Top 8 Fraudes detectados por Ironchip

La Inteligencia de localización como barrera ante la industrialización del cibercrimen

IRONCHIP
CYBERSECURITY

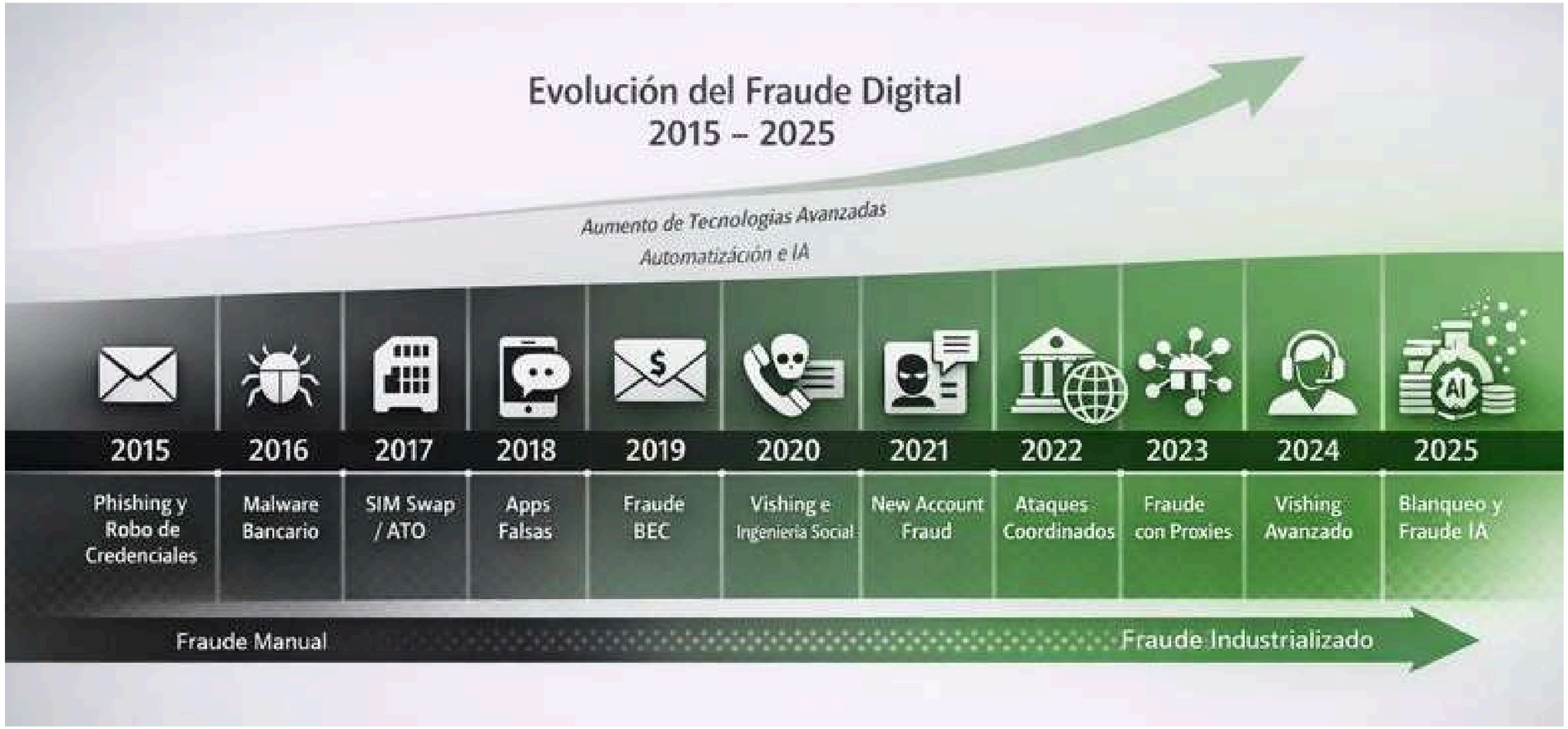
Índice

El fraude de identidad en entornos empresariales ya no responde a escenarios excepcionales ni a ataques aislados. En muchos casos, se produce a partir de accesos legítimos, procesos secundarios poco protegidos y flujos que quedan fuera del foco habitual de supervisión.

Cuando estos elementos se combinan, el fraude puede desarrollarse de forma gradual, sin levantar alertas inmediatas y aprovechando la confianza implícita de los sistemas.

En los casos analizados, esta dinámica se repite con frecuencia.

Evolución del Fraude Digital 2015 -2025



Hallazgos claves 2025

En 2025, el fraude digital ha alcanzado un punto de madurez industrial. Ya no se manifiesta como incidentes aislados, sino como operaciones coordinadas, automatizadas y altamente sofisticadas, capaces de eludir los controles tradicionales basados únicamente en identidad. Estos hallazgos reflejan un cambio estructural en la naturaleza del cibercrimen y evidencian la necesidad de adoptar modelos de seguridad que integren contexto, ubicación real y comportamiento como ejes centrales de protección.

