

Plataforma de identidad

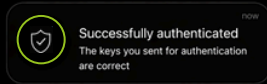
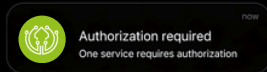
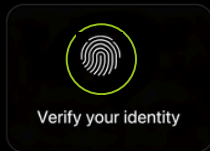
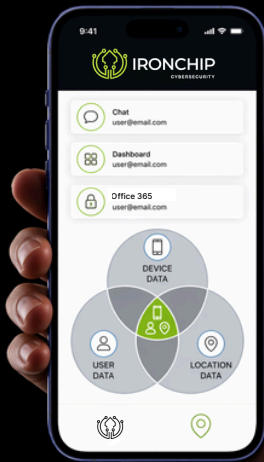
Gestión unificada de identidades con análisis de contexto avanzado



¿Quiénes somos?

Ironchip es una **plataforma de seguridad de identidad avanzada y unificada** que utiliza la identidad contextual para garantizar que cada usuario es quien dice ser basándose en su entorno físico único.

A través de un control de acceso inteligente y una vigilancia continua, blindamos los activos críticos de la empresa permitiendo conexiones solo desde ubicaciones seguras y autorizadas.



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.



PYME INNOVADORA



Entidades que confían en la solución



AAPP



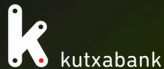
Industria



Banca



Energía



Tecnología



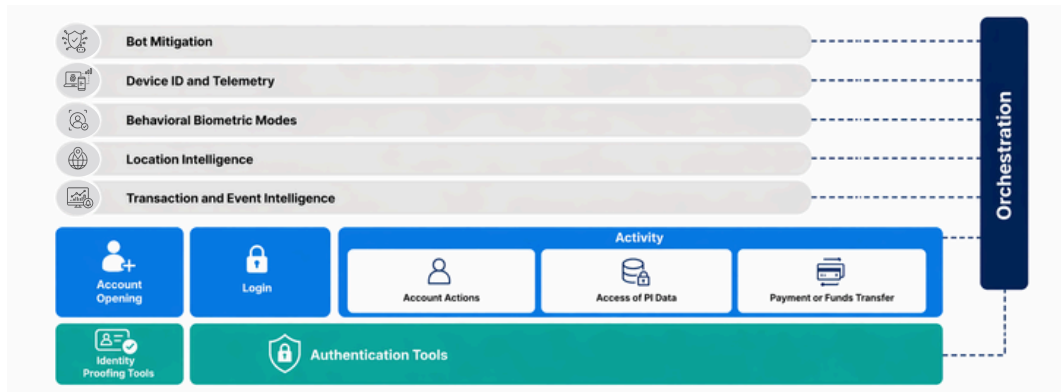
IRONCHIP
CYBERSECURITY



Localización inteligente - Localización precisa como prueba de identidad

Uso de la localización como parte del sistema de autenticación y gestión de identidad.

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

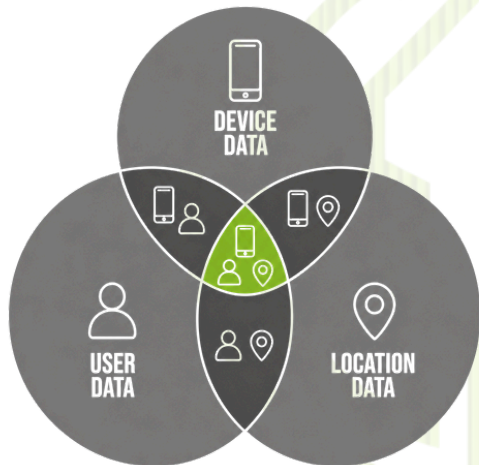
1.356.789



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 identidad



IRONCHIP
CYBERSECURITY

Nuestros pilares de seguridad

Experiencia passwordless

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.

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.

OIDC, LDAP, SMAL, RADIUS, HTTPS



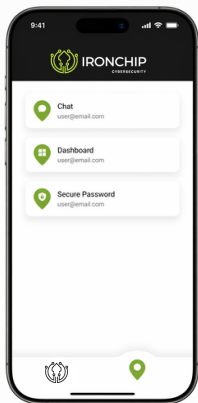
Seguridad basada en riesgo

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

Acceso multidispositivo

¿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.

