IRONCHIP
CYBERSECURITY

Política de Privacidad

Plataforma de identidad y Aplicación Móvil

Your Next Generation Identity

Tabla de contenido

La presente Política de Privacidad describe cómo **IRONCHIP TELCO, S.L.** trata los datos personales en relación con el uso del **Producto de Identidad y Autenticación** de Ironchip, disponible en sus versiones web, SDK, API, aplicación móvil, aplicación de escritorio, autenticadores, tokens, tarjetas NFC/RFID, autenticaciones delegadas y cualquier otro módulo asociado (en adelante, el "Servicio").

Esta Política se aplica a los **usuarios autorizados** del Servicio y a los **Clientes** (organizaciones) que contratan el producto.

1. Normativa aplicable

Nuestra Política de Privacidad se ha diseñado de acuerdo con el REGLAMENTO (UE) 2016/679 del PARLAMENTO EUROPEO y del CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), en adelante RGPD UE 2016/679, y en lo que no contradiga el mencionado Reglamento, por lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante LOPDGDD 3/2018. Ambas normas constituyen el marco jurídico aplicable al tratamiento de datos realizado a través del Servicio y determinan las obligaciones de Ironchip y los derechos de los usuarios.

La utilización del Servicio implica que el Cliente y/o usuario ha sido informado de acuerdo con estos textos legales y comprende las bases jurídicas, finalidades y condiciones bajo las cuales se tratarán sus datos personales conforme a lo establecido en esta Política.

2. Glosario técnico

Con el fin de facilitar la comprensión del funcionamiento del Servicio, se incluyen algunas definiciones básicas de los conceptos técnicos que intervienen en el proceso de autenticación. Se entiende por:

- Token: el elemento digital que permite validar temporalmente la identidad del usuario sin exponer sus credenciales;
- MFA o autenticación multifactor: el proceso mediante el cual se requiere más de un elemento de verificación para conceder acceso;
- Device ID: la huella técnica que vincula de forma segura a un usuario con su dispositivo habitual.
- Fingerprint: hace referencia al conjunto de parámetros técnicos que permiten identificar un dispositivo sin necesidad de utilizar datos personales directos
- Perímetros de confianza: son áreas geográficas o lógicas definidas por el Cliente que permiten reforzar el control de acceso mediante restricciones basadas en ubicación.
- Metadata: corresponde a la información técnica necesaria para asegurar el funcionamiento del Servicio, sin incluir contenidos personales del usuario.

Estas definiciones ayudan a que tanto el Cliente como los usuarios comprendan qué tipo de información se utiliza y con qué finalidad, reforzando la transparencia del Servicio sin comprometer su seguridad

3. Identidad del Responsable y datos de contacto

Responsable del tratamiento	IRONCHIP TELCO, S.L. Domicilio social: Calle Beurko Viejo, 17 – 48902 Barakaldo, Vizcaya (España) CIF: B95880332 Contacto: privacy@ironchip.com
Delegado de Protección de Datos (DPD/DPO):	María Llanas Villa - Equipo de Cumplimiento Contacto: dpo@ironchip.com

4. Rol de Ironchip y del Cliente (Responsable / Encargado del Tratamiento)

El tratamiento de datos realizado a través del Servicio puede implicar distintos niveles de responsabilidad en función de la naturaleza de la información tratada y de quién decide sus fines y medios. En lo que respecta a los datos necesarios para garantizar la seguridad, estabilidad y correcto funcionamiento del Servicio -incluidos los registros técnicos, la información derivada del uso del sistema, los eventos utilizados para la detección de accesos no autorizados y aquellos que se generan en el contexto del soporte- **Ironchip actúa como Responsable del Tratamiento,** dado que estos tratamientos forman parte de sus obligaciones técnicas y operativas y no dependen de las decisiones del Cliente.

De forma diferenciada, cuando el Servicio se utiliza dentro de la infraestructura del Cliente para autenticar a sus propios usuarios, Ironchip actúa como **Encargado del Tratamiento,** procesando los datos personales únicamente conforme a las instrucciones documentadas del Cliente y en los términos previstos en el artículo 28 del RGPD. En este ámbito, corresponde al **Cliente actuar como Responsable del Tratamiento,** pues es quien decide qué datos se incorporan al sistema, cómo se configuran las políticas de acceso y autenticación, qué usuarios intervienen y cuál es la base jurídica que legitima el tratamiento dentro de su organización.

