



# IRONCHIP

## **Fight Against Identity Threats**

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

**[www.ironchip.com](http://www.ironchip.com)**

## 1. Ironchip

- ¿Quiénes somos?
- Partners y Colaboradores
- Nuestros clientes

## 2. Nuestra tecnología y productos

- Localización segura de Ironchip
- La localización aplicada a la identidad
- Nuestros productos de ciberseguridad

## 3. Identity Platform

- Ventajas
- Solución personalizable
- Modos de autenticación configurables
- Métodos recomendados por roles
- Protección de identidad y accesos
- ¿Cómo funciona? Location Intelligence
- Add-Ons: Windows logon, Linux logon, Mac logon, Desktop application
- Intrusion Detection System
- Casos de éxito

## 4. Fraud Detection

- Detección de fraude por localización
- Propuesta de valor
- Casos de éxito

## ¿Porqué Ironchip ?

El **55% de los ciberataques** tienen éxito debido a la suplantación de identidad o el robo de credenciales. Para combatir esta amenaza, **Ironchip revoluciona la autenticación de usuarios**, integrando inteligencia de ubicación certificada y un análisis avanzado de contexto en cada acceso.

**Más que autenticacion, una garantía de identidad:** Ironchip monitoriza cada acceso en tiempo real, analizando redes de conexión, entornos de ondas, IPs, historiales de conexión, patrones de comportamiento y la integridad del dispositivo (detección de rooting, emulación o manipulación). Incluso evalúa el idioma del sistema y señales de riesgo, garantizando una coherencia total entre el usuario y su identidad digital.

**Máxima seguridad, y total versatilidad, sin fricciones:** Ironchip no solo fortalece la autenticación con múltiples factores adaptativos, siempre completamente personalizados en función de los niveles de riesgo de cada usuario, sino que también proporciona visibilidad total y control en caso de incidencias o anomalías. Con su tecnología, cada acceso es seguro, confiable y libre de suplantaciones.

## Ciberseguridad en nuestro ADN

En Ironchip, la **seguridad** no es solo una palabra, es nuestro **compromiso**. Por eso, nos sentimos orgullosos de contar con el aval de los más exigentes organismos de **certificación**.

Nuestras soluciones han sido certificadas con el nivel ALTO, la máxima calificación posible, por las entidades más prestigiosas del sector.

El gobierno de España avala la compañía mediante su inversión, convirtiendonos en empresa clave estratégica a nivel nacional.



## Nuestros clientes

### +100 Clientes

En Ironchip, nuestros clientes son nuestra prioridad absoluta, y nuestra dedicación a la excelencia en cada interacción es la piedra angular de nuestra garantía de servicio.





**IRONCHIP**

**Tecnología y productos**

[www.ironchip.com](http://www.ironchip.com)



*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.

