LIVE WEBINAR

IRONCHIP

PREVENCIÓN DEL FRAUDE BANCARIO CON INTELIGENCIA DE LOCALIZACIÓN

23 Oct, 2025
12.00 PM

SPEAKERS

JOSE FERNANDO GÓMEZ
Ciso
Ironchip

FRANCISCO SANTIBÁÑEZ
Gerente comercial
Seguridad América

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

La identidad es el nuevo perímetro...

Y es necesario dar cobertura a los nuevos ataques

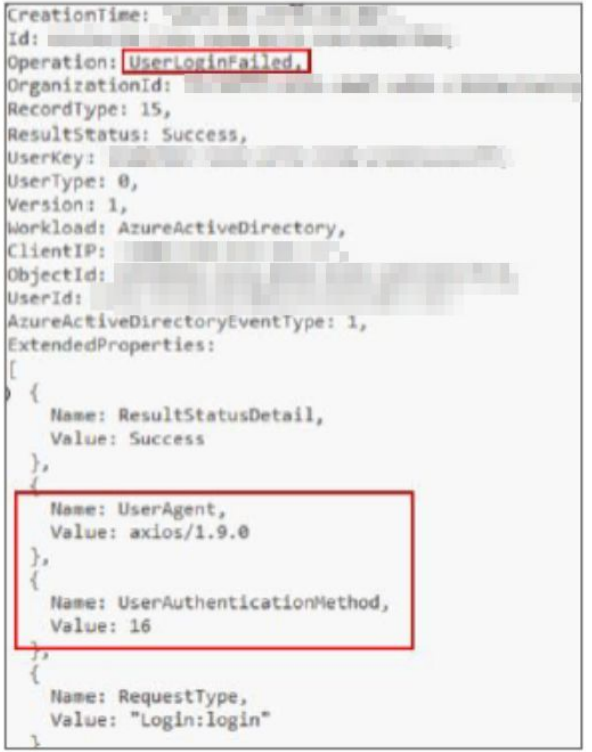
Dependencia de proveedores únicos de identidad:

¿Cuáles son las posibles consecuencias del ataque a Okta?

Los ciberdelincuentes del grupo Lapsus$ afirman haberse filtrado en Okta, un importante proveedor de sistemas de gestión de acceso. ¿Cuáles serán las consecuencias?

Nuevos ataques que se saltan el MFA:

Ataques reales detectados de robo de tokens:



```
CreationTime:
Id:
Operation: UserLoginFailed,
OrganizationId:
RecordType: 15,
ResultStatus: Success,
UserKey:
UserType: 0,
Version: 1,
Workload: AzureActiveDirectory,
ClientIP:
ObjectId:
UserId:
AzureActiveDirectoryEventType: 1,
ExtendedProperties:
[
  {
    Name: ResultStatusDetail,
    Value: Success
  },
  {
    Name: UserAgent,
    Value: axios/1.9.0
  },
  {
    Name: UserAuthenticationMethod,
    Value: 16
  },
  {
    Name: RequestType,
    Value: "Login:login"
  }
```

Tecnología de Detección basado en localización

Transacciones seguras por comportamiento

Zonas de operaciones habituales

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

Ubicación No Confiable

El **98%** 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 en dos ocasiones.

