

---

# Fraud detection platform

Mitigating digital fraud through advanced analytics  
and real-time tracking



---

# Table of Contents

## Ironchip

- About Us
- Certifications

## Our technology and products

- Location Intelligence
- Location Applied to Identity
- Location-Based Fraud Detection

## Anti-Malware Module

- Real-time detection of indicators of compromise
- Protection against overlays, keyloggers, RATs, SIM swapping, and hooking

## Anti-phishing module

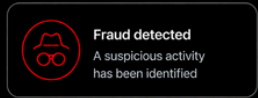
- Site detection
- Credential scanning

# Who are we?

Ironchip is a **leading global cybersecurity company specializing in identity protection and fraud detection.**

We use a unique technology based on Location Intelligence that validates user identity, providing real-time visibility, traceability, and control over every access attempt.

In this way, we guarantee **360° security**, connecting the physical world with digital protection and ensuring continuous, effective, and frictionless access for employees, customers, and third parties.



# Cybersecurity is in our DNA

At Ironchip, security isn't just a word—it's our **commitment**. That's why we hold certifications such as LINCE from the National Cryptology Center ([cpstic.ccn.cni.es](http://cpstic.ccn.cni.es)).

Our solutions have been certified at the HIGH level and included in the **CCN-CERT** Security Products Catalog, which endorses their use in critical environments. Additionally, we have defined secure usage procedures for high-security scenarios ([ccn-cert.cni.es](http://ccn-cert.cni.es)).

**The Spanish government supports the company** through its investment, making us a key strategic enterprise at the national level.



PYME INNOVADORA



---

# Technology



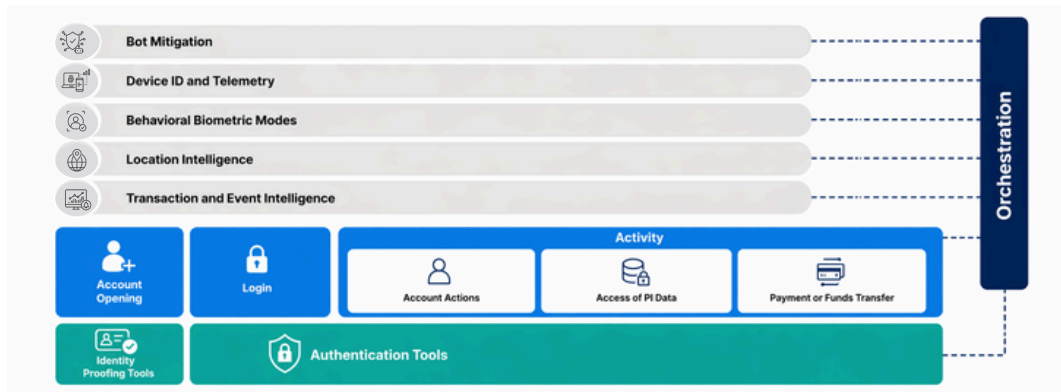
**IRONCHIP**  
CYBERSECURITY



## Location intelligence - Location identity proof

Scope of online fraud detection capabilities throughout a typical customer journey.

Gartner



# Location-based detection technology

## Common Operation Zones



The majority of identity processes take place in trusted locations.

## Untrusted Location



**92%** of attacks occur remotely, from a location the user has never been in.



**99%** of fraudsters commit fraud from the same location at least twice.

## ESPAÑA

# 10 EL PAÍS MÁS ATACADO

OAS	300 909
MAV	256 597
NAV	163 384
IDS	157 797
VUL	112 394
KAS	101 384
BAD	80 443

Detección de amenazas basadas en el número de fuentes en tiempo real.

[Más información](#)

Compartir información



AMENAZAS DETECTADAS

ÚLTIMAS 24 HORAS

**1.356.789**



## Trading-Based Allocation - Types of Protected Transactions



---

## Secure and localized transactions

### What is a Safe Zone?

A safe zone is a unique, familiar, and tamper-proof location for each user.

### How is a safe zone generated?

A safe zone is generated using AI, after capturing and analyzing the following signals every time a user interacts with a mobile or web app:

Mobile signals: 2G, 3G, 4G, or 5G.

Surrounding Wi-Fi signals and favorite Wi-Fi network.