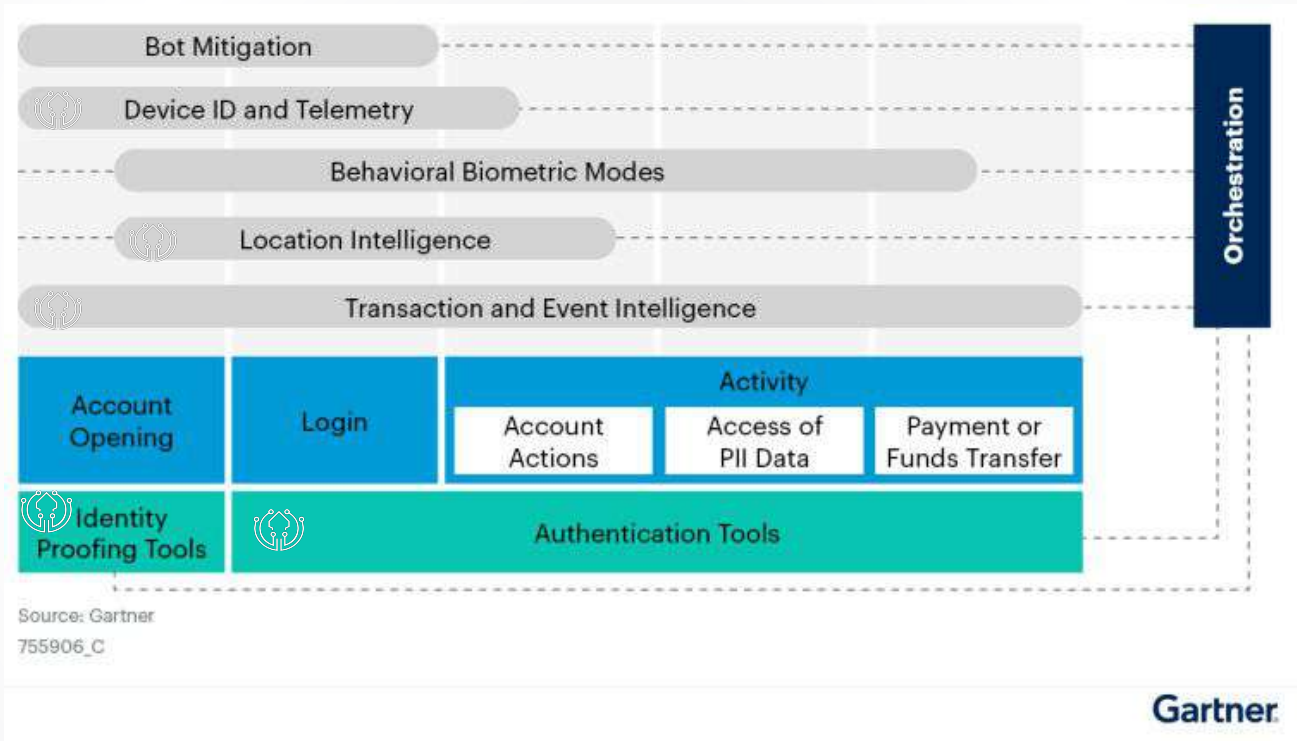
El **99%** de los estafadores cometen fraude desde la misma ubicación en dos ocasiones.



# 01 Location intelligence

## Location identity proof

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





## 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 esas relaciones lugar-dispositivo como parte de la identidad de cada usuario.

