Plataforma de deteccion de fraude

Mitigación del fraude digital mediante inteligencia avanzada y localización en tiempo real

IRONCHIP
CYBERSECURITY

© 2026 Ironchip Cybersecurity. All rights reserved.

Índice

¿Quiénes somos?

Ironchip es una compañía global de ciberseguridad **líder en la protección de la identidad y detección de fraudes**.

Utilizamos una tecnología única basada en Location Intelligence que permite validar la identidad del usuario, proporcionando visibilidad, trazabilidad y control en tiempo real sobre cada acceso.

De este modo, garantizamos una **seguridad 360°**, conectando el mundo físico con la protección digital y asegurando el acceso de empleados, clientes y terceros de forma continua, eficaz y sin fricción.

IRONCHIP
CYBERSECURITY

Ciberseguridad en nuestro ADN

En Ironchip, la seguridad no es solo una palabra: es nuestro **compromiso**. Por eso, contamos con certificaciones como LINCE del Centro Criptológico Nacional (cpstic.ccn.cni.es).

Nuestras soluciones han sido certificadas con nivel ALTO e incluidas en el Catálogo de Productos de Seguridad del **CCN-CERT**, lo que respalda su uso en entornos críticos. Además, contamos con procedimientos de empleo seguro definidos para escenarios de alta seguridad (ccn-cert.cni.es).

El **Gobierno de España avala a la compañía** mediante su inversión, convirtiéndonos en una empresa clave estratégica a nivel nacional.

IRONCHIP
CYBERSECURITY

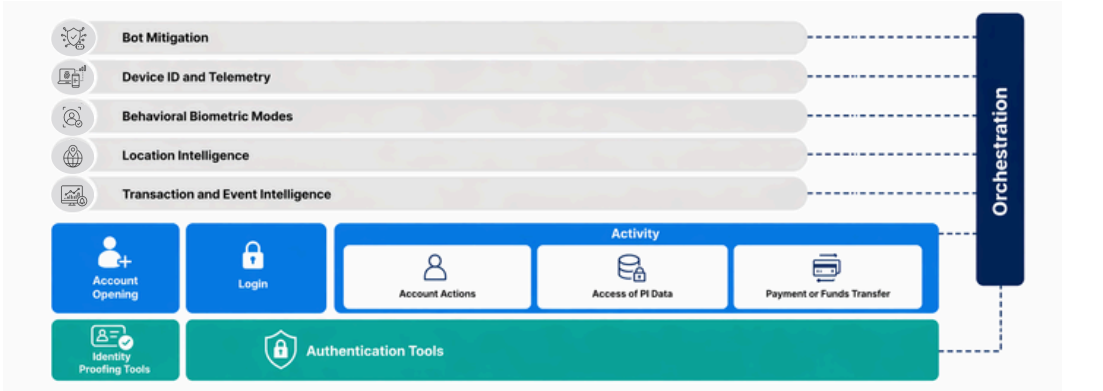
Tecnología

IRONCHIP
CYBERSECURITY

Localizacion inteligente - Localización precisa como prueba de identidad

Alcance de las capacidades de Online Fraud Detection a lo largo de un recorrido digital típico del cliente.