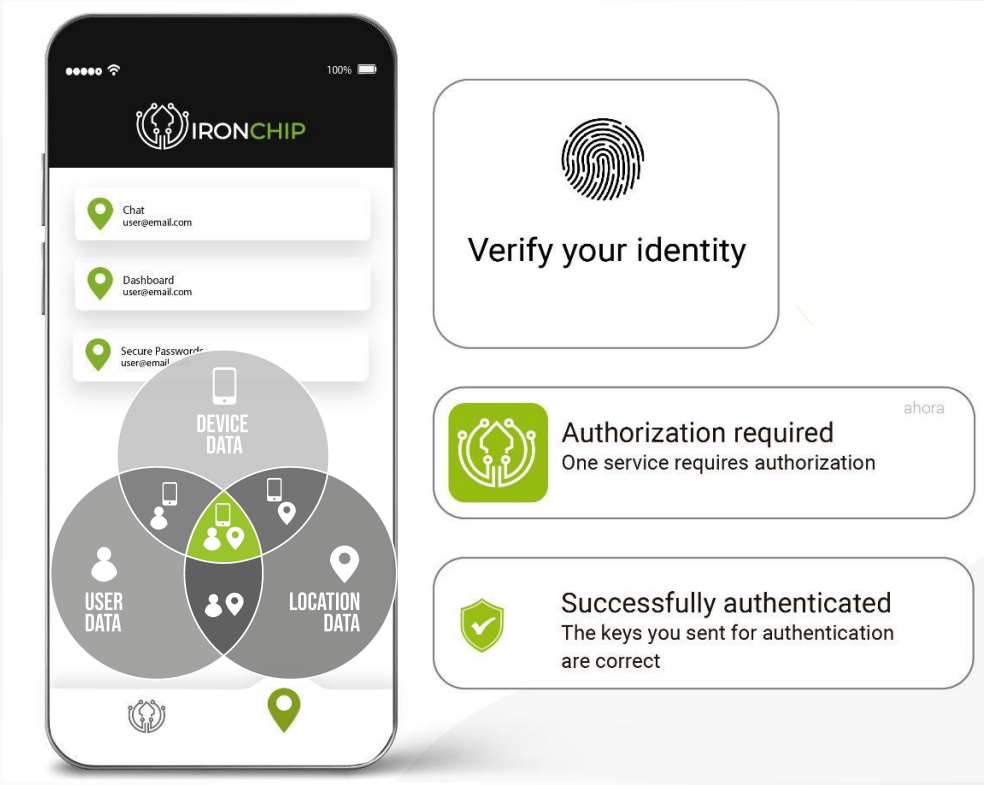
IRONCHIP

La solución definitiva contra los robos de identidad

Ironchip es una compañía de ciberseguridad global, especializada en protección de identidad digital y detección de fraude de nueva generación.

Con una **tecnología única en el mundo,** las soluciones de Ironchip ofrecen al cliente una **protección integral de la identidad** de todos sus servicios y recursos, así como también los de sus colaboradores.

Nuestra **tecnología de localización inteligente,** ofrece una trazabilidad, visibilidad y control en tiempo real de todos los usuarios, accesos y recursos, garantizando a las compañías una **seguridad 360.**



IRONCHIP

Tecnología y productos

www.ironchip.com

01 Usuarios y operaciones en una única solución

Tipos de transacciones protegidas

92% 

Registro de usuario

El 92% de los usuarios se registran en una aplicación desde lugares habituales

74% 

E-commerce

El 74% de las compras se realizan desde lugares habituales

68% 

Inicio de sesión

El 68% de los inicios de sesión se realizan desde lugares habituales

94% 

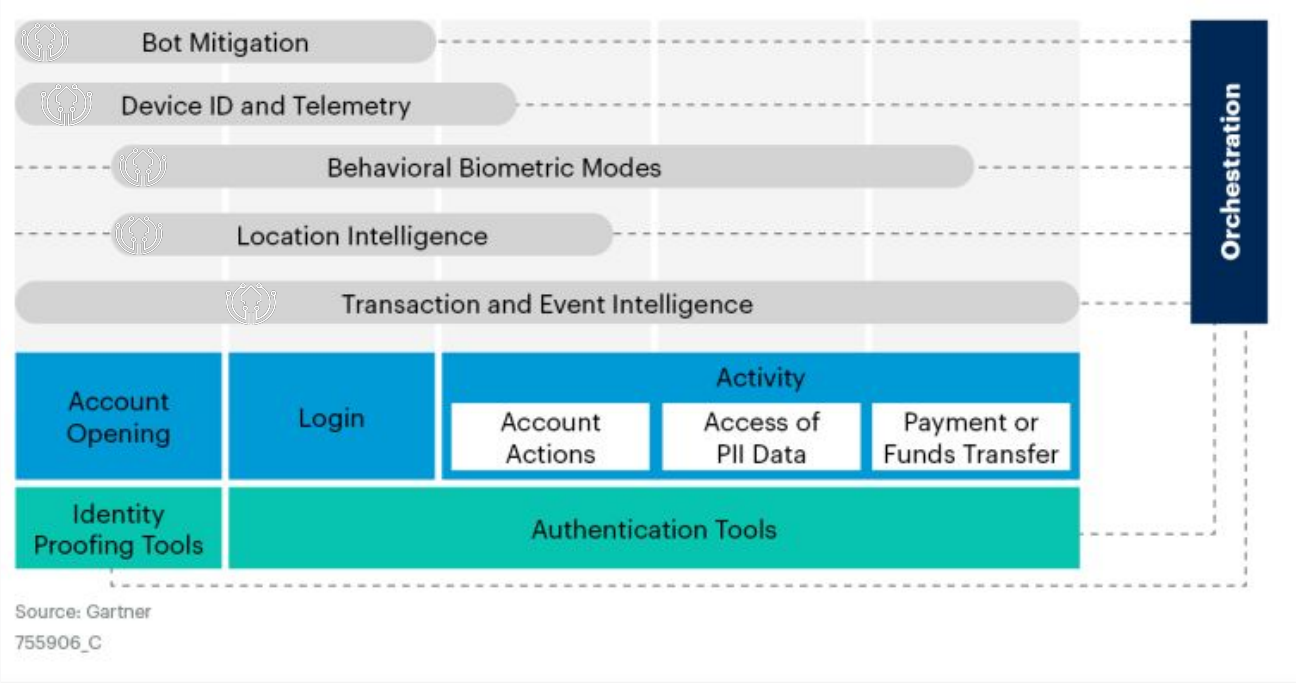
Transacciones +10.000€

Más del 95% de las transacciones de altos importes desde lugares habituales

Location intelligence

Location identity proof

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



¿Cómo funciona?