"Desde el 2025, el fraude ya no se detecta por señales aisladas, sino por la coherencia entre quién actúa, desde dónde lo hace y cómo se comporta", Julen Martínez, CEO de Ironchip.

Ubicación + Comportamiento como barrera más efectiva

Industrialización del fraude digital

Las mafias operan desde infraestructuras centralizadas, lanzando accesos simultáneos contra múltiples entidades con identidades aparentemente válidas.

Fraude autorizado (vishing) donde el consentimiento es inducido.

El consentimiento del usuario deja de ser una garantía de legitimidad., convirtiendo al vishing en uno de los fraudes más costosos y difíciles de detectar

New Account Fraud mediante identidades sintéticas.

Lavado de capitales a través de cuentas mula y operativas transfronterizas.

Resumen Ejecutivo

La nueva era de la ciberresiliencia: cuando la identidad no es suficiente

La dependencia digital ya no es una opción: es la columna vertebral de la economía global. Desde infraestructuras críticas como el agua y la energía, hasta la administración pública y el sector privado, la operatividad reside íntegramente en activos digitales. Sin embargo, esta hiperconectividad ha generado una vulnerabilidad sistémica: la falsa sensación de seguridad.

Hoy, muchas organizaciones creen erróneamente que validar la identidad del usuario mediante biometría o contraseñas garantiza la seguridad. Este es uno de los errores más costosos de la década. La evolución del cibercrimen, potenciada por Inteligencia Artificial capaz de clonar identidades a escala, ha demostrado que las murallas tradicionales ya no bastan.

El atacante de 2025 no derriba la puerta: utiliza la llave correcta. Gracias a la IA, el fraude se vuelve indetectable para los sistemas tradicionales, permitiendo suplantaciones perfectas. Un fallo en la validación deja expuestos los activos más sensibles y puede desencadenar un efecto dominó a nivel organizativo.

En este informe, Ironchip demuestra por qué la ciberseguridad debe evolucionar: no basta con saber quién es el usuario, sino dónde y cómo interactúa. El análisis contextual y de comportamiento se convierte en la última barrera efectiva contra el fraude avanzado.

Elementos comunes en los casos analizados

El fraude de identidad en entornos empresariales ya no responde a escenarios excepcionales ni a ataques aislados. En muchos casos, se produce a partir de accesos legítimos, procesos secundarios poco protegidos y flujos que quedan fuera del foco habitual de supervisión.

Cuando estos elementos se combinan, el fraude puede desarrollarse de forma gradual, sin levantar alertas inmediatas y aprovechando la confianza implícita de los sistemas.

En los casos analizados, esta dinámica se repite con frecuencia.

8

casos reales analizados a partir de incidentes detectados

100%

entornos empresariales en operación real

Elementos comunes en los casos analizados

El fraude de identidad en entornos empresariales ya no responde a escenarios excepcionales ni a ataques aislados. En muchos casos, se produce a partir de accesos legítimos, procesos secundarios poco protegidos y flujos que quedan fuera del foco habitual de supervisión.

Cuando estos elementos se combinan, el fraude puede desarrollarse de forma gradual, sin levantar alertas inmediatas y aprovechando la confianza implícita de los sistemas.

En los casos analizados, esta dinámica se repite con frecuencia.

El fraude de identidad en entornos empresariales ya no responde a escenarios excepcionales ni a ataques aislados. En muchos casos, se produce a partir de accesos legítimos, procesos secundarios poco protegidos y flujos que quedan fuera del foco habitual de supervisión.

Cuando estos elementos se combinan, el fraude puede desarrollarse de forma gradual, sin levantar alertas inmediatas y aprovechando la confianza implícita de los sistemas.

En los casos analizados, esta dinámica se repite con frecuencia.

El fraude de identidad en entornos empresariales

En muchos casos, se produce a partir de accesos legítimos, procesos secundarios poco protegidos y flujos que quedan fuera del foco habitual de supervisión.

Cuando estos elementos se combinan, el fraude puede desarrollarse de forma gradual, sin levantar alertas inmediatas y aprovechando la confianza implícita de los sistemas.

La tecnología de Ironchip

Frente a la sofisticación de las mafias, Ironchip propone un cambio de paradigma: la validación de la "Zona Segura".

A diferencia de los sistemas tradicionales que confían en el GPS (vulnerable a spoofing), la tecnología de Ironchip analiza el espectro invisible que rodea al usuario. Mediante Inteligencia Artificial, analizamos las ondas electromagnéticas de una ubicación específica (Wi-Fi, Bluetooth, torres de telefonía, señales de radio) para crear una firma única de ubicación no replicable.

Esto nos permite:

Validar el entorno físico

Saber si el dispositivo está realmente donde dice estar.

Analizar el hardware

Detectar si la tarjeta SIM, el operador o el dispositivo han sido manipulados para enmascarar su origen.