Gartner



Source: Gartner
755906_C

IRONCHIP
CYBERSECURITY

Tecnología de detección basada en localización

Zonas de operaciones habituales

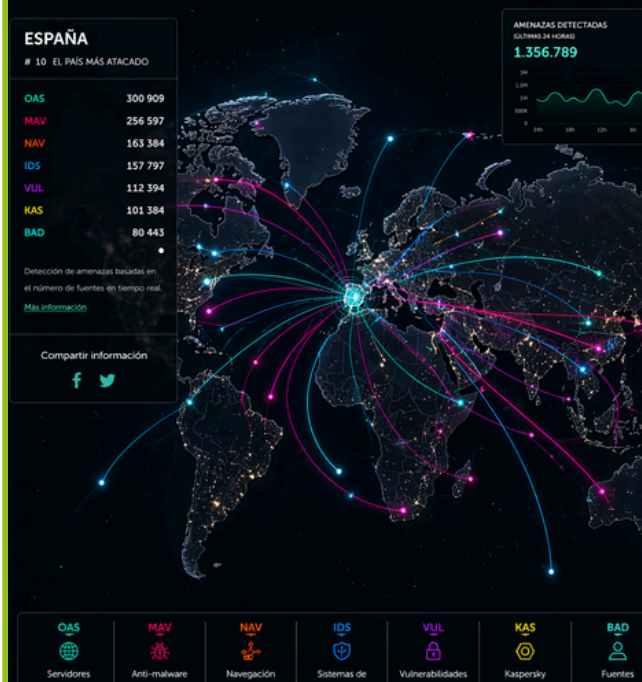
La mayoría de los procesos de identidad tienen lugar en ubicaciones confiables.

Ubicación No Confiable

El 92% de los ataques ocurren de forma remota, desde una ubicación en la que el usuario nunca ha estado.

El 99% de los estafadores cometen fraude desde la misma ubicación al menos en dos ocasiones.

IRONCHIP CYBERSECURITY



La localización por operaciones - Tipos de transacciones protegidas

IRONCHIP
CYBERSECURITY

Zonas seguras o habituales

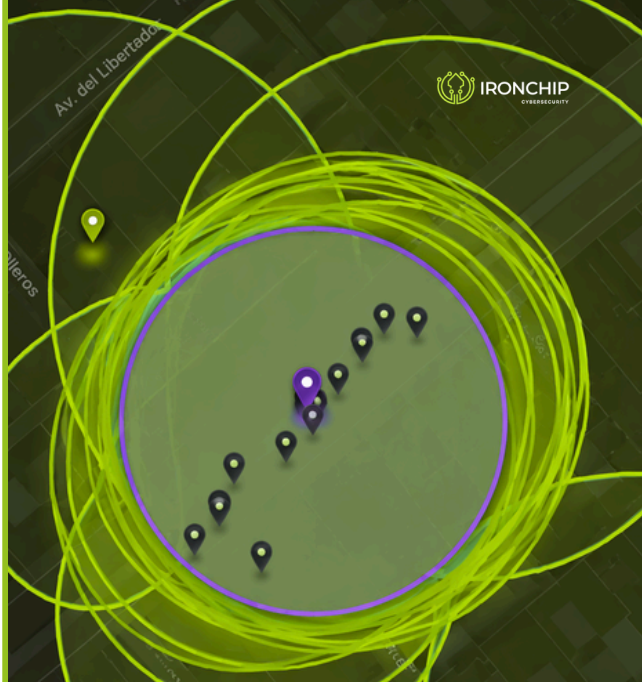
¿Qué es una Zona Segura?

Una zona segura es un lugar único, habitual e infalsificable para cada usuario.

¿Cómo se genera una zona segura?

Una zona segura se genera usando IA, tras captar y analizar las siguientes señales cada vez que un usuario opera en una aplicación móvil o web:

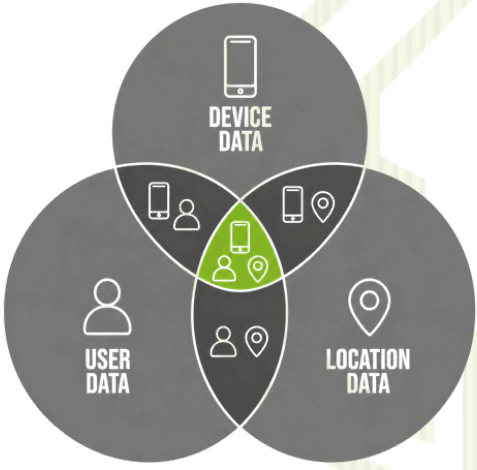
- Señales móviles: 2G, 3G, 4G o 5G.
- Señales WiFi alrededor y WiFi favorito.
- GPS e IP.
- Geolocalización basada en latencias.
- ISP contratado y conexión a antenas móviles.
- SIM nativa en uso.
- Suplantaciones de localización vía red VPN y TOR.