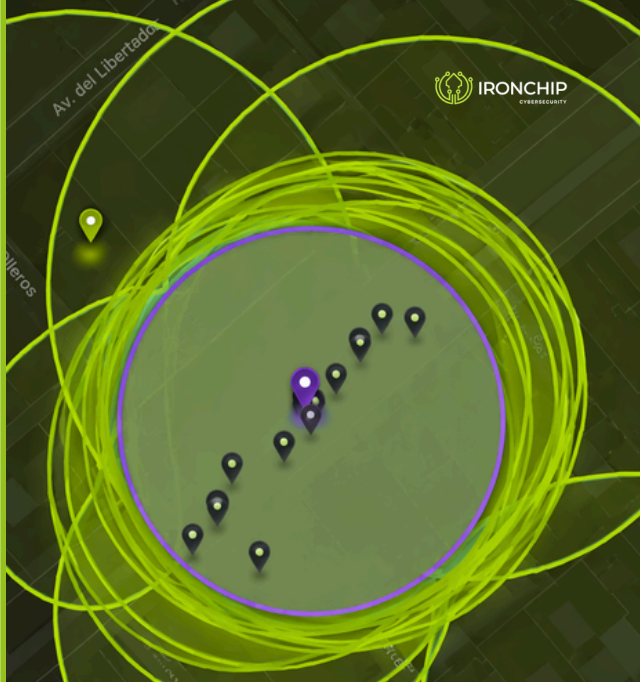
GPS and IP.

Geolocation based on latency.

Internet service provider (ISP) and connection to cell towers.

Native SIM card in use.

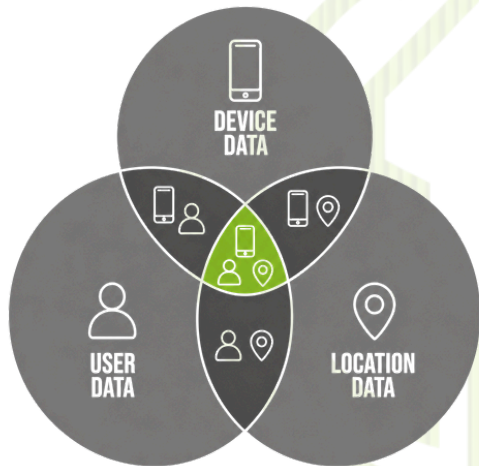
Location spoofing via VPN and TOR networks.



# Behavioral localization

Our technology uniquely links the device to its actual location using artificial intelligence and environmental signals (Wi-Fi and cellular networks).

This approach allows us to **model precise behavioral patterns**, which are essential for the secure identity of the future. The ability to understand where the user is and how they interact with their resources offers unprecedented control, setting the definitive standard for security and authentication in digital systems.





---

# Fraud Detection **Platform**



**IRONCHIP**  
CYBERSECURITY

## Unusual behavior: detected fraudulent activity



We detect the most advanced frauds



SIM SWAPPING



VISHING



PHISHING



SYNTHETIC IDENTITIES



MONEY MULE



With a set of unique methods



DEVICE  
FINGERPRINT



LOCATION  
INTELLIGENCE



DEVICE  
SWAPPING



TAMPERED  
DEVICE



TAMPERED  
APPLICATION

# SDK & API Installation

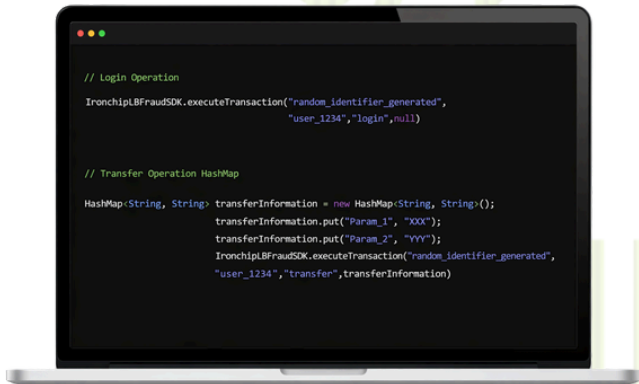
## Datasource SDK

An iOS/Android/JavaScript library that can be integrated into any mobile or web application to capture the necessary information.