Transacciones seguras y localizadas

¿Que es una Zona Segura?

Una zona segura es un **lugar único, anónimo e infalsificable.**

¿Cómo se genera una zona segura?

Una zona segura se genera captando y analizando las ondas **2G, 3G, 4G, 5G, WIFIs y GPS** cada vez que un usuario opera una aplicación móvil o web.

Cada interacción enseña **a la IA propia de Ironchip** la relación entre los lugares en el tiempo, y esto permite utilizar esos relaciones lugar-dispositivo como parte de la identidad de cada usuario.

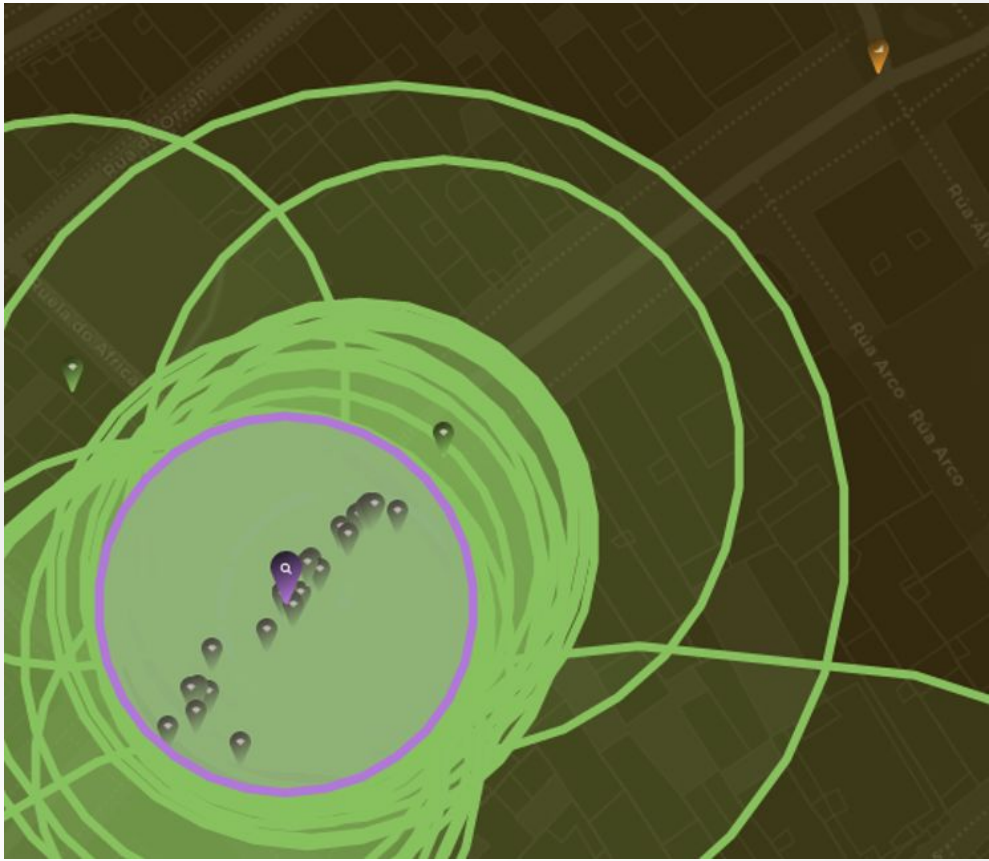


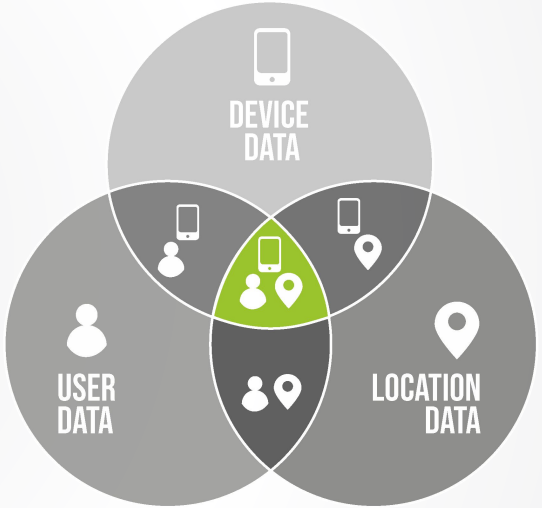
Image 1. Generated safe zone example with GPS, EM (2G, 3G, 4G, 5G) & IP signals.

