

Plataforma de detección de fraude

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



Índice

Ironchip

- ¿Quiénes somos?
- Certificaciones

Nuestra tecnología y productos

- Location Intelligence
- La localización aplicada a la identidad
- Detección de fraude por localización

Módulo Anti Malware

- Detección en tiempo real de indicadores de compromiso
- Protección frente a overlays, keyloggers, RATs, SIM swapping y hooking

Módulo antiphishing

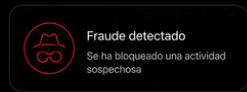
- Detección de sites
- Scanning de credenciales

¿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.



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.



Tecnología



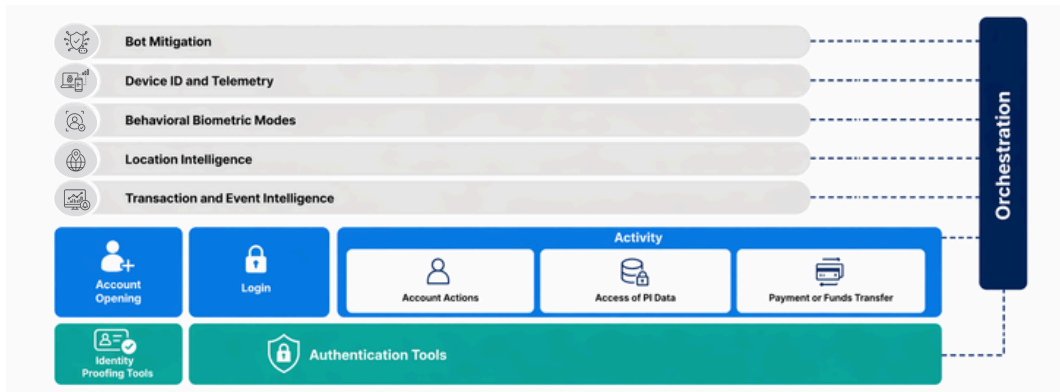
IRONCHIP
CYBERSECURITY



Localización 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



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.

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



La localización por operaciones - Tipos de transacciones protegidas



Zonas seguras o habituales

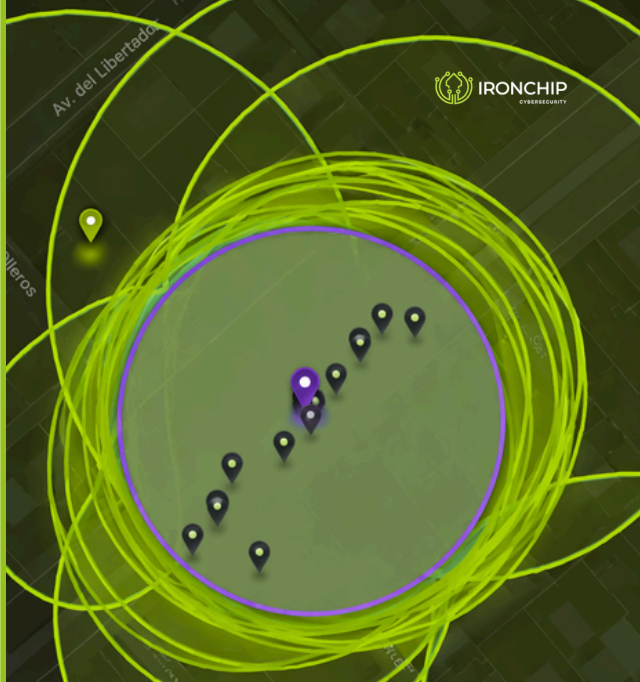
¿Qué es una Zona Segura?