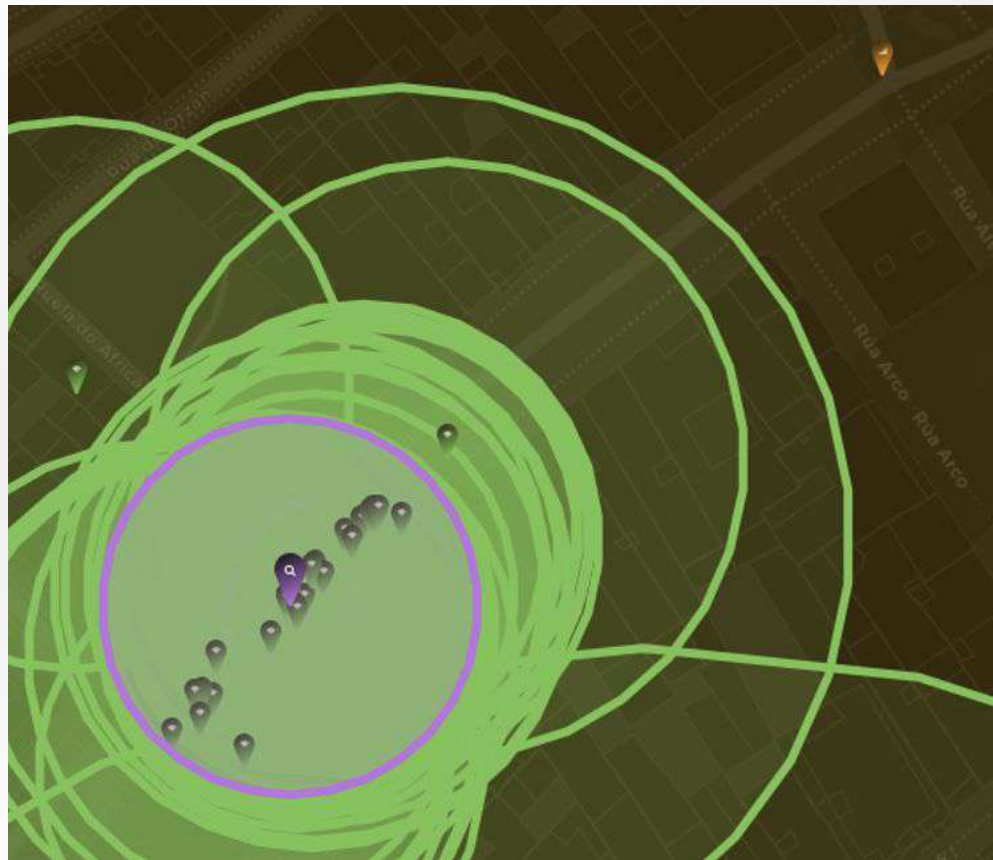


Image 1. Generated safe zone example with GPS, EM (2G, 3G, 4G, 5G) & IP signals.



**IRONCHIP**

**Identity Platform**

[www.ironchip.com](http://www.ironchip.com)

## 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 fáciles 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



## Passwordless Authentication



## Device Intelligence + Biometry + Hardware Keys

## User experience

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

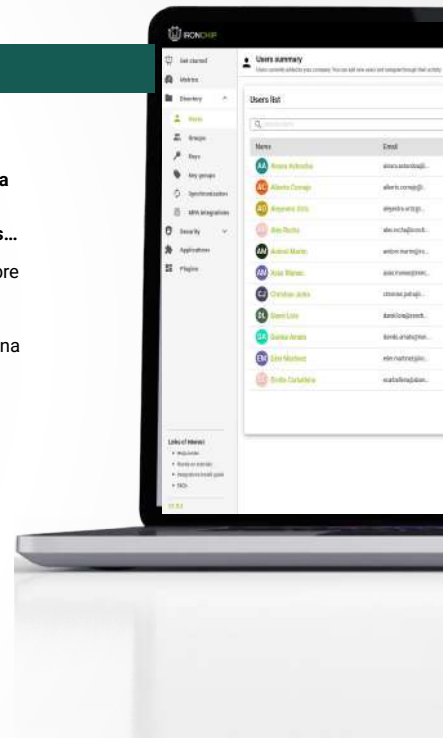
## Easiest Management

## 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 fáciles 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

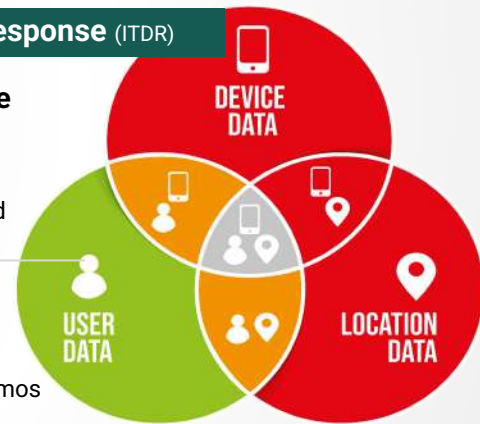
### Identity Threat Detection & Response (ITDR)

#### 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.







### 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.





## FREE

Enable passwordless authentication to seamlessly integrate and configure access to your services, endpoints and applications.

### Authentication:

- ➔ Agentless Authenticator
- ➔ Computer Authenticator
- ➔ Mobile Authenticator

### Identity & Access Management:

- ➔ Users, groups & devices management

- ➔ 1-10 users

### Plugins:

- ➔ NPS Plugin
- ➔ Microsoft ADFS Plugin

### Security:

- ➔ Access logs

### Metrics & Others:

- ➔ Basic metrics

## ENTERPRISE

Passwordless authentication enhances security with advanced configuration and monitoring features. Includes standard capabilities, plus:

### Authentication:

- ➔ USB Token Authenticator
- ➔ Smartcard Authenticator

### Identity & Access Management:

- ➔ Automatic provision from other directories i.e. Active Directory
- ➔ Configure conditional access policies