Localización en el comportamiento

Nuestra tecnología vincula de forma única el dispositivo con su ubicación real mediante inteligencia artificial y señales ambientales (WiFi y redes móviles).

Este enfoque nos permite **modelar patrones de comportamiento precisos**, esenciales para la identidad segura del futuro. La capacidad de entender dónde está el usuario y cómo interactúa con sus recursos ofrece un control sin precedentes, convirtiéndose en el estándar definitivo para la seguridad y autenticación en sistemas digitales.



IRONCHIP
CYBERSECURITY

Plataforma de **detección de fraudes**

IRONCHIP
CYBERSECURITY

Comportamientos anómalos: comportamientos fraudulentos detectados

IRONCHIP
CYBERSECURITY

Instalación
SDK & API

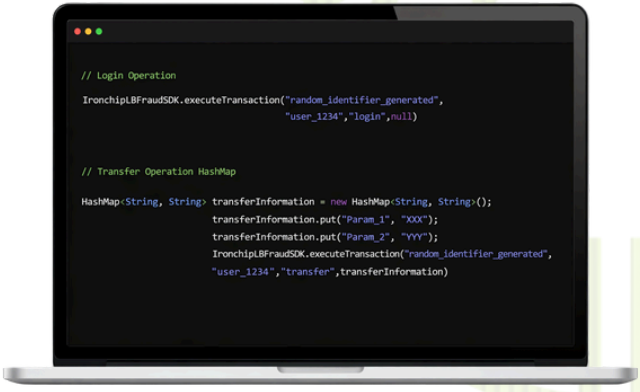
Datasource SDK

Una librería iOS/Android/JavaScript que puede integrarse en cualquier aplicación móvil o web para capturar la información necesaria.

Fraud Detection API

Una API HTTP para solicitar resultados, integrables con cualquier BPM o SIEM.

Documentación



IRONCHIP
CYBERSECURITY

Operaciones a proteger

IRONCHIP
CYBERSECURITY

Motor de reglas de seguridad avanzada

Reglas de ubicación de riesgo

- Ubicaciones de origen en países GAFI.
- Conexión por red TOR o VPN.
- Si la geolocalización RF no coincide con GPS o SIM.
- Existencia de proxy residencial.
- ISP de alto riesgo o en lista negra.
- Suplantación de ubicación (spoofing).
- El carrier de la SIM difiere de la ubicación o del origen del ISP.
- Viajes imposibles.
- Red WiFi pública (high).
- Red WiFi privada.
- Ubicaciones asociadas a ataques confirmados en otras entidades.
- IP en lista negra o de riesgo.

Reglas de dispositivo de riesgo

- Software malicioso instalado.
- Proceso de depuración o debugging activo.
- Dispositivo marcado en lista negra.
- Dispositivo de riesgo (ALPS, TECNO, INFINIX, Fairphone, Nothing, MobiWire).
- Dispositivo con root o jailbreak.
- Desactualización del dispositivo en el historial de actualizaciones.
- Roaming inesperado.