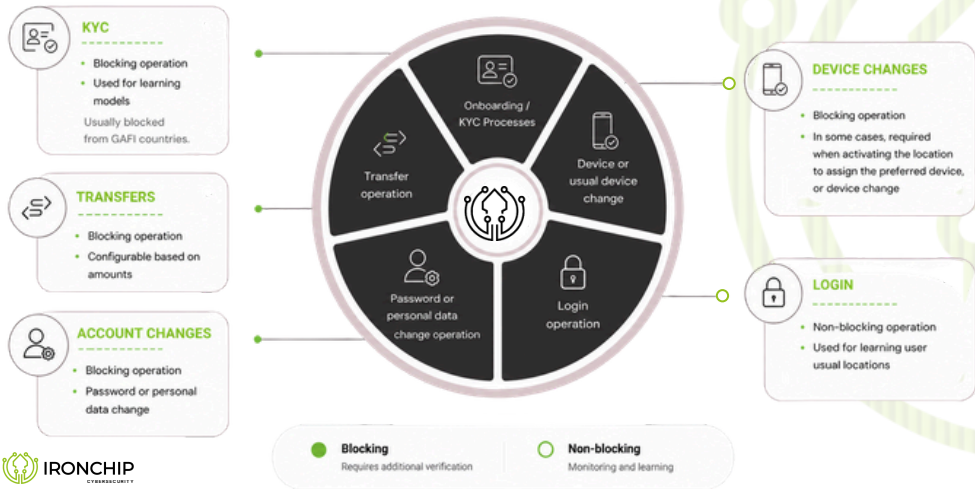
## Fraud Detection API

An HTTP API for retrieving results, which can be integrated with any BPM or SIEM.

[Documentation](#)



## Transactions to be protected



# Advanced security rules engine

## Risk Placement Rules

- Origin locations in FATF countries.
- Connection via the TOR network or a VPN.
- If RF geolocation does not match GPS or SIM data.
- Presence of a residential proxy.
- High-risk or blacklisted ISP.
- Location spoofing.
- The SIM carrier differs from the location or ISP origin.
- Impossible travel.
- Public Wi-Fi network (high).
- Private Wi-Fi network.
- Locations associated with confirmed attacks on other entities.
- Blacklisted or high-risk IP.

## Rules for High-Risk Devices

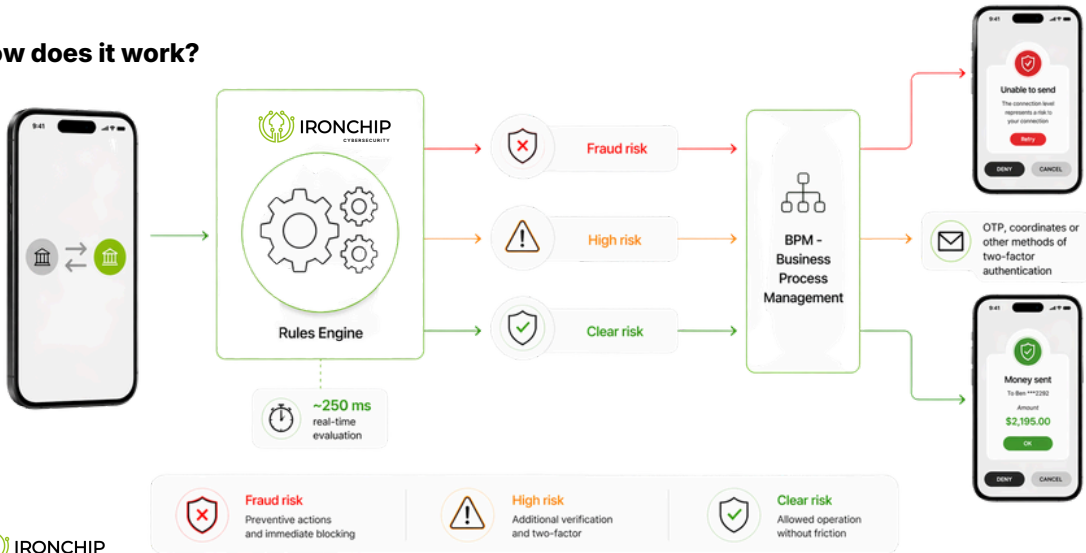
- Malware installed.
- Debugging process active.
- Device blacklisted.
- High-risk device (ALPS, TECNO, INFINIX, Fairphone, Nothing, MobiWire).
- Rooted or jailbroken device.
- Outdated device in the update history.
- Unexpected roaming.