Comportamiento de usuario

Localización en el comportamiento

La vinculación entre el lugar y el dispositivo que integramos en nuestra tecnología, junto con la inteligencia artificial de localización basada en señales de redes móviles y WIFIS, junto con los datos del usuario, es fundamental para la **generación de patrones de comportamiento**.

Esta combinación permite entender el comportamiento del usuario y su ubicación de manera precisa, lo que resulta indispensable para una identidad segura en el futuro. La capacidad de **comprender dónde se encuentra el usuario y cómo interactúa con sus dispositivos** es inigualable, y representa la clave para garantizar la seguridad y la autenticación en los sistemas digitales.



Tecnología de localización aplicada a la identidad digital

Nuestros productos de seguridad

IDENTITY PLATFORM

Servicios corporativos

- Empleados
- Partners
- ...

Multi-plataforma

FRAUD DETECTION

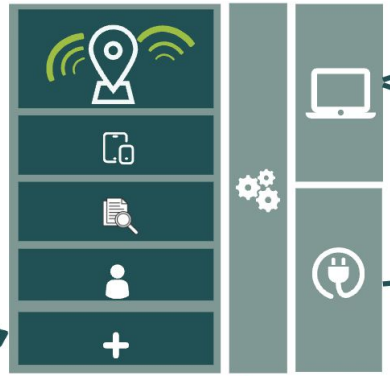
Banca digital

- Particulares
- Empresas
- ...

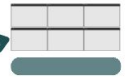
JS Web

SDK ios

SDK Android



Saas



Analistas Operadores

Administradores IT

Decisión automática / Analytics

- SIEM
- BPM
- TRANSACCIONAL
- ...

Usuarios | **Ironchip** | **Cliente**

Identity Platform

www.ironchip.com

Identity Platform

Modelo de madurez y seguridad de las soluciones de autenticación

El **Customer Authentication Strong and Maturity Model (CASMM) v2** es la versión actualizada del marco de referencia global que ayuda a las organizaciones a **evaluar la madurez de sus prácticas de autenticación**. Esta nueva versión se basa en la experiencia adquirida con la versión anterior e incorpora las últimas tendencias y mejores prácticas en materia de autenticación.

Ironchip Identity Platform consigue que las compañias se situen en el nivel 8 de este estandar, **evitando ataques de phising, malware, sim swapping, toma de cuenta y obtención de credenciales**.

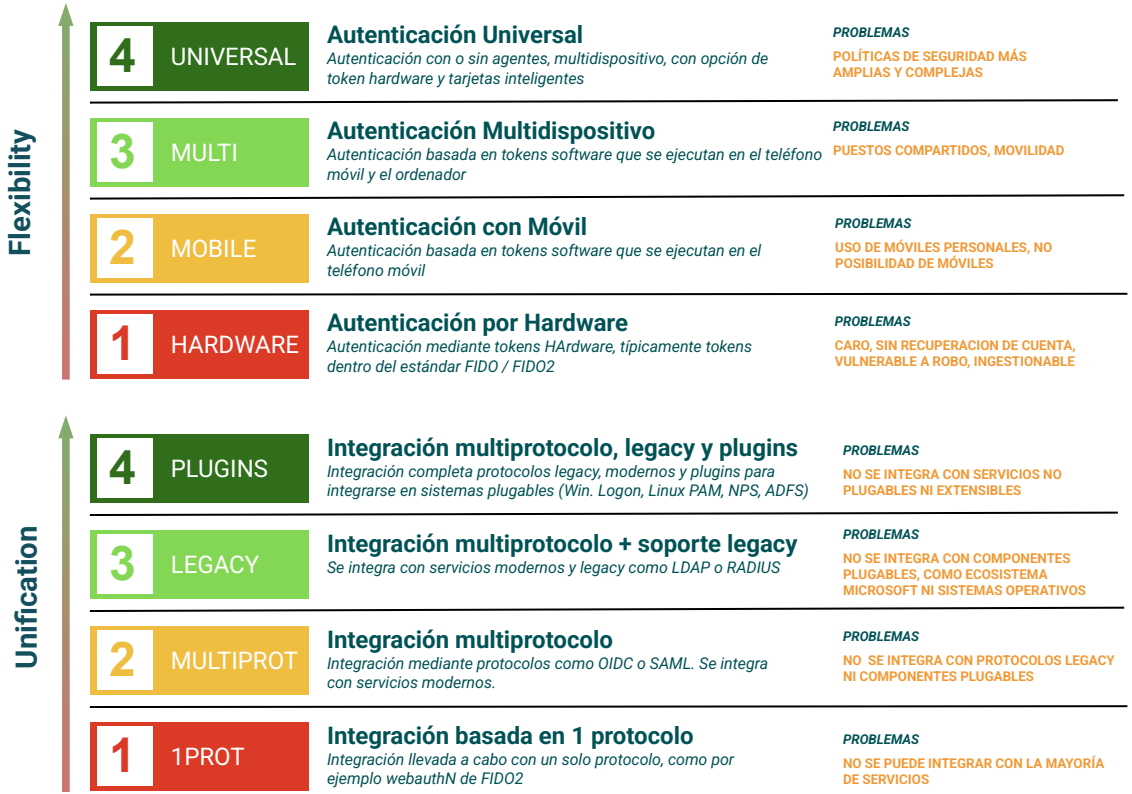
Además, nuestra plataforma de identidad mejora el dia a dia de los usuarios y los administradores, **reduciendo hasta en un 60% las incidencias relacionadas con la identidad**