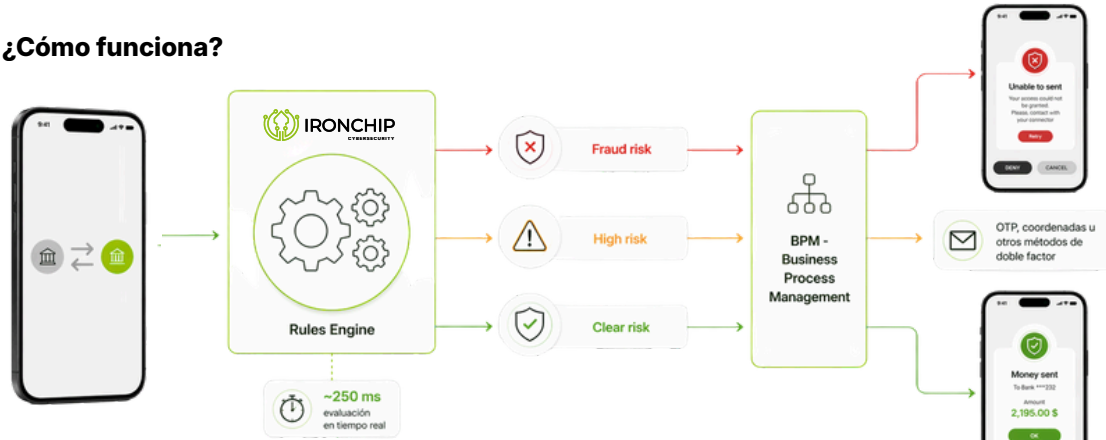
Reglas de comportamiento

- Roaming + SIM virtual.
- Cambio de idioma sin cambio de dispositivo ni ubicación habitual.
- Transferencia en llamada o en redirección activa.
- Dispositivo asociado a más de 3 usuarios.
- Idiomas en cirílico desde ubicaciones de no uso.
- Múltiples conexiones en ventanas temporales pequeñas.
- Patrones consistentes con campañas de ataque conocidas.

Gracias a la combinación inteligente de variables, **nuestro motor de reglas establece políticas de comportamiento ultra-precisas y adaptadas a cada escenario**

IRONCHIP
CYBERSECURITY

¿Cómo funciona?



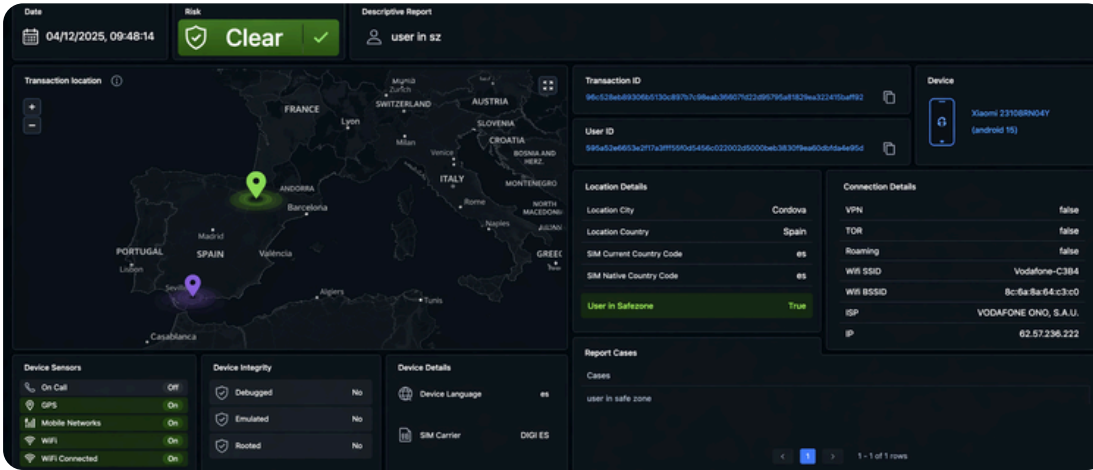
Fraud risk
Acciones preventivas y bloqueo inmediato

High risk
Verificación adicional y doble factor

Clear risk
Operación permitida sin fricción

IRONCHIP
CYBERSECURITY

Comportamiento normal y seguro



Comportamiento anómalo - Money mule

Uso repentino de VPN

El 12 de septiembre se observó por primera vez una conexión a través de una VPN, específicamente NordVPN. Esto supone una desviación significativa del comportamiento habitual del usuario.

Cambio de SIM Carrier

El dispositivo pasó de estar conectado en España a otra ubicación, también reportada como España, pero con una tarjeta SIM de origen en Benín. Esto fue posible mediante un cambio de proveedor de servicios móviles, de DiGI (España) a MTN Benin.

Comportamiento anómalo - Money mule

Viaje imposible

En 5 minutos viajo de España a Benin. Un cambio de ubicación tan drástico en tan poco tiempo es logísticamente imposible sin el uso de herramientas tecnológicas para manipular la ubicación.