Aprender hábitos

Entender cuáles son las zonas de confianza del usuario para reducir la fricción en accesos legítimos y bloquear anomalías.

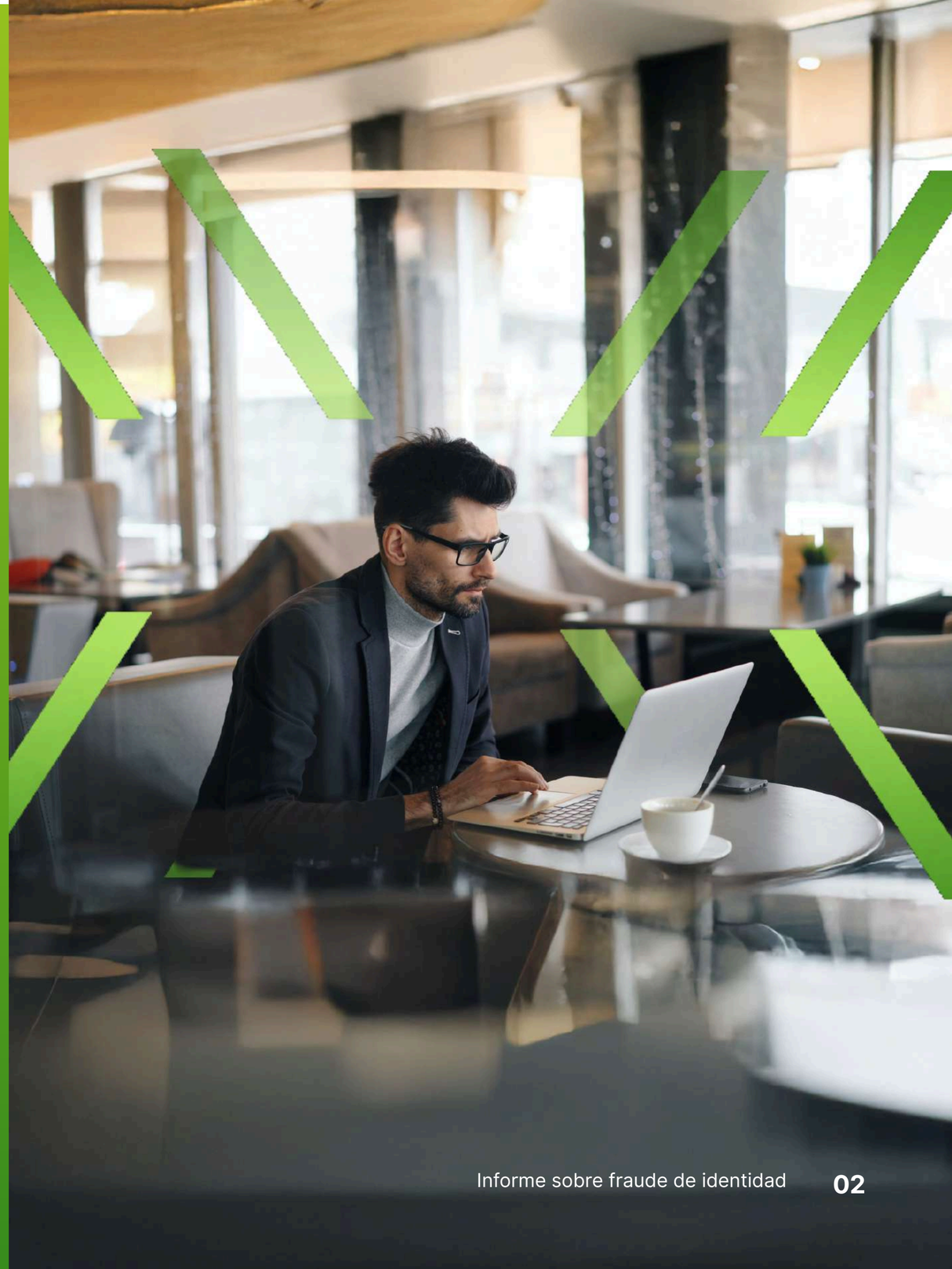
Falsificación de entornos y dispositivos

Técnicas más peligrosas de fraude

Los atacantes ya no se limitan a usar un "Fake GPS" básico. Han industrializado la ofuscación. Su objetivo es presentar al banco un dispositivo "limpio" y una conexión "residencial" legítima, cuando en realidad operan desde granjas de bots o redes anónimas.

Para lograrlo, combinan cuatro técnicas avanzadas:

IRONCHIP CYBERSECURITY



Cuatro técnicas avanzadas

Redes de anonimización (TOR & VPNs): Enmascaran la IP real para ocultar el origen (países sancionados o centros de fraude).

Proxies residenciales: El vector más peligroso. Alquilan IPs de usuarios reales (a menudo infectados por malware) para que la conexión parezca venir de un hogar legítimo, mostrando una ciudad específica: Ejemplo Madrid, Barcelona, burlando las listas negras de IPs tradicionales.