8	PASSLESS	**Passwordless** *Además de las contraseñas gestionadas, tu 2FA proviene de un token físico o del centro de confianza integrado en tu móvil/escritorio.*	***VULNERABLE A:*** COMPROMISO DE HARDWARE, EXTORSIÓN
7	CODELESS	**2FA Sin Códigos Basados en Aplicaciones** *Además de las contraseñas gestionadas, tienes una aplicación 2FA que te pide que aceptes o rechaces un intento de autenticación.*	***VULNERABLE A:*** MALWARE, EXTORSIÓN
6	APP2FA	**Códigos 2FA Basados en Aplicaciones** *Además de contraseñas gestionadas, obtienes códigos MFA generados para ti por una aplicación a la que sólo tú puedes acceder.*	***VULNERABLE A:*** PHISHING, MALWARE
5	SMS2FA	**Códigos 2FA Basados en SMS** *Además de las contraseñas gestionadas, se le envían códigos MFA por mensaje de texto (SMS).*	***VULNERABLE A:*** PHISHING, SIM-SWAPPING
4	PASSMAN	**Gestor de Contraseñas** *Además de tener contraseñas únicas, también las almacena de forma segura en un archivo cifrado.*	***VULNERABLE A*** RESTABLECIMIENTO / TOMA DE CONTROL DE CUENTA
3	QUALPASS	**Contraseñas Cualificadas** *Tus contraseñas no sólo son únicas, sino que son largas, aleatorias e incluyen caracteres especiales.*	***VULNERABLE A:*** VOLCADO / DESCIFRADO DE CONTRASEÑAS
2	UNIQPASS	**Contraseñas Únicas** *Tus contraseñas son únicas, pero son demasiado cortas, simples o contienen información personal.*	***VULNERABLE A:*** ROBO DE CONTRASEÑAS EN DIRECTO
1	SHARPASS	**Contraseñas Compartidas** *Utilizas la misma contraseña en varios sitios de Internet.*	***VULNERABLE A:*** OBTENCIÓN DE CREDENCIALES

Identity Platform

Modelo de flexibilidad y unificación de las soluciones de autenticación

El **Customer Authentication Flexibility and Unification Model (CAFUM) v1** es la versión adaptada del marco de referencia global CASMM, con el que Ironchip ayuda a las organizaciones a **evaluar la escalabilidad de sus prácticas de autenticación**. Esta nueva versión se basa en la experiencia adquirida en los proyectos ejecutados con Ironchip

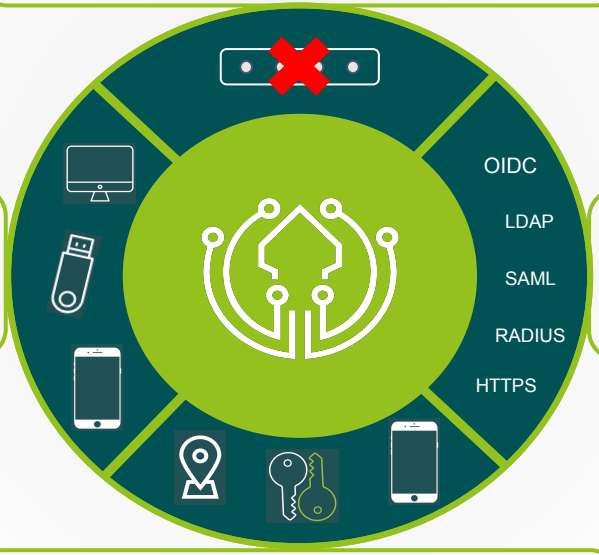


Identity Platform

Una experiencia unificada ligada a la excelencia

La experiencia más sencilla

Colocamos la experiencia del usuario en el núcleo de nuestro diseño, siendo capaces de sustituir el uso de contraseñas por factores más seguros y faciles de utilizar y administrar.