Cambio de ISP

Además, se identificó un cambio de proveedor de internet. El usuario pasó de estar conectado a través de Red Digital de Telecomunicaciones de las Islas Baleares S.L. (España) a conectarse a través de NordVPN, lo cual coincide con la aparición de la tarjeta SIM de Benín.

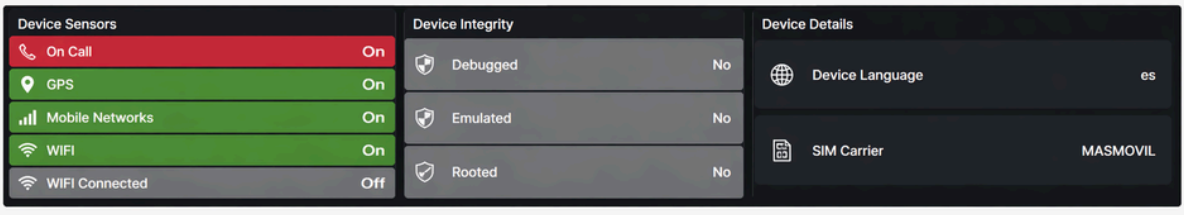
Comportamiento anómalo - Vishing para fraude autorizado

Detección de llamadas corrientes en operaciones de transacciones.

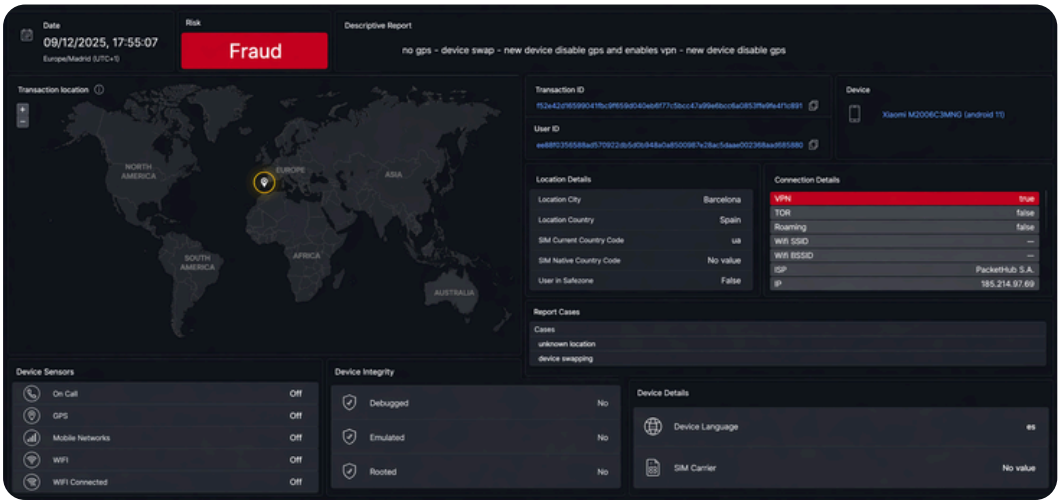
Detección de llamadas IP:

- Telegram, Discord, WhatsApp...

Redirección de llamadas y detección de Roaming



Comportamiento anómalo - Suplantación de ubicación o SIM virtuales



Antimalware con protección activa en tiempo real

Nuestro módulo Antimalware de nueva generación actúa como una capa de defensa activa durante la sesión. A diferencia de las soluciones estáticas, nuestra tecnología detecta en tiempo real indicadores de compromiso (IoC) como ataques de inyección, superposición de pantallas (overlays) y herramientas de acceso remoto no autorizadas. Esta vigilancia constante garantiza que el entorno donde se valida la identidad esté **libre de interferencias maliciosas, blindando la integridad de cada transacción**.

Overlay Attacks
Pantallas falsas superpuestas a la App real para robar credenciales. Robo de contraseñas y códigos 2FA.

Remote Access Trojans (RATs)
Herramientas de control remoto (AnyDesk, TeamViewer) ocultas o activas. Que un tercero realice la transacción en nombre del usuario.

Keyloggers
Scripts o apps que capturan cada pulsación de tecla del usuario. Captura de PINs, datos de tarjetas y claves privadas.