Dispositivos Comprometidos (Root/Jailbreak): Rompen la seguridad del sistema operativo para obtener privilegios de administrador, lo que les permite instalar herramientas de ataque (como Frida o Magisk) y ocultarlas de la app bancaria.

App Tampering: Modifican o "inyectan" código en la propia aplicación de la entidad para interceptar datos o alterar su funcionamiento lógico.

Nuestra plataforma de detección funciona como capaz de detección profunda, que se van retroalimentando del propio comportamiento del usuario, según las reglas aplicadas en cada caso: Con una detección no binaria, al desición se toma tras un análisis multicapa que desmonta la anomalía del atacante paso a paso:

Mapeo de ondas y coordenadas GPS

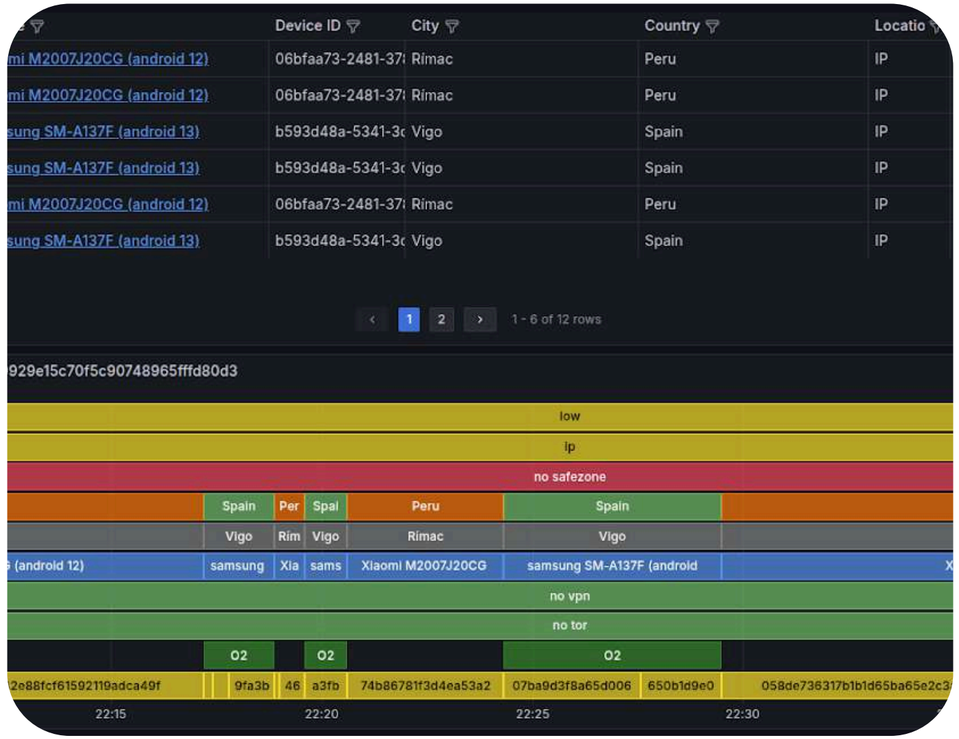
No confiamos en la coordenada que entrega el sistema operativo (que puede estar inyectada por software). Ironchip escanea el espectro electromagnético real que rodea al dispositivo (Wi-Fi, Bluetooth, Torres de telefonía).

El caso del Proxy Residencial: Aunque la IP diga que el usuario está en una casa en Valencia (porque usa un proxy residencial de alta calidad), si nuestro escáner de ondas no detecta las redes Wi-Fi vecinas coherentes con esa zona geográfica, o detecta un entorno de "vacío espectral", bloqueamos el acceso. La IP miente; las ondas no.

Análisis de Integridad del Dispositivo (Root & Hooking Detection)

Realizamos un chequeo forense del entorno de ejecución. Buscamos binarios sueltos, permisos inusuales o rastros de herramientas de ocultación (Magisk Hide, emuladores avanzados).

Tampering: En este caso Detectamos si la aplicación ha sido reempaquetada o si hay hooks activos intentando modificar la memoria del proceso en tiempo real. Si el dispositivo no es "íntegro", no es confiable.



Detección de Redes Anónimas (TOR/VPN)

Identificamos si la conexión de salida coincide con nodos de salida conocidos de la red TOR o rangos de IPs de datacenters asociados a VPNs comerciales.

En este caso, cruzamos este dato con la velocidad de movimiento. Si un usuario salta de una IP residencial a un nodo TOR en segundos, se marca como comportamiento evasivo.

Los atacantes utilizan aplicaciones de Fake GPS, VPNs y Proxies para simular que se encuentran en una zona habitual del usuario legítimo, eludiendo las alertas de seguridad tradicionales.