Como Responsable, el Cliente debe garantizar que los datos personales facilitados al Servicio son lícitos, exactos y adecuados para los fines perseguidos, así como gestionar las altas y bajas de usuarios, determinar los criterios de conservación y cumplir con la normativa interna y sectorial que le resulte aplicable. Por su parte, Ironchip limitará su actuación a la prestación del Servicio bajo dichas instrucciones, sin utilizar estos datos para finalidades propias ajenas a la relación con el Cliente.

5. Definición del Servicio y arquitectura de privacidad

El Servicio de Identidad de Ironchip está diseñado para ofrecer un sistema de autenticación robusto que combina diferentes mecanismos de verificación y protección con el fin de garantizar que solo los usuarios legítimos puedan acceder a los recursos autorizados. Para lograrlo, el Servicio integra métodos avanzados de autenticación multifactor, técnicas de seguridad basadas en el contexto y procesos de vinculación segura entre el usuario y sus dispositivos. Todo ello se complementa con un modelo de cifrado que protege las claves y elementos críticos directamente en el entorno del usuario, evitando que Ironchip o terceros puedan acceder a información sensible.

Además, el Servicio puede operar mediante integraciones que permiten su uso en aplicaciones y sistemas corporativos a través de APIs, SDK o elementos físicos como tarjetas, tokens o autenticadores delegados, entre otros. La arquitectura incorpora mecanismos de verificación basados en la ubicación o en zonas de confianza definidas por el Cliente, así como un sistema continuo de supervisión que permite identificar comportamientos anómalos y reforzar la seguridad sin interferir en la experiencia del usuario.

Es importante destacar que Ironchip no almacena contraseñas en texto claro, no tiene acceso a las claves privadas del usuario y no utiliza la información tratada para fines de marketing, elaboración de perfiles comerciales o actividades ajenas a la prestación del Servicio. La arquitectura se sustenta en principios de minimización, protección criptográfica y privacidad por diseño, asegurando que solo se utilicen los datos estrictamente necesarios para garantizar la autenticación y la seguridad del entorno.

6. ¿Qué datos personales tratamos?

El Servicio trata únicamente aquellos datos personales que resultan indispensables para identificar al usuario, verificar su autenticidad y garantizar la seguridad del entorno. Estos datos pueden variar en función de la configuración establecida por tu organización -Cliente de Ironchip-, pero en términos generales incluyen la información básica necesaria para reconocer a cada usuario dentro del sistema -como su nombre, apellidos, correo electrónico corporativo o identificador asignado-, así como determinados atributos profesionales que tu propia organización gestione, tales como el rol o el nivel de permisos que tenga dentro de la organización.

Para permitir la autenticación y proteger los accesos, el Servicio genera y utiliza información vinculada a los mecanismos de seguridad, como los tokens y claves derivadas que permiten validar la sesión, los factores de autenticación que se hayan activado o la huella técnica del dispositivo desde el que se accede. También se trata información procedente del propio funcionamiento técnico del sistema, como la dirección IP, el tipo de dispositivo, la configuración regional, los parámetros del navegador o la telemetría estrictamente necesaria para detectar anomalías y garantizar la integridad del Servicio.

Cuando el Cliente activa funciones avanzadas basadas en el contexto, el sistema puede procesar datos de localización aproximada, así como información relativa a zonas de confianza. Estos datos se gestionan aplicando medidas de cifrado o técnicas de seudonimización, y se utilizan exclusivamente para reforzar la seguridad del acceso, nunca para trazar movimientos o elaborar historiales de ubicación del usuario.

Durante el uso del Servicio también se generan registros asociados a la actividad de autenticación, como la fecha y hora de acceso, los eventos de seguridad, las incidencias detectadas o los cambios de configuración. Esta información resulta esencial para la trazabilidad, la prevención del fraude y la resolución de incidencias. En el contexto de soporte técnico, pueden tratarse además aquellos datos que el propio usuario facilite al comunicarse con Ironchip, tales como mensajes, capturas o registros necesarios para analizar una incidencia.

Es importante subrayar que Ironchip no trata en ningún caso contraseñas en texto claro, ni accede a contenidos almacenados por los usuarios, ni procesa categorías especiales de datos, ni recibe información biométrica cruda. Cuando un usuario emplea autenticación biométrica en su dispositivo, Ironchip solo recibe la confirmación de éxito o fallo emitida por el propio dispositivo, sin acceder al dato biométrico en sí.