### Plugins:

- ➔ LDAP Server
- ➔ Windows, Linux & MAC Logon

### Security:

- ➔ Permissions Management
- ➔ Configurable IP whitelist
- ➔ Activity logs

### Metrics & others:

- ➔ Realtime timeline
- ➔ Corporative Look&Feel

## PREMIUM

The Ironchip's identity full experience to zero account takeover

### Authentication:

- ➔ Location-based authentication
- ➔ Context-based authentication

### Identity & Access Management:

- ➔ Secure location Management
- ➔ Generate corporate perimeter of trust

### Intrusion Threat Detection & Response:

- ➔ Detect identity threats
- ➔ Define customized risk rules based on the context
- ➔ Block attacks automatically
- ➔ Get realtime reports via API

### Metrics & others:

- ➔ Advanced metrics
- ➔ Syslog / API for SIEM integration



**IRONCHIP**

**Fraud Detection Platform**

[www.ironchip.com](http://www.ironchip.com)

# 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**

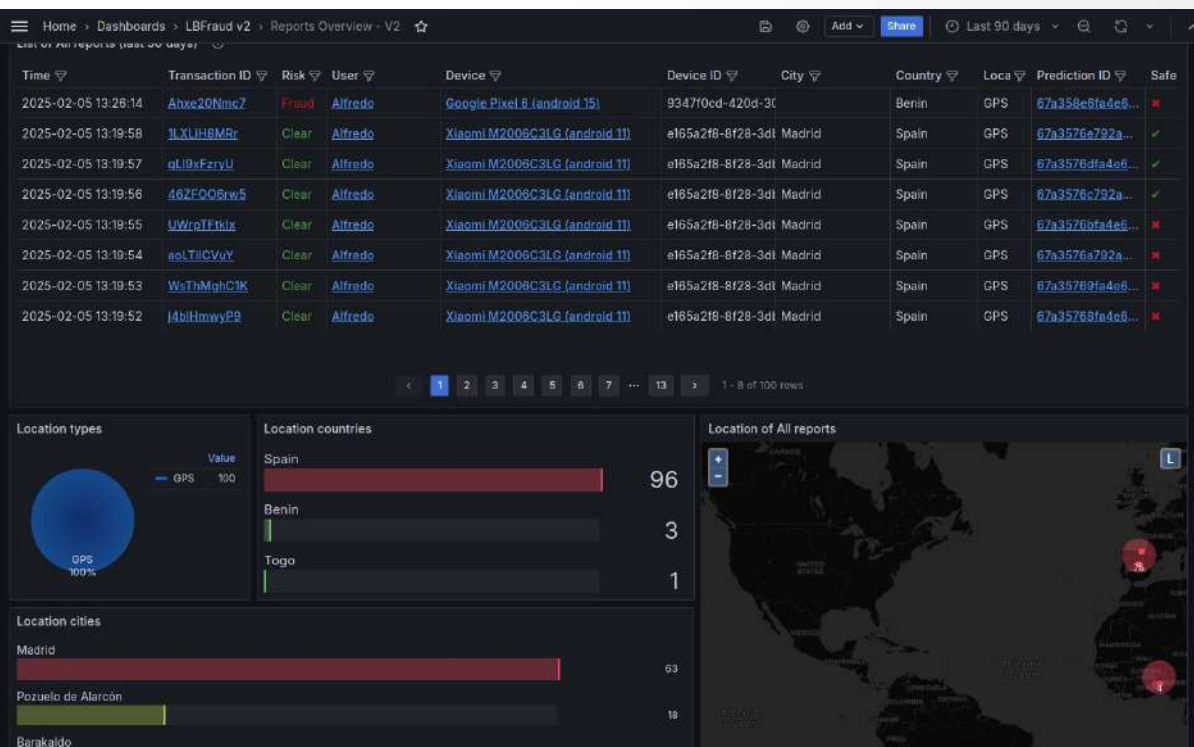
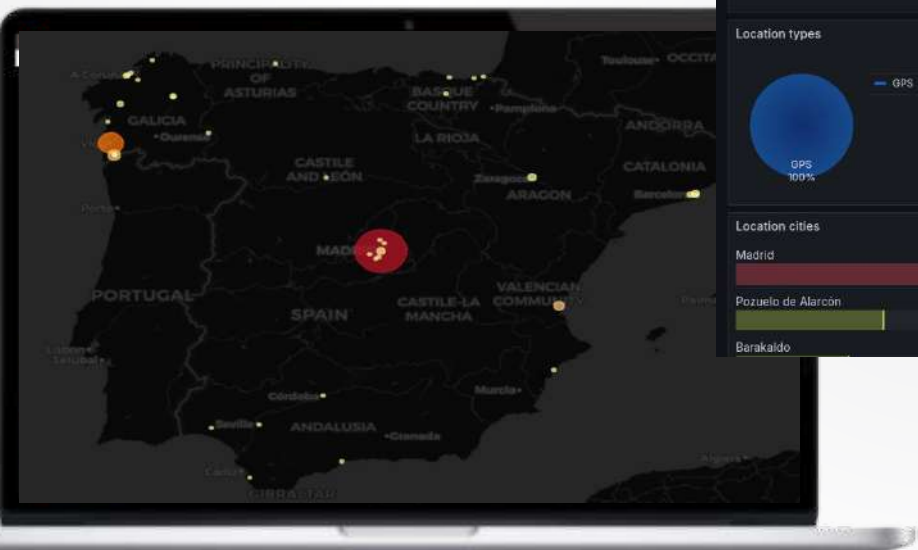