Experiencia de autenticación sin contraseñas



Autenticación sin contraseña



Inteligencia del dispositivo + Biometría + Claves hardware

Experiencia del usuario

- ✓ Sin esfuerzo: 3 pruebas de identidad en 1 interacción
- ✓ Seguro: Resistente a phishing, malware y SIM swapping
- ✓ Passwordless: Sin contraseñas, OTPs...

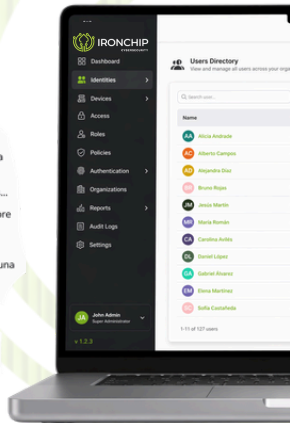
La gestión más sencilla

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
- Solución **multitenant**: Gestiona diferentes unidades organizativas y territoriales desde una única herramienta

Inteligencia basada en datos

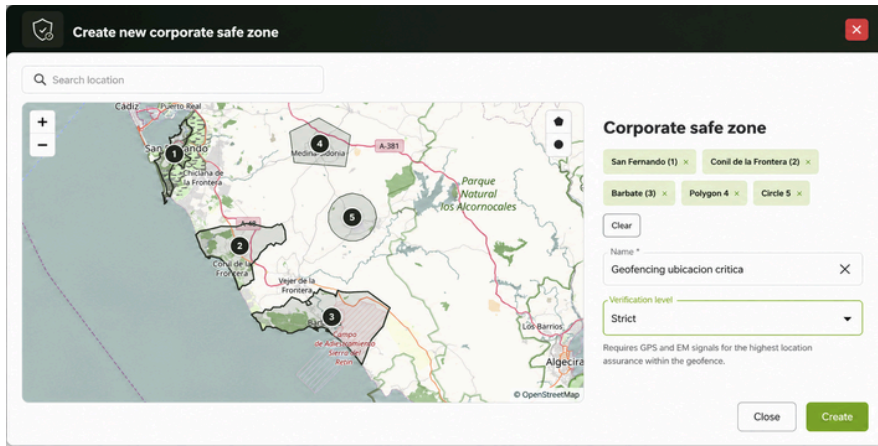
- **Trazabilidad completa**: Todo lo que ocurra dentro de la herramienta queda registrado



Ubicación como clave de acceso

Definición de zonas seguras para controlar el acceso a aplicaciones y recursos críticos

Create new corporate safe zone
✕



Map showing geofencing zones (1-5) around San Fernando and Conil de la Frontera. Zone 1 is a circle around San Fernando. Zone 2 is a polygon around Conil de la Frontera. Zone 3 is a polygon around Vejer de la Frontera. Zone 4 is a polygon around Medina Sidonia. Zone 5 is a circle around Parque Natural los Alcornocales.

Corporate safe zone

San Fernando (1) ✕
Conil de la Frontera (2) ✕

Barbate (3) ✕
Polygon 4 ✕
Circle 5 ✕

✕

Verification level

Strict

Requires GPS and EM signals for the highest location assurance within the geofence.

Identidad por contexto y análisis de riesgo



Pruebas de conocimiento cero



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.



Detección y respuesta ante amenazas de identidad



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.



ITDR - Real-time feed

Track identity threats and suspicious activity in real-time and neutralize risks instantly.