Ataques coordinados desde infraestructuras centralizadas

En 2025, el fraude digital ha dejado de ser una actividad aislada para convertirse en una operación industrializada. Las mafias de cibercrimen operan desde infraestructuras centralizadas, que son, literalmente, oficinas de fraude, granjas de dispositivos o centros de control, desde las que lanzan ataques masivos y simultáneos contra múltiples entidades financieras, plataformas digitales o grupos de usuarios.

El resultado es un entorno donde cada banco o empresa ve solo “su parte” del ataque, mientras la organización criminal actúa de forma transversal y sincronizada.

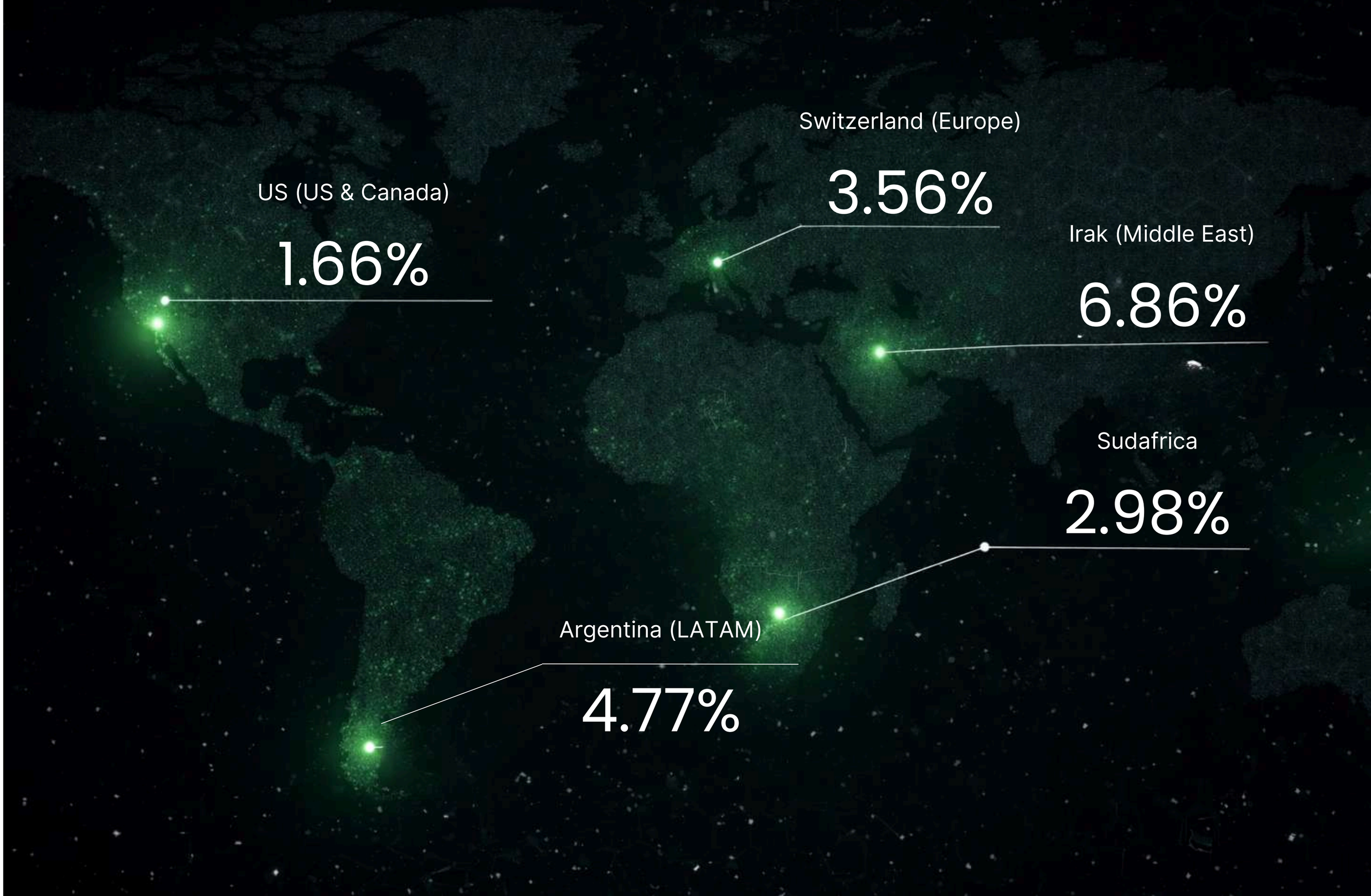
1 Alta simultaneidad de conexiones hacia distintos objetivos.

2 Uso de identidades digitales aparentemente legítimas, robadas o suplantadas.

3 Dificultad de detección con sistemas tradicionales, que analizan el fraude de forma aislada por entidad y no como un fenómeno coordinado.

La solución Ironchip: inteligencia colectiva y respuesta geográfica en tiempo real

Ironchip introduce un enfoque de inteligencia colectiva aplicada a la identidad digital, capaz de detectar y neutralizar operaciones criminales completas, no solo intentos individuales de fraude.