Flexibilidad sin limites

¿Tus empleados no tienen móvil corporativo? Ironchip funciona en android, iOS, Windows, Linux y Mac. Además, puedes reforzar tu seguridad con hardware tokens o dispositivos USB. O incluso autenticarte sin agentes

Identidad unificada

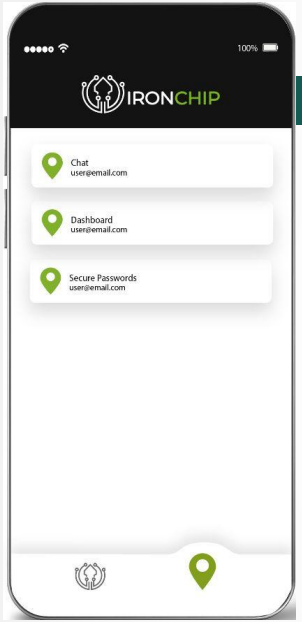
Nuestra plataforma se integra sin problemas con todas tus herramientas corporativas, centralizando la gestión de la identidad y asegurando la privacidad de tus datos.

Seguridad basada en riesgo

No almacenamos credenciales en nuestros servidores para garantizar la seguridad. Cero robos de cuenta gracias a detector de intrusos basado en dispositivo y ubicación

Identity Platform

La experiencia Passwordless más sencilla



Passwordless Authentication

Device Intelligence + Biometry + Hardware Keys

User experience

- **Effortless** 3 identity proofs 1 interaction
- **Secure:** Phising, Malware & Sim Swapping resistant
- **Passwordless** Without passwords, OTPs...

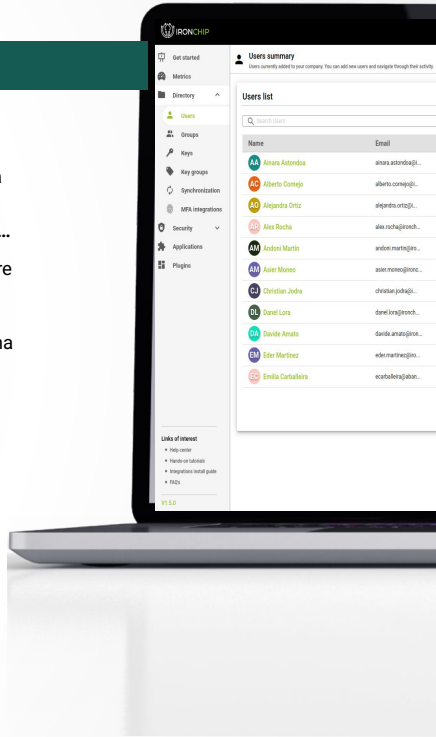
Easiest Management

Ciclo de vida de identidad

- **Altas, bajas, modificaciones e integraciones a golpe de click.**
- **Sin passwords, sin renovaciones, sin códigos...**
- **Sin puntos muertos.** Visibilidad completa sobre TODA tu identidad
- **Solucion multi-tenant:** Gestiona diferentes unidades organizativas y territoriales desde una única herramienta

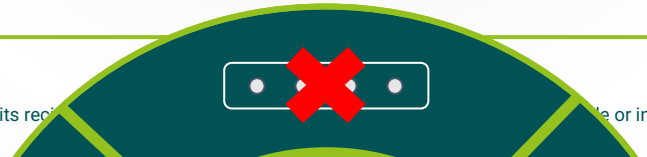
Datos, datos y más datos

- **Trazabilidad completa:** Todo lo que ocurra dentro de la herramienta queda registrado



La experiencia más sencilla

Colocamos la experiencia del usuario en el núcleo de nuestro diseño, siendo capaces de sustituir el uso de contraseñas por factores más seguros y faciles de utilizar y administrar.



Seguridad basada en riesgo

No almacenamos credenciales en nuestros servidores para garantizar la seguridad. Cero robos de cuenta gracias a detector de intrusos basado en dispositivo y ubicación

Zero Knowledge Proofs

Identidad soberana corporativa

- **Seguridad:** No almacenamos credenciales en nuestros servidores para garantizar la seguridad.
- **No más sustos innecesarios:** Sin posibilidad de ataques al proveedor de identidad.