**TAMPERED APPLICATION**



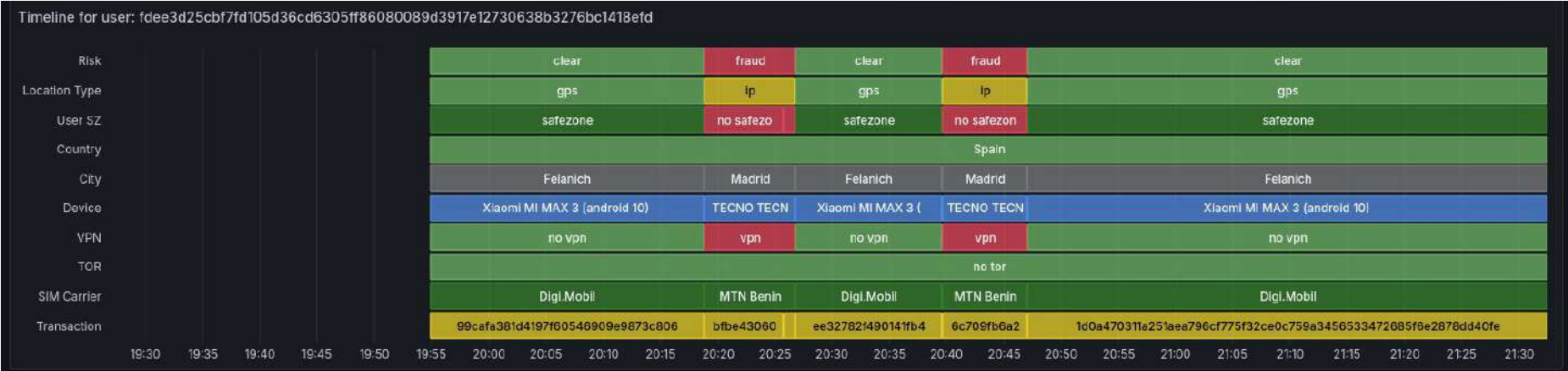
## Dashboard

- Mapa de calor con puntos negros del origen de los ataques.
- Reportes históricos de los ataques por usuario descargables.



- Análisis forense de los casos a petición.
- Motor de reglas configurable.
- Alerta en tiempo real. (SLA < 1 seg)

¿Y si el hacker no nos da el GPS?: Pillando a un 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.

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.



# IRONCHIP

## **Fight Against Identity Threats**

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

**[www.ironchip.com](http://www.ironchip.com)**