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:

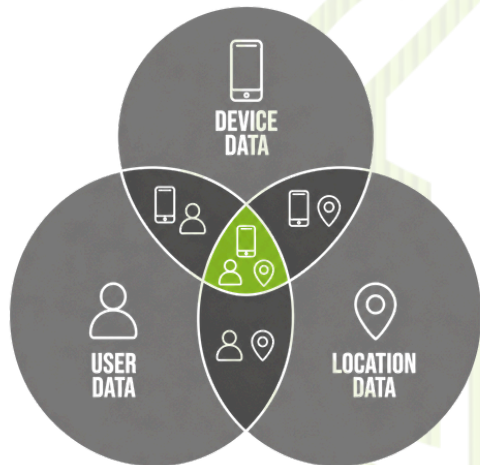
- Señales móviles: 2G, 3G, 4G o 5G.
- Señales WiFi alrededor y WiFi favorito.
- GPS e IP.
- Geolocalización basada en latencias.
- ISP contratado y conexión a antenas móviles.
- SIM nativa en uso.
- Suplantaciones de localización vía red VPN y TOR.



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.




Plataforma de **detección** **de fraudes**



IRONCHIP
CYBERSECURITY

Comportamientos anómalos: comportamientos fraudulentos detectados

 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

Instalación SDK & API

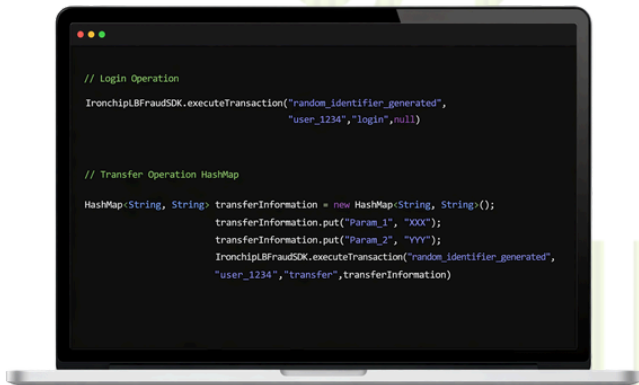
Datasource SDK

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](#)



Operaciones a proteger



KYC

- Operación bloqueante
- Usado para aprendizaje del usuario

Usualmente bloqueos desde países GAFI.



TRANSFERENCIAS

- Operación bloqueante
- Configurable en función de cantidades



MODIFICACIONES DE LA CUENTA

- Operación bloqueante
- Cambio de contraseña o datos personales



CAMBIO DE CONFIGURACIONES

- Operación bloqueante
- En algunos casos obligatoriedad de activación de la ubicación para asignar el dispositivo favorito, o cambio de dispositivo



LOGIN

- Operación no bloqueante
- Usado para aprendizaje de las ubicaciones habituales de los usuarios



Bloqueante

Requiere verificación adicional



No bloqueante

Monitoreo y aprendizaje

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

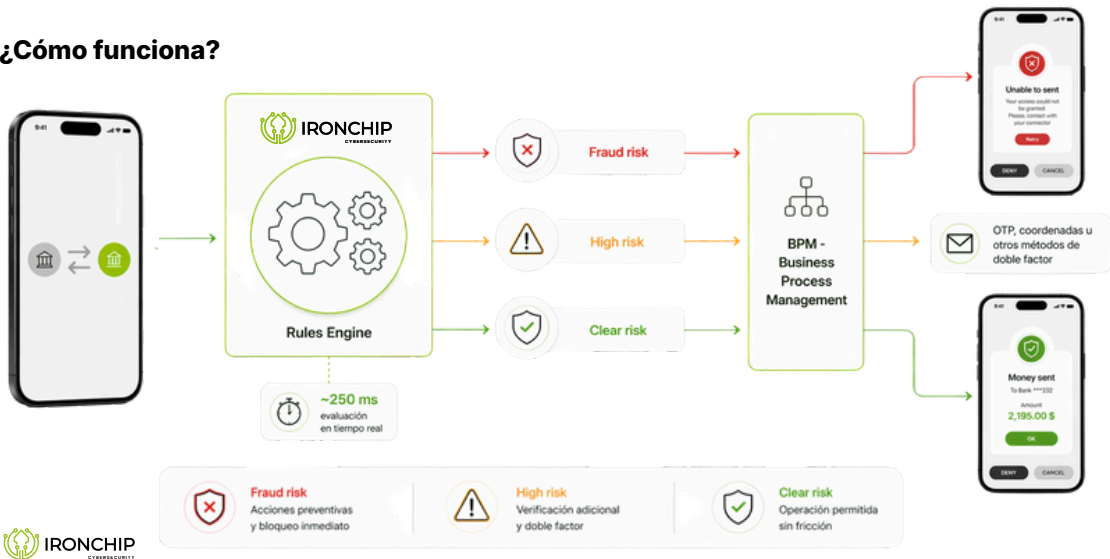
- Software malicioso instalado.
- Proceso de depuración o debugging activo.
- Dispositivo marcado en lista negra.
- Dispositivo de riesgo (ALPS, TECNO, INFINIX, Fairphone, Nothing, MobiWire).
- Dispositivo con root o jailbreak.
- Desactualización del dispositivo en el historial de actualizaciones.
-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