Sim Swapping / SMS Sniffers
Malware que intercepta los SMS de confirmación del banco. Autorizar transferencias sin que el usuario vea el código.

Inyección de código / Hooking
Manipulación de la memoria del navegador o app para alterar el destino de un pago.
Cambiar el IBAN del destinatario en el último segundo.

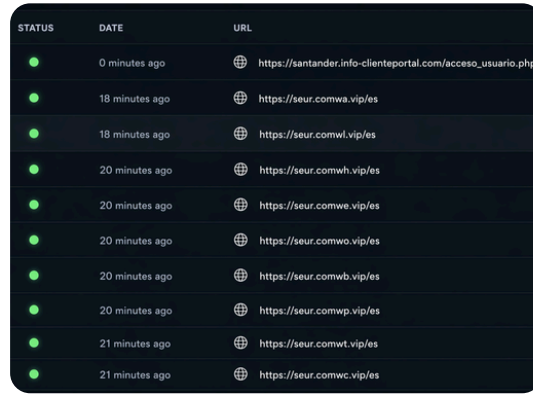
IRONCHIP
CYBERSECURITY

Módulo phishing/smishing - Scanning de sites maliciosos

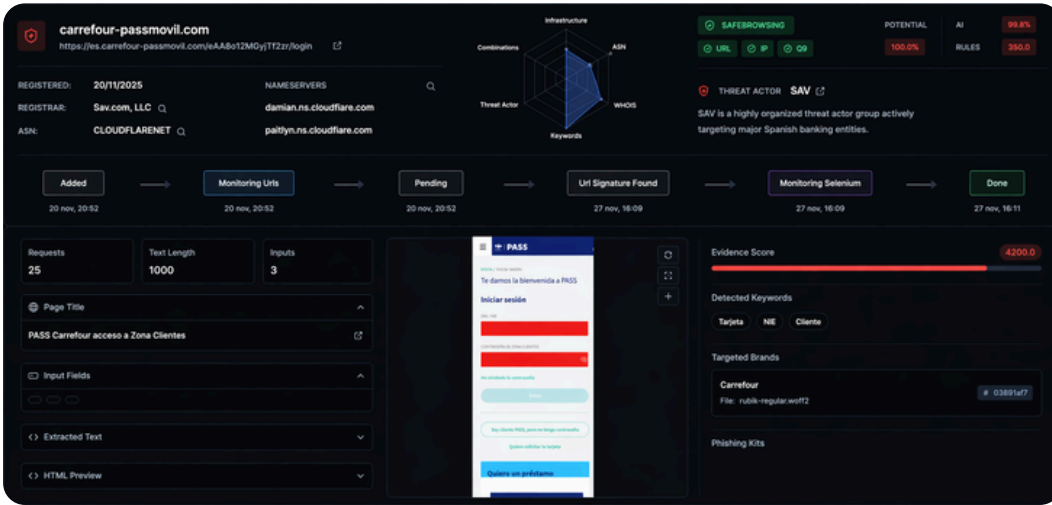
Nuestra **tecnología de detección de phishing** realiza un escaneo continuo de internet para identificar páginas que suplantan a entidades financieras. Cuando las localizamos, analizamos automáticamente sus vulnerabilidades, aprovechando que estas infraestructuras suelen ser débiles y poco seguras.

Cuando es posible, establecemos un sistema de monitorización que permite **capturar en tiempo real** la información que los atacantes intentan robar. Estos datos se notifican de inmediato a las entidades afectadas para bloquear accesos, restablecer credenciales y prevenir el fraude.