## Rules of Conduct

- Roaming + Virtual SIM.
- Language switching without changing devices or usual location.
- Call transfer or active call forwarding.
- Device associated with more than 3 users.
- Cyrillic languages from locations where the device is not in use.
- Multiple connections within short time windows.
- Patterns consistent with known attack campaigns.


Thanks to the intelligent combination of variables, **our rules engine establishes highly precise behavioral policies tailored to each scenario**

## How does it work?





## Normal and safe behavior


Date

 04/12/2025, 09:48:14

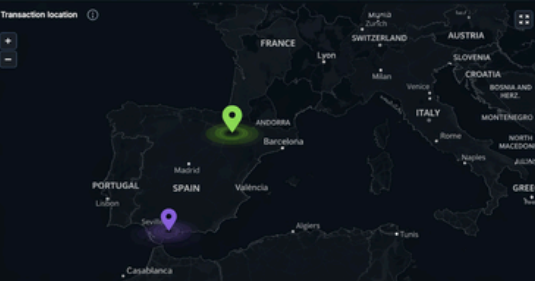
Risk

 **Clear** 


Descriptive Report

 user in sz


Transaction location  ⓘ




Transaction ID

96c528eb49306b5130c897b7c98eb36607d22d96795e81829ea3224750af792 

User ID

995e52e6653e2f17a3ff5f0d5456c022002d5000eb3830f9ea60dbfda4e95d 

Device

 Xiaomi 2310BRN04Y  
(android 15)






Location Details

Location City	Cordova
Location Country	Spain
SIM Current Country Code	es
SIM Native Country Code	es
<b>User in Safezone</b>	<b>True</b>




Connection Details

VPN	false
TOR	false
Roaming	false
WIFI SSID	Vodafone-C3B4
WIFI BSSID	8c-6a-8a-64-c3-c0
ISP	VODAFONE ONO, S.A.U.
IP	62.57.236.222



Device Sensors

-  On Call Off
-  GPS On
-  Mobile Networks On
-  WiFi On
-  WiFi Connected On

Device Integrity

-  Debugged No
-  Emulated No
-  Rooted No


Device Details

-  Device Language es
-  SIM Carrier DIGI ES

Report Cases

Cases

user in safe zone

<  > 1 - 1 of 1 rows

## Anomalous behaviour - Money mule

### Sudden use of a VPN

On September 12, a connection via a VPN—specifically NordVPN—was observed for the first time. This represents a significant deviation from the user's usual behavior.

### Changing the SIM Card Carrier

The device went from being connected in Spain to another location, also reported as Spain, but with a SIM card originally from Benin. This was made possible by switching mobile service providers from Digi (Spain) to MTN Benin.



# Anomalous behaviour - Money mule

## An Impossible Journey

In 5 minutes, I'll be traveling from Spain to Benin. Such a drastic change of location in such a short time is logistically impossible without using technology to manipulate the location.

## Changing ISPs

In addition, a change in internet service provider was identified. The user switched from connecting via Red Digital de Telecomunicaciones de las Islas Baleares S.L. (Spain) to connecting via NordVPN, which coincides with the appearance of the SIM card from Benin.



## Anomalous behavior - Vishing for authorized fraud



Real-time call detection in transaction operations.









IP call detection:

- Telegram, Discord, WhatsApp...



Call redirection and roaming detection.

Device Sensors	Device Integrity	Device Details
 On Call <span>On</span>	 Debugged <span>No</span>	 Device Language <span>es</span>
 GPS <span>On</span>	 Emulated <span>No</span>	 SIM Carrier <span>MASMOVIL</span>
 Mobile Networks <span>On</span>	 Rooted <span>No</span>	
 WIFI <span>On</span>		
 WIFI Connected <span>Off</span>		

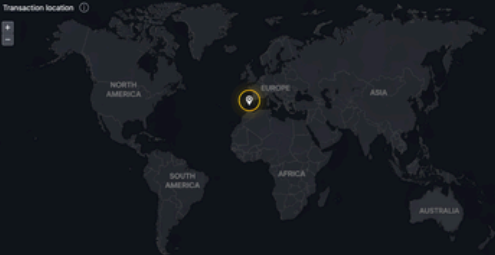
## Abnormal behavior - Location spoofing or virtual SIMs

Date  
**09/12/2025, 17:55:07**  
Europe/Madrid (UTC+1)