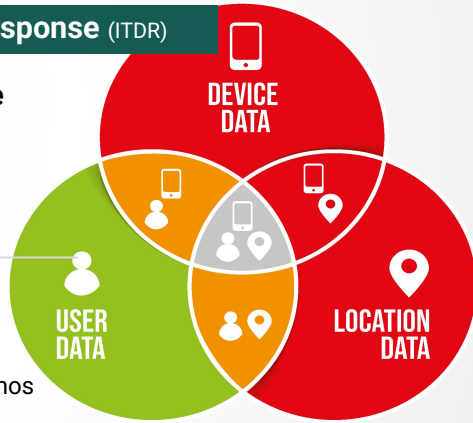
Cero robos de cuenta

- **Anti MITM:** Conexiones seguras imposibles de descifrar por un tercero
- **Anti Phishing:** La clave de acceso nunca abandona el dispositivo, impidiendo los ataques de Phishing

Identity Threat Detection & Response (ITDR)

Análisis de riesgo transparente

- **Detección de scams:** Detectamos ataques de ingeniería social como el vishing o la suplantación de identidad
- **Alertas en tiempo real:** Detecta y/o bloquea los ataques en tiempo real

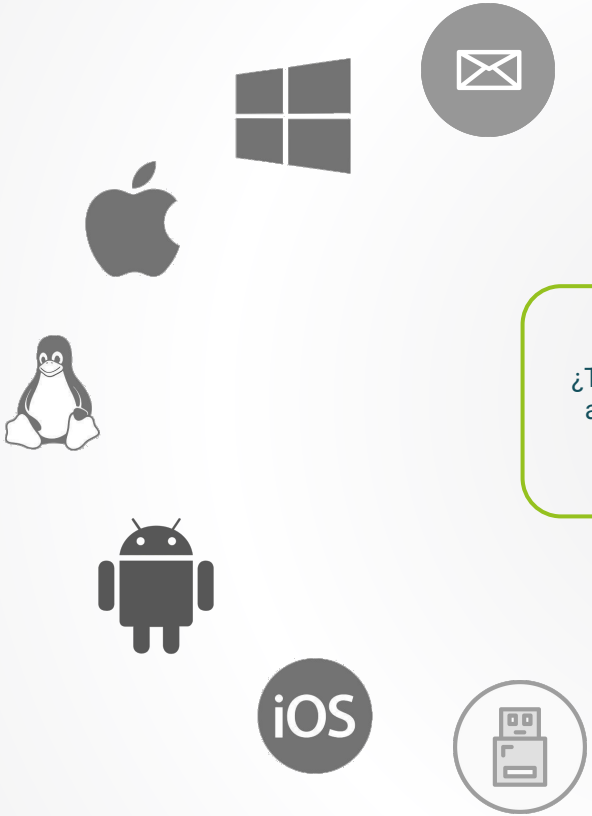


Métodos de detección únicos

- **Inteligencia de localización:** Detectamos falsificaciones de ubicación, viajes imposibles, VPNs, Tor ...
- **Tampering de dispositivo:** Sabemos si el dispositivo ha sido alterado, mediante root, emulación o depuración.

Identity Platform

Flexibilidad sin limites

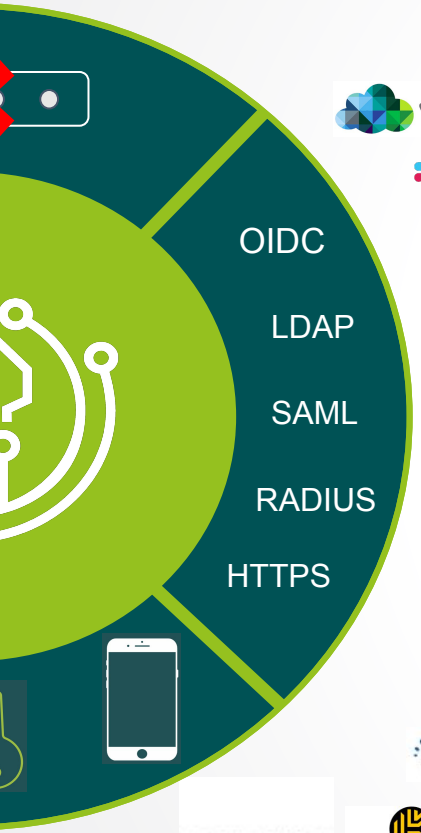


Flexibilidad sin límites

¿Tus empleados no tienen móvil corporativo? Ironchip funciona en android, iOS, Windows, Linux y Mac. Además, puedes reforzar tu seguridad con hardware tokens o dispositivos USB. O incluso autenticarte sin agentes mediante correo electrónico.

Identity Platform

Unificación total



Identidad unificada

Nuestra plataforma se integra sin problemas con todas tus herramientas corporativas, centralizando la gestión de la identidad y asegurando la privacidad de tus datos.