US (US & Canada)
1.66%
Switzerland (Europe)
3.56%
Irak (Middle East)
6.86%
Sudafrica
2.98%
Argentina (LATAM)
4.77%

Detección de picos coordinados

Los algoritmos de Ironchip analizan patrones globales de autenticación y acceso, identificando:

- Picos anómalos de conexiones simultáneas.
- Coincidencias geográficas precisas desde las que se originan accesos hacia múltiples organizaciones o usuarios.
- Comportamientos imposibles para usuarios legítimos (velocidad, simultaneidad, repetición).

Este análisis permite elevar el fraude de evento aislado a patrón criminal organizado.

Identificación de zonas de ataque

Cuando se confirma un patrón coordinado, Ironchip define automáticamente una **“zona de ataque”**, que puede corresponder a:

- Un edificio concreto.
- Un polígono industrial.
- Una localización urbana específica.
- Infraestructuras de fraude conocidas o emergentes.

Esta capacidad transforma la localización en un **atributo de seguridad activo**, no meramente contextual.

Bloqueo geográfico automático y desmantelamiento operativo

Una vez identificada la zona de ataque, Ironchip permite:

- Bloquear en tiempo real todas las conexiones provenientes de esa área geográfica concreta.

- Interrumpir simultáneamente los ataques contra todas las entidades protegidas.

- Neutralizar la operación de la mafia en su punto de origen, no solo mitigar sus efectos.

El impacto es inmediato: la infraestructura criminal queda inutilizada, obligando a los atacantes a reconstruir toda su operación, con un coste elevado y pérdida de efectividad.

Valor estratégico: de la prevención individual a la defensa colectiva

Este enfoque convierte a Ironchip en un sistema de defensa colaborativa frente al cibercrimen organizado:
Cuantos más entornos protegidos, mayor capacidad de detección global.

Las mafias pierden su principal ventaja: la coordinación invisible entre víctimas.

El fraude deja de ser reactivo y pasa a ser proactivamente desmantelado.

Viajes Imposibles

Este es uno de los casos más ”obvios”, pero sigue entrando en nuestro ranking como los más populares. Podemos verlo cuando un usuario accede a su cuenta desde Madrid y, minutos después, se registra un acceso desde Tokio. Aunque las credenciales sean correctas, el desplazamiento físico es inviable.

Con una tecnología de detección avanzada, que además analiza el comportamiento podemos calcular el desplazamiento con estos elementos:

Elementos

Lógica espacio-temporal

Calculamos la viabilidad del desplazamiento basándonos en el tiempo transcurrido entre conexiones.

Evidencia Forense

Generamos un registro de auditoría con marcas de tiempo y ubicación precisas que sirve como prueba judicial para demostrar que el usuario no pudo haber realizado esa operación.

Elementos

Análisis de la SIM (MCC/MNC)

Leemos los códigos internos de la tarjeta SIM (Mobile Country Code) para revelar el verdadero país de origen de la conexión, independientemente de lo que diga la IP o el GPS.

Triangulación de antenas

Verificamos la coherencia entre la antena de telefonía a la que está conectado el móvil y su supuesta ubicación.

Robo de cuenta sin GPS. Localización del ciberdelincuente

El fraude que todos conocemos. El atacante desactiva el GPS o usa emuladores avanzados para ocultar su país de origen, intentando parecer un usuario local. Sin embargo, con nuestro análisis podemos aplicar estos dos principios que nos permiten determinar la localización real.

Vishing y fraude autorizado

Cuando el consentimiento ya no es prueba de legitimidad

El vishing se ha consolidado como una de las formas de fraude más efectivas en 2025 porque explota el eslabón más vulnerable del sistema de seguridad: el comportamiento humano bajo presión. Indetectable por muchas otras herramientas de detección del fraude.

En este tipo de ataque:

- El usuario recibe una llamada de un supuesto gestor bancario o agente de seguridad.
- El atacante genera un escenario de urgencia (bloqueo de cuenta, fraude en curso, verificación inmediata).

El usuario autoriza conscientemente una transacción o acción crítica, creyendo que está protegiendo su cuenta.

Vishing y fraude autorizado

Desde el punto de vista de los sistemas tradicionales:

- La identidad es correcta.
- El dispositivo es legítimo.
- El consentimiento existe.

Sin embargo, el consentimiento ha sido forzado mediante ingeniería social, lo que invalida su valor como señal de seguridad.

Detección de coerción contextual, no solo identidad y Correlación avanzada de señales de riesgo

Cuando el consentimiento ya no es prueba de legitimidad

El vishing se ha consolidado como una de las formas de fraude más efectivas en 2025 porque explota el eslabón más vulnerable del sistema de seguridad: el comportamiento humano bajo presión. Indetectable por muchas otras herramientas de detección del fraude.

En este tipo de ataque:

- El usuario recibe una llamada de un supuesto gestor bancario o agente de seguridad.
- El atacante genera un escenario de urgencia (bloqueo de cuenta, fraude en curso, verificación inmediata).