7. Finalidades del tratamiento y bases jurídicas

El tratamiento de los datos personales a través del Servicio se fundamenta en finalidades claramente definidas y en bases jurídicas plenamente alineadas con el Reglamento General de Protección de Datos. En primer lugar, la información del usuario se utiliza para permitir su autenticación y gestionar el acceso al Servicio, lo que incluye la validación de credenciales, la creación de sesiones seguras y el funcionamiento de los diferentes factores de autenticación disponibles. Esta finalidad constituye el núcleo de la prestación contratada y se ampara en la *ejecución del contrato*, dado que sin estos datos sería imposible ofrecer el Servicio ni garantizar su operatividad.

De manera complementaria, el Servicio trata datos indispensables para preservar la seguridad del entorno digital del Cliente, anticipar comportamientos anómalos y prevenir accesos no autorizados. Este tratamiento implica analizar ciertos indicadores técnicos, registrar eventos de uso y aplicar mecanismos automáticos o manuales de refuerzo de seguridad cuando sea necesario. Tales actuaciones se encuentran respaldadas por el *interés legítimo* de Ironchip y del Cliente en proteger la integridad de las cuentas, las credenciales y la infraestructura tecnológica; un interés legítimo que, además, resulta esencial para cumplir obligaciones en materia de ciberseguridad, trazabilidad y prevención del fraude. Este interés ha sido ponderado internamente para asegurar que prevalece la protección del usuario y que se aplican salvaguardas que eviten un impacto desproporcionado sobre sus derechos.

Asimismo, se procesan determinados datos técnicos para mejorar el rendimiento del Servicio, corregir fallos, optimizar la experiencia de uso y garantizar que la plataforma se mantenga disponible y estable. Estas actividades, que no afectan de forma significativa a los usuarios,

también se basan en el *interés legítimo* de Ironchip de mantener un sistema técnicamente robusto y en constante evolución, aplicando en todo momento medidas de minimización y seudonimización.

Cuando el usuario solicita asistencia o soporte técnico, los datos tratados para resolver su consulta -incluidos aquellos que él mismo facilite voluntariamente- se procesan en el contexto de la *ejecución contractual,* dado que forman parte del propio servicio contratado y resultan necesarios para atender correctamente la incidencia planteada.

Finalmente, existen tratamientos que pueden resultar obligatorios en virtud de la normativa vigente, como atender requerimientos de autoridades competentes o colaborar en procedimientos administrativos o judiciales. En estos casos, la base jurídica aplicable es el *cumplimiento de obligaciones legales*, y el tratamiento se limita estrictamente a aquello que resulte imprescindible para satisfacer dichos requerimientos.

En aquellas funcionalidades opcionales cuya activación implique un tratamiento adicional de datos -como la localización o factores avanzados de autenticación-, será el Cliente, en su condición de Responsable del Tratamiento, quien deberá obtener el *consentimiento explícito* de los usuarios cuando corresponda, asegurando que dicho consentimiento es libre, informado y revocable. Ironchip solo procesará estos datos cuando la funcionalidad haya sido habilitada por el Cliente y bajo la garantía de que este ha cumplido con las obligaciones previstas en los artículos 6 y 7 del RGPD.

8. Toma de decisiones automatizadas

El Servicio incorpora mecanismos automatizados destinados a reforzar la seguridad de los accesos y a proteger tanto a los usuarios como a la propia infraestructura frente a comportamientos anómalos. Estos sistemas analizan determinados indicadores técnicos -como patrones de uso, coherencia del dispositivo o señales de riesgo- con el único objetivo de identificar situaciones que puedan comprometer la integridad del acceso. En función de esta evaluación, el sistema puede aplicar medidas preventivas, como solicitar autenticaciones adicionales o bloquear temporalmente un intento que resulte claramente sospechoso.

Aun cuando estas acciones se basan en procesos automáticos, no generan por sí mismas consecuencias que afecten de manera irreversible o significativa a los derechos del usuario. Cualquier bloqueo o alerta que derive de este análisis puede ser revisado por un equipo humano, y el usuario tiene la posibilidad de solicitar dicha revisión para garantizar que no se produzcan errores o decisiones equivocadas. De este modo, combinamos la rapidez y eficacia de la detección automática con la supervisión humana necesaria para asegurar un tratamiento justo y conforme al RGPD.

9. Plazos de conservación

La conservación de los datos tratados a través del Servicio se ajusta a los plazos que Ironchip y el Cliente hayan establecido en el contrato de servicio, siempre dentro de los límites

previstos por la legislación aplicable. Con carácter general, los datos asociados a la gestión de cuentas y autenticaciones se mantienen mientras el usuario permanezca activo en el sistema, mientras que los registros técnicos y de seguridad se conservan durante el periodo necesario para garantizar la trazabilidad, la detección de incidentes y el cumplimiento de las obligaciones de seguridad acordadas contractualmente.