SEGURIDADAMÉRICA.COM Fortaleciendo Internet

IRONCHIP

CYBERARK

Microsoft Azure

OpenID Connect

Exchange

paloalto NETWORKS

vmware

slack

LDAP

VT Scada

Signifyd

WordPress

salesforce

WatchGuard

Jira Software

SONICWALL

zoom

Office 365

f5

SOPHOS

ForgeRock

Airtable

CISCO

FORTINET

Google Workspace

GitLab

odoo

IBM

workday

SAML

HubSpot

HashiCorp Terraform

CHECK POINT

aws

opennac enterprise

SailPoint

Dropbox

HashiCorp Boundary

HashiCorp Vault

Pulse Secure Acquired by Ivanti

SAP

SmarterServices

Microsoft Windows Logon

zscaler

KEEPER

ADFS

GitHub

citrix

RADIUS

Santander

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

Autenticación multifactor en Santander: seguridad y usabilidad con tecnología de Ironchip

Santander mejora la seguridad de sus accesos críticos con una solución MFA sin móvil, personalizada y compatible con Azure gracias a Ironchip.

Industria
Banca

País
España

Tamaño
207.137 empleados

THE RESULTS

0
móviles corporativos necesarios para autenticarse.

1
aplicación de escritorio personalizada. Compatible con Windows, Linux y Mac.

+ 25.000
empleados accediendo de forma segura sin necesidad de contraseñas.

"Gracias a la aplicación de escritorio de Ironchip, el Banco Santander ha podido reforzar la seguridad de sus accesos críticos sin sacrificar usabilidad, ni invertir en flotas de móviles. La autenticación es ahora más simple, segura y estratégica."

IRONCHIP

Casos de Estudio | Necesidades y solución

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

THE CHALLENGE

Cumplir el ENS sin fricciones ni móviles corporativos.

- Acceder de forma segura desde múltiples dispositivos sin depender de móviles personales.
- Eliminar barreras técnicas y logísticas en una organización multinacional.
- Cumplir con normativas como el ENS sin comprometer la experiencia del usuario.
- Garantizar seguridad sin necesidad de dotar a todos los empleados de dispositivos adicionales.
- Habilitar un acceso homogéneo, sin importar la sede, el país o la normativa local.

THE SOLUTION

Autenticación adaptada, segura y escalable para el ecosistema global de Santander.

- Aplicación desktop personalizada para login con MFA sin móviles.
- Integración nativa con Azure y despliegue multientorno (Windows, Linux, Mac).
- Interfaz corporativa alineada con la identidad visual de Santander.
- Monitorización contextual en tiempo real por usuario, ubicación y recurso.
- Formación a usuarios finales e impulso a la cultura de ciberseguridad.

Reducción de costes, aumento de eficiencia y cumplimiento normativo completo.

CLAVES DE LA TRANSFORMACIÓN DE ACCESOS EN SANTANDER

IRONCHIP

Fraud Detection Platform

www.ironchip.com

Anomalous behaviour

Los nuevos (y viejos) fraudes

SIM SWAPPING
6.500.000 M$

VISHING
Crecimiento 625%

SYNTHETIC ID
20% Fraude financiero EEUU

PHISHING
486.000.000 M$

Anomalous behaviour

Detected fraud behaviours

Detectamos los fraudes más avanzados

SIM SWAPPING

VISHING

PHISHING

SYNTHETIC IDENTITIES

MONEY MULE

Con un conjunto de métodos únicos

DEVICE FINGERPRINT

LOCATION INTELLIGENCE

DEVICE SWAPPING

TAMPERED DEVICE

TAMPERED APPLICATION

//ABANCA Banesco

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

ABANCA REFUERZA SU SISTEMA ANTIFRAUDE CON INTELIGENCIA DE UBICACIÓN

ABANCA necesitabafortalecer sus sistemas de detecciónde fraudedeIBM, que no lograban identificar con precisión dispositivos únicos. Esta limitación suponía un riesgo creciente en un contexto de rápida expansión.

THE RESULTS

+1
capaadicionaldeseguridad basada en localización.

1
integrado opcionalmente en procesos clave como login y recuperación de PIN.

GPS
mejora en la detección y prevención del fraude.

Desafío
ABANCA requería mejorar sus sistemas antifraude existentes debido a la falta de diferenciación entre dispositivos individuales, lo que generaba vulnerabilidades en un entorno de crecimiento acelerado.

Solución
Ironchip incorporó su solución de Fraud Detection basada en inteligencia de ubicación, integrándola con los sistemas de IBM. A través de un enfoque colaborativo y una prueba de concepto exitosa, se introdujo una capa adicional de protección, incluyendo la posibilidad de usar GPS en procesos clave como el inicio de sesión, la incorporación de nuevos usuarios y la recuperación de PIN. El resultado: una detección más efectiva, operaciones más eficientes y una mayor capacidad de prevención.

IRONCHIP

Fight Against Identity Threats

Ironchip's Identity & Access Management and Fraud Detection solutions powered by location intelligence technology

www.ironchip.com