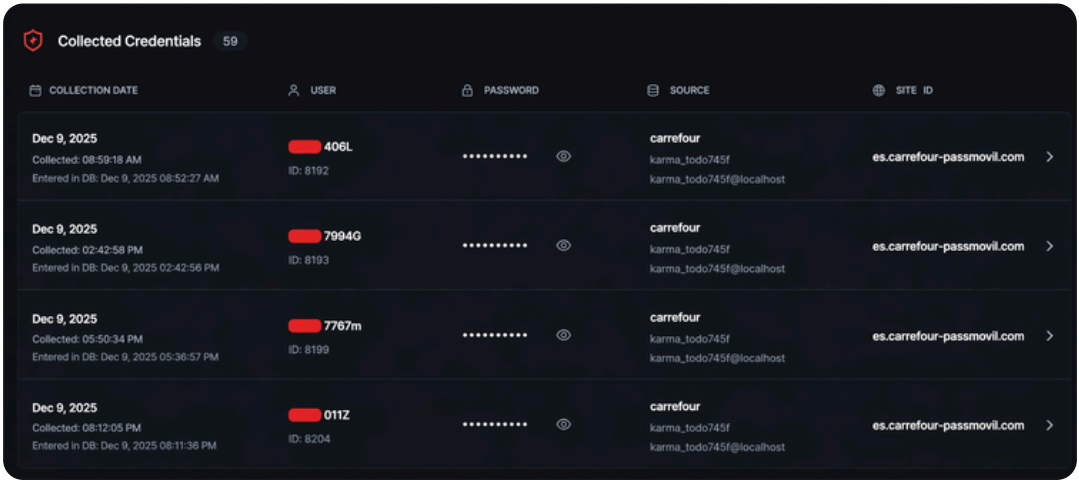
Además, detectamos tarjetas comprometidas y **rastreamos los canales** donde los delincuentes centralizan la información robada —incluidos bots de Telegram descubiertos a través de estas vulnerabilidades— para anticipar riesgos y reforzar la protección de los clientes financieros.



Módulo phishing/smishing - Perfiles de site



Módulo phishing/smishing - Análisis de credenciales y tarjetas



Caso de **éxito**

IRONCHIP
CYBERSECURITY

//ABANCA

Industria
Banca

Localidad
España

Tamaño
+ 8000 empleados

Detección de fraude bancario **avanzado en entornos digitales**

Detección de patrones asociados a fraude como money mule y SIM swapping mediante análisis continuo de comportamiento

RETO

Abanca se enfrentaba a la creciente complejidad del fraude bancario, con amenazas como money mule y SIM swapping difíciles de detectar mediante sistemas tradicionales. La falta de visibilidad sobre ubicación, dispositivo y comportamiento limitaba la identificación de anomalías en tiempo real. Esto dificultaba distinguir entre accesos legítimos y fraudulentos en operaciones críticas. Además, era necesario reforzar la seguridad sin afectar la experiencia del usuario.

SOLUCIÓN

Se implementó una solución basada en el análisis continuo del comportamiento del usuario, incorporando ubicación y dispositivo como factores de identidad, lo que permite detectar accesos anómalos y fraudes como SIM swapping sin afectar la experiencia del usuario.

IRONCHIP CYBERSECURITY

RESULTADOS

- Detección de múltiples casos de **fraude** como **money mule** y **SIM swapping**
- Identificación en tiempo real de accesos anómalos basados en comportamiento, ubicación y dispositivo
- Mayor capacidad para diferenciar entre usuarios legítimos y actividades fraudulentas

> Ironchip implementa su producto en un punto clave de la autenticación de manera sencilla, no costosa y combinada con una experiencia de usuario difícil de encontrar hoy en día.

– Fatima Cereijo, Gerente de Control de Fraude y Privacidad, Abanca

Confián en nosotros

Santander

CAIXAGUISSONA

Ibercaja

//ABANCA

arquia banca

kutxabank

IRONCHIP
CYBERSECURITY

IRONCHIP
CYBERSECURITY

Controla la identidad antes de que se convierta en un incidente.

IRONCHIP
CYBERSECURITY

IRONCHIP
Identity Security Platform

Beurko Viejo 1, Barakaldo
Paseo de la Castellana 200, Madrid

+34 944 075 954
www.ironchip.com

© 2026 Ironchip. Todos los derechos reservados. Ironchip y su logotipo son marcas registradas de Ironchip Telco S.L. El resto de marcas pertenecen a sus respectivos propietarios.