No obstante, estos plazos pueden ampliarse cuando exista un motivo legal que así lo exija, como la necesidad de atender requerimientos de autoridades, cumplir obligaciones normativas específicas del sector del Cliente o preservar evidencias relacionadas con investigaciones internas o procedimientos judiciales. En el ámbito del soporte técnico, los datos se conservan únicamente durante el tiempo imprescindible para gestionar la incidencia y durante los periodos derivados de la responsabilidad legal aplicable.

Una vez concluidos los plazos aplicables —contractuales o legales—, Ironchip aplicará los principios de minimización y limitará la conservación conforme al RGPD, procediendo a la supresión de los datos mediante su bloqueo, anonimización o eliminación segura. Estas operaciones se realizarán siguiendo la normativa vigente y los procedimientos definidos en el Sistema de Gestión de Seguridad de la Información y de Privacidad de Ironchip.

10. Destinatarios y comunicaciones de datos

Los datos tratados a través del Servicio pueden ser comunicados únicamente a aquellos terceros cuya intervención resulta imprescindible para garantizar su funcionamiento y para cumplir las obligaciones legales aplicables. En primer lugar, el propio Cliente tiene acceso a la información necesaria para administrar a sus usuarios, supervisar los accesos y cumplir con sus controles internos de seguridad y auditoría, ya que actúa como Responsable del Tratamiento respecto de los datos de sus propios usuarios.

Asimismo, determinados proveedores tecnológicos colaboran con Ironchip en la prestación del Servicio, proporcionando infraestructuras de alojamiento, sistemas de mensajería para factores de autenticación, herramientas de soporte o soluciones técnicas esenciales para la gestión de logs y la continuidad operativa. Estos terceros actúan siempre como Encargados del Tratamiento, sujetos a contratos que cumplen estrictamente con lo previsto en el artículo 28 del RGPD y que les obligan a tratar los datos únicamente para los fines vinculados al Servicio, bajo las instrucciones de Ironchip y con las debidas garantías de seguridad.

En situaciones en las que exista un requerimiento válido por parte de autoridades judiciales, administrativas o de seguridad, Ironchip podrá comunicar aquellos datos que legalmente esté obligado a facilitar, limitándose a lo estrictamente necesario para atender dicho mandato y garantizando en todo momento el cumplimiento del RGPD y de la normativa nacional.

Fuera de estos supuestos, Ironchip no cede datos personales a terceros para finalidades ajenas al Servicio, ni los vende, ni los utiliza para acciones comerciales o de marketing de terceros. El tratamiento de la información se limita exclusivamente a la prestación segura, eficaz y legítima del producto de identidad.

11. Transferencias internacionales

El tratamiento de los datos personales asociado al Servicio se realiza, por defecto, dentro del Espacio Económico Europeo, donde Ironchip mantiene su infraestructura principal y aplica las garantías de seguridad exigidas por la normativa europea. No obstante, es posible que, para prestar determinados componentes del Servicio o para garantizar su continuidad operativa, sea necesario recurrir a proveedores o infraestructuras ubicadas fuera del EEE. En esos casos, cualquier transferencia internacional se llevará a cabo únicamente cuando resulte imprescindible para la prestación del Servicio y siempre bajo mecanismos jurídicos que aseguren un nivel de protección equivalente al exigido por el RGPD. Estos mecanismos pueden incluir decisiones de adecuación, la firma de Cláusulas Contractuales Tipo o la adopción de medidas técnicas adicionales como el cifrado o la seudonimización de la información, asegurando que los datos permanezcan protegidos en todo momento, incluso cuando se encuentren fuera del entorno europeo. Ironchip no realizará transferencias internacionales que no cumplan estrictamente con los requisitos legales aplicables ni que comprometan la seguridad o confidencialidad de los datos tratados.

12. Seguridad de la información

La protección de los datos personales es un elemento central del Servicio y se integra desde su diseño, siguiendo el principio de privacidad por defecto y por construcción establecido en el artículo 25 del RGPD. Con este enfoque, Ironchip aplica un conjunto de medidas técnicas y organizativas concebidas para garantizar la confidencialidad, integridad y disponibilidad de la información en todo momento. El Servicio emplea sistemas de cifrado tanto en las comunicaciones como en los datos almacenados, así como mecanismos de vinculación segura entre el usuario y sus dispositivos para evitar accesos no autorizados.