Risk level	Date	User id
High	Apr 29, 2026, 15:32:04	john.doe@ironchip.com
High	Apr 29, 2026, 15:32:04	john.doe@ironchip.com
Low	Apr 29, 2026, 15:17:49	maria.garcia@ironchip.com
Low	Apr 29, 2026, 15:17:39	maria.garcia@ironchip.com
Low	Apr 29, 2026, 15:15:19	john.doe@ironchip.com
Low	Apr 29, 2026, 15:15:01	john.doe@ironchip.com
Low	Apr 29, 2026, 15:14:23	john.doe@ironchip.com
Low	Apr 29, 2026, 15:06:14	maria.garcia@ironchip.com
Low	Apr 29, 2026, 15:04:11	maria.garcia@ironchip.com
Low	Apr 29, 2026, 15:04:44	john.doe@ironchip.com
Low	Apr 29, 2026, 15:04:41	john.doe@ironchip.com
Low	Apr 29, 2026, 15:03:16	maria.garcia@ironchip.com

Unificación total de aplicaciones

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

CYBERARK

Microsoft
Azure

slack

WatchGuard

aws

SOPHOS

vmware

salesforce

Office 365

CISCO

Exchange

SmarterServices

IBM

GitHub

Dropbox

HubSpot

KEEPER

paloalto

WordPress

Signifyd

CHECK POINT

Airtable

VTscada

zoom

f5

workday

SAP

Microsoft

SailPoint

Fortinet

SONICWALL

ForgeRock

GitLab

Google Workspace

Jira Software

odoo

Terraform

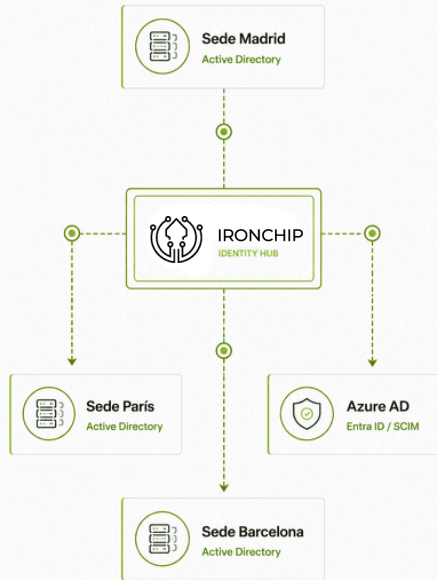
ADFS

Sincronización y vigilancia continua de Identidades

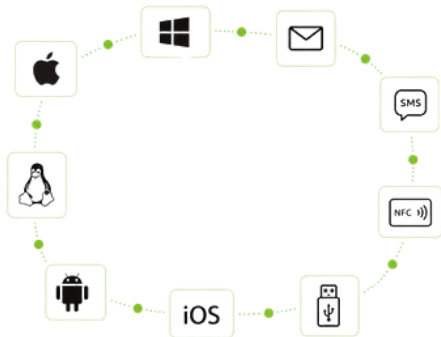
Sincronización en tiempo real de todas las identidades, eliminando brechas entre entornos locales y nube.

Nuestro agente ADConnect integra cualquier Active Directory on-premise de forma segura y automática. Mediante SCIM, conectamos directamente con Azure AD (Entra ID) y otros proveedores cloud.

Cada cambio de rol o baja se propaga instantáneamente a Ironchip, garantizando que ningún acceso quede activo sin autorización.



Todos los métodos de autenticación

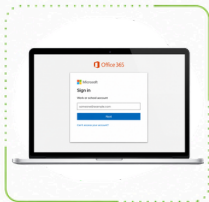


Seguridad sin fricción, en cualquier dispositivo.

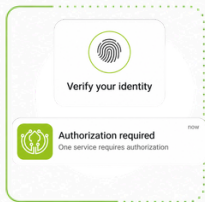
Implemente la identidad contextual donde la necesite. Desde aplicaciones nativas en móvil y escritorio hasta métodos "passwordless" y físicos:

- Dispositivos: Soporte multiplataforma total y aplicaciones dedicadas.
- Posesión física: Refuerce la seguridad con tokens USB o tecnología NFC/RFID.
- Conectividad directa: Acceso rápido mediante Magic Links y verificación por SMS.

Solución con teléfonos móviles



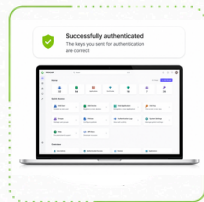
El usuario intenta acceder al recurso corporativo Office 365



Recibe una notificación push en su dispositivo móvil

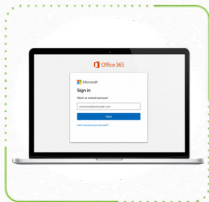


Abre la notificación y aprueba el acceso a través de la aplicación móvil



Se verifica la identidad contextual; si es válida, se permite el acceso, y si es incorrecta, se bloquea y se alerta al SIEM o administrador.

