ Recursos
Medios de comunicación, técnicas y herramientas que conforman la infraestructura digital del ataque

→ Susplantación de identidad
Tipos de identidades utilizadas indebidamente, incluyendo marcas, empleados y aplicaciones

→ Ingeniería social
Detalle de cómo se aplicó la ingeniería social en el contexto de la temática

→ Conversión
Técnicas empleadas para convertir el ataque en beneficios financieros u otros fines ilícitos

→ Impacto
Impactos asociados al fraude, tanto en la infraestructura de TI como en el negocio



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.

Lo que dicen los equipos de seguridad

Gartner Peer Insights™ 5/5

★★★★★

Explorando la poderosa alianza con Axur

Axur es nuestra alianza, ¡la mejor! Si necesito ayuda o tengo alguna pregunta, los contacto y siempre me asisten.

Gerente de TI y Riesgos

★★★★★

Consola intuitiva para una configuración eficiente de alertas

Velocidad para identificar amenazas y reportarlas al cliente, con implementación fácil y rápida.

Gerente de Tecnología

Descubra cómo nuestras soluciones pueden mejorar su estrategia de seguridad

Agende una demo

///AXUR

Experiencias digitales más seguras

Descubra nuestras soluciones en www.axur.com