El usuario autoriza conscientemente una transacción o acción crítica, creyendo que está protegiendo su cuenta.

Detección de coerción contextual, no solo identidad

Ironchip aborda el vishing desde una premisa clave: No todo consentimiento es voluntario, y el contexto en el que se produce una acción es tan importante como la autenticación en sí.

1. Detección de llamada activa en el momento crítico
La tecnología de Ironchip es capaz de identificar si, en el instante exacto de una transacción sensible, el usuario:

- **Mantiene una llamada de voz activa.** Sea por red GSM tradicional o por VoIP (WhatsApp, Telegram u otras aplicaciones).

Este dato contextual es crítico, porque el vishing siempre requiere una interacción en tiempo real entre atacante y víctima durante la ejecución del fraude.

Correlación avanzada de señales de riesgo

Ironchip no toma decisiones basadas en un único indicador, sino en la correlación simultánea de múltiples señales:

- Llamada activa → posible canal de coerción.
- Transacción de alto valor o acción crítica → objetivo típico del fraude.
- Usuario fuera de su zona geográfica habitual → ruptura de patrón de comportamiento.
- (Opcional) Cambio de dispositivo, horario anómalo o repetición de intentos.

Cuando estas señales coinciden, el sistema identifica un escenario de alto riesgo de fraude autorizado por coerción.

Reinterpretación del consentimiento

En este contexto, Ironchip introduce un cambio de paradigma:

- El consentimiento explícito no se considera suficiente si el contexto indica coerción.
- La transacción se re-clasifica como potencialmente fraudulenta, aunque haya sido iniciada por el propio usuario.

Esto permite a la institución financiera analizar la transacción y determinar si le interesa bloquear o pausar la operación, activar un segundo canal de verificación fuera de la llamada, generar alertas específicas para los equipos antifraude.

Los sistemas antifraude tradicionales analizan: Credenciales, dispositivo, firma de comportamiento histórico.

Ironchip añade una capa crítica:

- Contexto humano en tiempo real.

- Detección de coacción activa, no solo de suplantación.

Esto convierte a Ironchip en una herramienta clave contra el Vishing, fraude del “gestor falso”, estafas con consentimiento inducido.

Ayudamos a reducir el impacto de este tipo de fraude en nuestros clientes, quienes como consecuencia, obtienen una reducción drástica del fraude autorizado, uno de los más costosos y difíciles de gestionar.

- Mejora de la protección del cliente sin responsabilizarle del ataque. Manteniendo la imagen corporativa de la banca fortalecida.
-
- Alineación con marcos regulatorios que exigen protección efectiva incluso ante ingeniería social (DORA, PSD3,entre otras).

Lavado de capitales y redes de cuentas mula

El lavado de capitales en 2025 se apoya cada vez más en infraestructuras digitales organizadas, donde los ciberdelincuentes:

- Utilizan cuentas de usuarios legítimos (mulas conscientes o inconscientes).
- Crean redes de cuentas distribuidas en distintas entidades financieras.
- Gestionan estas cuentas de forma centralizada desde uno o muy pocos dispositivos físicos.
- Canalizan fondos hacia paraísos fiscales o jurisdicciones incluidas en listas de alto riesgo del GAFI.

1 Transacciones de forma individual.

2 Riesgo por cuenta, no por infraestructura operativa.

Detección de redes de mulas

Identificar **clusters de cuentas** aparentemente independientes.

Demostrar que están siendo controladas desde la **misma infraestructura física.**

Elevar automáticamente **el riesgo AML** de todas las cuentas vinculadas al dispositivo.

Equipos de prevención

Esto aporta una evidencia clave para que los equipos de prevención de blanqueo, puedan realizar sus investigaciones internas y su posterior reportes regulatorios y SAR/STR.

Control de operativas internacionales de alto riesgo

Accesos desde o hacia **paraísos fiscales**

Jurisdicciones incluidas en **listas GAFI.**

Cambios frecuentes de **cuentas destino**.

Señal de riesgo

Ironchip refuerza la señal de riesgo, permitiendo identificar estructuras de lavado transfronterizo, priorizando los casos de alto impacto económico y reputacional.

Listas negras de dispositivos: neutralización definitiva

El dispositivo físico se incorpora a una **lista negra**.

Se bloquea su **acceso futuro**, incluso si: Cambian las cuentas y se crean nuevas identidades.

Se reutiliza el terminal en otras entidades protegidas por Ironchip

Esto impide la reincidencia, uno de los mayores problemas en redes de mulas.

En 2025, el lavado de capitales ya no se combate solo siguiendo el dinero, sino **identificando y desmantelando** las infraestructuras que lo mueven. Ironchip permite hacerlo desde el origen.