Solución con app de escritorio



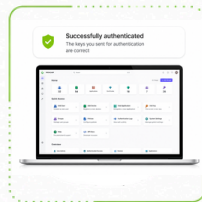
El usuario intenta acceder al recurso corporativo Office 365



Recibe una notificación push en su aplicación de escritorio



Abre la notificación y aprueba el acceso a través de la aplicación de escritorio



Una vez autenticado, el usuario puede acceder a los recursos solicitados

Solución con token USB



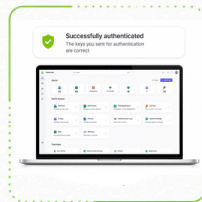
**El usuario conecta su USB
e intenta acceder al
recurso corporativo
Office 365**



**El token USB se sincroniza
con la app de escritorio y
genera la identidad a partir de
las dos claves en la app de
escritorio y el token USB**



**La aplicación lee la clave
generada y realiza la
autenticación**



**Una vez autenticado, el
usuario puede acceder a los
recursos solicitados**

Solución con tarjeta NFC



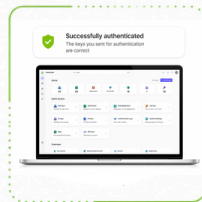
El usuario pasa su tarjeta NFC/RFIS a través del lector para intentar acceder al recurso corporativo Office 365



El lector lee la identificación de la tarjeta y la transforma en la identidad del AD

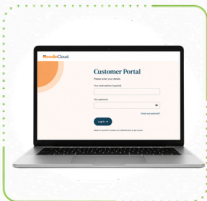


La tarjeta actúa como una prueba de lo que tiene y rellena la información del servicio para activar la autorización

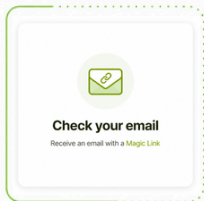


Una vez autenticado, el usuario puede acceder a los recursos solicitados

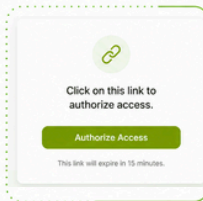
Solución para acceso de proveedores o terceros



El usuario intenta acceder al recurso corporativo de manera remota



Recibe un correo electrónico con un Magic Link



Hace clic en el enlace para autorizar el acceso



Una vez autenticado, el usuario puede acceder a los recursos solicitados

Casos de éxito



Control de accesos y detección de amenazas en la administración pública

Autenticación mediante app móvil combinada con monitorización SIEM para detección y respuesta en tiempo real

RETO

El Ayuntamiento se enfrentaba a la necesidad de asegurar accesos a sistemas críticos en un entorno con múltiples usuarios, dispositivos y servicios conectados. La falta de visibilidad centralizada dificultaba detectar accesos anómalos y responder a amenazas en tiempo real. Además, la creciente exposición a ataques mediante credenciales comprometidas requería reforzar tanto la autenticación como la monitorización continua. Todo ello debía integrarse sin aumentar la carga operativa y cumpliendo con normativas como el ENS.

SOLUCIÓN

Se implementó una solución que integra autenticación mediante app móvil con capacidades de monitorización SIEM, permitiendo supervisar y correlacionar eventos en tiempo real. Esto facilita la detección de accesos anómalos y la activación de respuestas automáticas, reforzando la seguridad sin aumentar la complejidad operativa.

RESULTADOS

- **Detección temprana de accesos anómalos** mediante correlación de eventos
- **Mayor visibilidad y control** gracias a la monitorización continua tipo SIEM
- **Capacidad de respuesta automatizada** ante accesos sospechosos

“Generalmente solemos tener resistencia a los cambios por parte de los usuarios y debo destacar, que en este caso, está siendo muy bien aceptado dada la buena experiencia de usuario que nos está aportando.