Risk  
**Fraud**

Descriptive Report  
no gps - device swap - new device disable gps and enables vpn - new device disable gps

Transaction location



Transaction ID  
`f52e422f95990411bc9f659d040ee8f77c3bcc47a99efbc0fa0833f9e4f1c891`

User ID  
`ee8f0356588ad570922db5405b948a0a8500967e28ac5daa002368aa9951880`

Device  
Xiaomi M2006C3MNG (android 10)

Location Details

Location City	Barcelona
Location Country	Spain
SIM Current Country Code	us
SIM Native Country Code	No value
User in Safezone	False

Connection Details

VPN	True
TOR	False
Roaming	False
WiFi SSGO	---
WiFi BSSID	---
ISP	PacketHub S.A.
IP	185.214.97.69

Report Cases

Cases	unknown location
	device swapping

Device Sensors

On Call	Off
GPS	Off
Mobile Networks	Off
WiFi	Off
WiFi Connected	Off

Device Integrity

Debugged	No
Emulated	No
Rooted	No

Device Details

Device Language	es
SIM Carrier	No value

# Antimalware with active real-time protection

Our next-generation antimalware module acts as an active defense layer during the session. Unlike static solutions, our technology detects indicators of compromise (IoCs) in real time, such as injection attacks, screen overlays, and unauthorized remote access tools. This constant monitoring ensures that the environment where identity is validated is **free from malicious interference, safeguarding the integrity of every transaction.**

## Overlay Attacks

Fake screens overlaid on top of the real app to steal credentials. Theft of passwords and 2FA codes.

## Remote Access Trojans (RATs)

Hidden or active remote control tools (AnyDesk, TeamViewer). A third party performs the transaction on the user's behalf.

## Keyloggers

Scripts or apps that capture every keystroke the user makes. Capturing PINs, card details, and private keys.

## SIM Swapping / SMS Sniffers

Malware that intercepts confirmation SMS messages from the bank. Authorizing transfers without the user seeing the code.

## Code injection / Hooking











Manipulation of the browser or app's memory to alter the destination of a payment.  
Changing the recipient's IBAN at the last second.

## Phishing/Smishing Module - Malicious Site Scanning

Our **phishing detection technology** continuously scans the internet to identify websites impersonating financial institutions. When we locate them, we automatically analyze their vulnerabilities, taking advantage of the fact that these infrastructures are often weak and insecure.

Whenever possible, we set up a monitoring **system that captures, in real time**, the information attackers are attempting to steal. This data is immediately reported to the affected institutions so they can block access, reset credentials, and prevent fraud.


In addition, **we detect compromised cards and track the channels** where criminals centralize the stolen information—including Telegram bots discovered through these vulnerabilities—to anticipate risks and strengthen protection for financial customers.

STATUS	DATE	URL
●	0 minutes ago	 <a href="https://santander.info-clienteportal.com/acceso_usuario.php">https://santander.info-clienteportal.com/acceso_usuario.php</a>
●	18 minutes ago	 <a href="https://seur.comwa.vip/es">https://seur.comwa.vip/es</a>
●	18 minutes ago	 <a href="https://seur.comwl.vip/es">https://seur.comwl.vip/es</a>
●	20 minutes ago	 <a href="https://seur.comwh.vip/es">https://seur.comwh.vip/es</a>
●	20 minutes ago	 <a href="https://seur.comwe.vip/es">https://seur.comwe.vip/es</a>
●	20 minutes ago	 <a href="https://seur.comwo.vip/es">https://seur.comwo.vip/es</a>
●	20 minutes ago	 <a href="https://seur.comwb.vip/es">https://seur.comwb.vip/es</a>
●	20 minutes ago	 <a href="https://seur.comwp.vip/es">https://seur.comwp.vip/es</a>
●	21 minutes ago	 <a href="https://seur.comwt.vip/es">https://seur.comwt.vip/es</a>
●	21 minutes ago	 <a href="https://seur.comwc.vip/es">https://seur.comwc.vip/es</a>

## Phishing/Smishing Module - Site Profiles

**carrefour-passmovil.com**  
<https://es.carrefour-passmovil.com/eAABo12MGyJTf2zr/login>

REGISTERED: 20/11/2025      NAMESERVERS: damian.ns.cloudflare.com  
 REGISTRAR: Sav.com, LLC      damian.ns.cloudflare.com  
 ASN: CLOUDFLARENET      paltyn.ns.cloudflare.com



SAFEBROWSING: ON      POTENTIAL: 100.0%      AI: 99.8%  
 URL: ON      IP: ON      QR: ON      RULES: 390.0

THREAT ACTOR: **SAV**  
 SAV is a highly organized threat actor group actively targeting major Spanish banking entities.