¿Cómo funciona?





Comportamiento normal y seguro


Date

 04/12/2025, 09:48:14

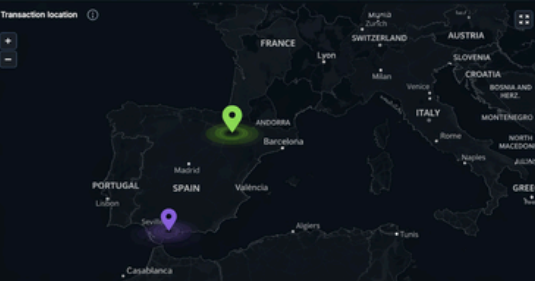
Risk

 **Clear** 


Descriptive Report

 user in sz


Transaction location ⓘ



Transaction ID

96c528eb49306b5130c897b7c98eb36607d22d96795e81829ea3224750af792 

User ID

995e52e6653e2f17a3ff5f0d5456c022002d5500eb3830f9ea60dbfda4e95d 






Location Details

Location City	Cordova
Location Country	Spain
SIM Current Country Code	es
SIM Native Country Code	es
User in Safezone	True




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

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



Device Sensors

 On Call	On
 GPS	On
 Mobile Networks	On
 WIFI	On
 WIFI Connected	Off

Device Integrity

 Debugged	No
 Emulated	No
 Rooted	No

Device Details

 Device Language	es
 SIM Carrier	MASMOVIL

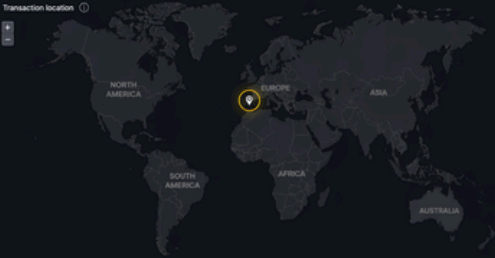
Comportamiento anómalo - Suplantación de ubicación o SIM virtuales

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
f52e422f95990411bc9f559d040ee6f77c3bc47a99efbc0fa0833f9e4f1c891

User ID
ee8f0356588a05709228b540b948a0a8500967e28ac5daa002368aa0951880

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 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.

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.


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

Módulo phishing/smishing - Perfiles de site

carrefour-passmovil.com
<https://es.carrefour-passmovil.com/eAAA8o12MGyJTf2zr/login>

REGISTERED: 20/11/2025
 REGISTRAR: Sav.com, LLC
 ASN: CLOUDFLARENET

NAMESERVERS: damian.ns.cloudflare.com
 paltyn.ns.cloudflare.com



SAFEBROWSING
 URL IP QR

POTENTIAL: 100.0%
 AI: 99.8%
 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: 3

Extracted Text

HTML Preview











Evidence Score: 4200.0

Detected Keywords: Tarjeta, NIE, Cliente

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

Phishing Kits

Módulo phishing/smishing - Análisis de credenciales y tarjetas

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

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.

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





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



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.