– José Luis Miguel, Responsable de Seguridad, Ayuntamiento de Alcobendas



Sector

Banca

Localidad

España

Tamaño

+200.000 empleados

Control de accesos en entornos corporativos sin uso de móviles

Autenticación basada en aplicación de escritorio que permite acceso seguro sin depender de dispositivos móviles



RETO

Santander necesitaba implementar una solución de autenticación multifactor conforme a normativas como el ENS, garantizando accesos seguros a su ecosistema digital. La dependencia de dispositivos móviles suponía una limitación en entornos donde los usuarios no disponían de ellos o no podían utilizarlos. Esto dificultaba asegurar el acceso a sistemas críticos de forma homogénea en toda la organización. Además, era necesario mantener la accesibilidad sin comprometer la seguridad ni la experiencia del usuario.

SOLUCIÓN

Se implementó una solución de autenticación multifactor basada en una aplicación de escritorio que combina contraseña y OTP sin necesidad de un segundo dispositivo. Esto permite asegurar el acceso a los sistemas corporativos desde cualquier entorno, manteniendo el control y la accesibilidad para todos los usuarios.

RESULTADOS

- Accesos seguros a sistemas corporativos sin necesidad de dispositivos móviles
- **Cumplimiento de normativas como el ENS** sin afectar la accesibilidad
- **Mayor control y gestión centralizada** de accesos en entornos globales

Inicio de sesión sólido sin ataduras móviles gracias a nuestra solución de escritorio para Linux, Mac y Windows.

Protección de accesos mediante **autenticación con token físico**

Acceso a datos sensibles mediante autenticación basada en token físico, garantizando seguridad sin fricción



RETO

Nalanda necesitaba asegurar el acceso a información sensible gestionada en sus equipos corporativos, garantizando que solo los usuarios autorizados pudieran acceder. La dependencia de dispositivos móviles para la autenticación suponía una limitación operativa en su entorno. Además, era necesario implementar un sistema robusto sin comprometer la facilidad de uso para los empleados. Todo ello debía garantizar control total de accesos manteniendo la eficiencia en los procesos.

SOLUCIÓN

Se implementó una solución de autenticación multifactor personalizada que sustituye el uso del móvil por un token físico, dividiendo la identidad entre el usuario y su equipo. Esto permite garantizar accesos seguros a los sistemas corporativos manteniendo la simplicidad en la experiencia de uso.

RESULTADOS

- **Accesos seguros a datos sensibles** sin dependencia de dispositivos móviles
- **Mayor control y visibilidad** para los equipos de TI en la gestión de accesos
- **Autenticación sin fricción** que mantiene la eficiencia en el uso diario

Consideramos que es una empresa en constante cambio y crecimiento basándose en las necesidades de los clientes para cumplir sus expectativas.

– Administración de sistemas

¿Tienes control real sobre la identidad en tu organización?

Estas preguntas reflejan el nivel real de control sobre tu identidad digital. Cualquier punto no cubierto supone una brecha potencial.

Si la respuesta a alguna de estas preguntas es negativa, es el momento de actuar.

[Habla con nosotros](#)

- ¿Tienes usuarios **sin dispositivo móvil** que necesitan un MFA robusto y no sabes cómo dárselo?
- ¿Podrías **bloquear instantáneamente un acceso** si el usuario está en la ciudad correcta pero en una ubicación no autorizada?
- ¿Es tu **MFA actual vulnerable a ataques de Fatiga** de Notificaciones (Push Spam) o Phishing?
- ¿Sufre tu **equipo de IT gestionando altas y bajas** de identidades en múltiples plataformas de forma manual?
- ¿Cumples con las **normativas más estrictas (NIS2, ISO 27001)** en lo que respecta a control de acceso y trazabilidad?
- ¿Tienes **bajo control total el acceso de terceros** y proveedores externos a tu infraestructura crítica?
- ¿Puedes certificar **con total seguridad los lugares físicos exactos** desde donde se conectan tus empleados?
- ¿Eres **capaz de unificar todos tus AD (locales y nube)** y auditar cambios de políticas en tiempo real?
- ¿Tu **sistema actual te avisa de comportamientos anómalos** en el mismo instante en que alguien accede a tus sistemas?
- ¿Están tus **accesos remotos por RDP o SSH protegidos** por algo más que una simple contraseña?



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.