New Account Fraud y identidades sintéticas

El New Account Fraud, especialmente a través de identidades sintéticas, representa uno de los mayores retos en 2025 para banca y servicios financieros. En estos escenarios:

- Se crean cuentas nuevas utilizando datos falsos, combinados o robados.
- No existe historial previo de comportamiento que permita detectar anomalías clásicas.
- El proceso de KYC se convierte en el principal punto de decisión… y también en el principal punto de ataque.

Los defraudadores saben que, una vez superado el KYC inicial, disponen de una ventana de tiempo crítica para operar antes de que los sistemas detecten incoherencias.

En este caso, la herramienta aplica sus recursos avanzados para validar la identidad desde la coherencia, no desde el histórico

Cruce de información KYC con localización real

Durante el proceso de alta, el usuario proporciona múltiples datos: Dirección declarada, país o región de residencia, contexto personal o profesional.

Ironchip contrasta esta información con: La localización real de la conexión inicial, el tipo de entorno desde el que se produce el acceso.

Esto permite identificar incoherencias tempranas, como: Altas que declaran residencia local pero se originan desde centros de datos, hosting o infraestructuras cloud y patrones típicos de bots o granjas de creación de cuentas.

Este análisis no invalida automáticamente la cuenta, pero eleva el nivel de riesgo desde el KYC.

Evaluación del entorno técnico inicial

Más allá de la geografía, Ironchip analiza si la conexión procede de un entorno residencial realista, o de infraestructuras comúnmente utilizadas para fraude automatizado. Este punto es clave en identidades sintéticas, donde: Los datos pueden parecer válidos, pero el entorno técnico delata una creación industrializada de cuentas.

Consistencia temprana: aprendizaje desde el minuto cero

Ironchip no necesita semanas de datos para aprender. Desde las primeras horas:

- Aprende el patrón inicial de ubicación y dispositivo.
- Establece una línea base mínima de coherencia.

Si una cuenta recién creada:

- Cambia drásticamente de ubicación en sus primeras horas o días.
- Alterna dispositivos de forma anómala.
- Presenta saltos geográficos incompatibles con un comportamiento legítimo.

Se marca automáticamente como cuenta de alto riesgo, incluso aunque todas las credenciales sean correctas.

Consistencia temprana: aprendizaje desde el minuto cero

- Reducción del fraude en las primeras fases del ciclo de vida del cliente.
- Mejora del KYC sin fricción adicional para el usuario legítimo.
- Identificación temprana de cuentas destinadas a fraude, mulas o blanqueo.
- Alineación con exigencias regulatorias de diligencia reforzada desde el onboarding.

En 2025, el fraude ya no se detecta esperando a que ocurra un comportamiento anómalo, sino validando desde el inicio que la identidad es coherente con su realidad técnica.
Ironchip permite hacer ese cruce de forma automática, continua y fiable.

Detección específica de identidades sintéticas

Este enfoque permite identificar identidades sintéticas porque:

- No pueden mantener coherencia entre lo declarado y lo ejecutado.
- Operan con rapidez para monetizar antes de ser detectadas.
- Reutilizan infraestructuras técnicas entre múltiples altas.

Ironchip convierte esa debilidad operativa en una señal antifraude estructural.

Account Takeover (ATO)

Leyenda. En esta imagen podemos observar cómo un mismo dispositivo intenta acceder desde dos ubicaciones distintas. En el reporte detalla todo el análisis y sus resultados.

El Account Takeover ocurre cuando un atacante roba las credenciales de un usuario y accede a su cuenta. Aunque la contraseña sea correcta, los sistemas tradicionales suelen permitir el ingreso sin cuestionarlo. Ironchip añade una capa de protección basada en comportamiento y contexto: analiza si el acceso se produce desde localizaciones habituales del usuario, como su casa u oficina, y detecta cualquier desviación significativa. Ante accesos desde zonas atípicas, el sistema aplica fricción dinámica, solicitando autenticación reforzada o bloqueando la operación hasta confirmar la identidad. Esto permite prevenir fraudes incluso cuando las credenciales son legítimas.

1 Validación de hábito: detección de accesos fuera de las zonas habituales.

2 Fricción dinámica: autenticación reforzada o bloqueo preventivo según riesgo.

El camino a seguir

En 2025, los ataques al sistema financiero ya no se limitan a usuarios aislados: son operaciones criminales industrializadas, coordinadas y potentes. Ironchip demuestra que la inteligencia de localización combinada con análisis de comportamiento permite:

- Detectar fraude antes de que se materialice, incluso cuando las credenciales son legítimas.
- Prevenir vishing, fraude de identidad, lavado de capitales y ataques coordinados desde infraestructuras criminales.
- Transformar la protección de cada usuario en una defensa colectiva, aumentando la resiliencia de toda la organización.
- La seguridad del futuro requiere no sólo saber “quién” es el usuario, sino “dónde” y “desde qué dispositivo” opera. Ironchip convierte esta información en un activo estratégico que protege a los clientes, reduce el riesgo operativo y cumple con los estándares regulatorios más exigentes.

IRONCHIP

CYBERSECURITY