Added (20 nov, 20:52) → Monitoring Urls (20 nov, 20:52) → Pending (20 nov, 20:52) → Url Signature Found (27 nov, 16:09) → Monitoring Selenium (27 nov, 16:09) → Done (27 nov, 16:11)

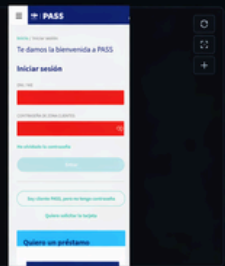
Requests: 25      Text Length: 1000      Inputs: 3

Page Title: PASS Carrefour acceso a Zona Clientes

Input Fields: [ ] [ ] [ ]

Extracted Text

HTML Preview











Evidence Score: 4200.0

Detected Keywords: Tarjeta, NIE, Cliente

Targeted Brands: Carrefour (File: rubik-regular.woff2)

Phishing Kits

## Phishing/Smishing Module - Credential and Card Analysis

COLLECTION DATE	USER	PASSWORD	SOURCE	SITE ID
<b>Dec 9, 2025</b> Collected: 08:59:18 AM Entered in DB: Dec 9, 2025 08:52:27 AM	 <b>406L</b> ID: 8192	..... 	<b>carrefour</b> karma_todo745f karma_todo745f@localhost	<b>es.carrefour-passmovil.com</b> >
<b>Dec 9, 2025</b> Collected: 02:42:58 PM Entered in DB: Dec 9, 2025 02:42:56 PM	 <b>7994G</b> ID: 8193	..... 	<b>carrefour</b> karma_todo745f karma_todo745f@localhost	<b>es.carrefour-passmovil.com</b> >
<b>Dec 9, 2025</b> Collected: 05:50:34 PM Entered in DB: Dec 9, 2025 05:36:57 PM	 <b>7767m</b> ID: 8199	..... 	<b>carrefour</b> karma_todo745f karma_todo745f@localhost	<b>es.carrefour-passmovil.com</b> >
<b>Dec 9, 2025</b> Collected: 08:12:05 PM Entered in DB: Dec 9, 2025 08:11:36 PM	 <b>011Z</b> ID: 8204	..... 	<b>carrefour</b> karma_todo745f karma_todo745f@localhost	<b>es.carrefour-passmovil.com</b> >

---

# Case **study**



**IRONCHIP**  
CYBERSECURITY





Sector

Banking

Location

Spain

Size

+ 8,000 employees

# Advanced detection of banking fraud in digital environments

Detection of fraud-related patterns, such as money mule schemes and SIM swapping, through continuous behavioral analysis



## CHALLENGE

Abanca was facing the growing complexity of banking fraud, with threats such as money mules and SIM swapping that were difficult to detect using traditional systems. The lack of visibility into location, device, and behavior limited the ability to identify anomalies in real time. This made it difficult to distinguish between legitimate and fraudulent access in critical transactions. Furthermore, it was necessary to strengthen security without compromising the user experience.

## SOLUTION

A solution was implemented that relies on continuous analysis of user behavior, incorporating location and device information as identity factors, enabling the detection of anomalous access attempts and fraud—such as SIM swapping—without affecting the user experience.

## RESULTS

- Detection of multiple types of fraud, such as **money mule schemes and SIM swapping**
- Real-time identification of anomalous access based on behavior, location, and device
- Enhanced ability to distinguish between legitimate users and fraudulent activity

Ironchip integrates its product into a key stage of the authentication process in a simple, cost-effective way, offering a user experience that is hard to find these days.

– **Fatima Cereijo**, Manager of Fraud Control and Privacy, Abanca



---

**They trust us**





**Verify identities** before  
they become a security  
incident.



**IRONCHIP**  
Identity Security Platform

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

+34 944 075 954  
[www.ironchip.com](http://www.ironchip.com)

© 2026 Ironchip. All rights reserved. Ironchip and its logo are registered trademarks of Ironchip Telco S.L. All other trademarks are the property of their respective owners.