El tratamiento de la información se basa en criterios estrictos de minimización, de forma que únicamente se procesa aquello que resulta imprescindible para la autenticación y la seguridad, aplicando técnicas de seudonimización o tokenización cuando es posible para reducir aún más la exposición de datos. Estas medidas se complementan con un modelo robusto de gestión de identidades y control de accesos, junto con una supervisión continua orientada a detectar actividades potencialmente anómalas o riesgosas.

El funcionamiento seguro del Servicio se apoya también en un sistema de registro de eventos diseñado para conservar la trazabilidad necesaria en materia de seguridad, así como en pruebas periódicas destinadas a verificar su resistencia frente a amenazas y vulnerabilidades. Además, Ironchip mantiene procedimientos de gestión de incidentes, así como planes de continuidad y recuperación que garantizan el restablecimiento del Servicio ante fallos o contingencias. Todo ello se desarrolla dentro de un marco de cumplimiento alineado con estándares reconocidos internacionalmente, como ISO 27001 e ISO 27701, así como con los requisitos del Esquema Nacional de Seguridad, reforzando el compromiso de Ironchip con un tratamiento seguro y responsable de los datos.

13. Registro de Actividades de Tratamiento

Ironchip mantiene un Registro de Actividades de Tratamiento propio en el que documenta de forma detallada todos los procesos vinculados al funcionamiento del Servicio, cumpliendo así con lo establecido en el artículo 30 del RGPD. Este registro incorpora la información necesaria para demostrar la responsabilidad proactiva del Servicio, describiendo las categorías de datos tratadas, las finalidades asociadas, las bases jurídicas aplicables y las medidas de seguridad que garantizan su protección.

De manera paralela, el Cliente está obligado a mantener su propio Registro de Actividades de Tratamiento respecto de los datos personales de sus usuarios internos, ya que actúa como Responsable del Tratamiento dentro de su organización. Ambos registros deben ser coherentes entre sí en aquellos puntos en los que el flujo de datos dependa de la interacción entre Cliente e Ironchip, especialmente en auditorías, revisiones de conformidad o requerimientos de autoridades de control. Esta coordinación asegura una trazabilidad completa y permite acreditar que cada parte cumple adecuadamente con sus obligaciones legales en materia de protección de datos.

14. Derechos de los usuarios

Los usuarios del Servicio conservan en todo momento los derechos que les reconoce el Reglamento General de Protección de Datos, lo que significa que pueden solicitar a Ironchip información sobre el tratamiento de sus datos personales, corregir aquellos que resulten inexactos, pedir su eliminación cuando ya no sean necesarios o cuando consideren que se han tratado de forma indebida, oponerse a determinados usos o solicitar que el tratamiento se limite en situaciones concretas. También pueden recibir sus datos en un formato estructurado y de uso común para trasladarlos a otro proveedor, así como solicitar la revisión humana de aquellas decisiones que se basen exclusivamente en procesos automatizados cuando puedan afectarles de manera relevante.

Para ejercer cualquiera de estos derechos, basta con dirigirse a Ironchip a través del correo electrónico dpo@ironchip.com o mediante comunicación escrita enviada a la dirección Calle Beurko Viejo, 17 – 48902 Barakaldo (Bizkaia), indicando de forma clara la solicitud que se desea realizar. Ironchip atenderá las peticiones dentro de los plazos y condiciones previstos por el RGPD y la legislación española en materia de protección de datos.

En caso de que el usuario considere que su solicitud no ha sido atendida adecuadamente o que se ha producido alguna vulneración de sus derechos, tiene la posibilidad de presentar una reclamación ante la Agencia Española de Protección de Datos, a través de su sitio web oficial www.aepd.es, sin perjuicio de que pueda contactar previamente con Ironchip para intentar resolver cualquier incidencia de manera directa y eficaz.

15. Cambios y Modificaciones en esta Política

Ironchip podrá modificar esta Política de Privacidad cuando resulte necesario para adaptarla a nuevas obligaciones legales, a criterios actualizados de las autoridades de protección de datos o a mejoras y evoluciones del propio Servicio. Cualquier cambio se incorporará con el propósito de mantener una información precisa y ajustada a la realidad del tratamiento, garantizando que los usuarios y el Cliente disponen siempre de una versión actualizada.
Cuando las modificaciones introduzcan variaciones relevantes en la forma en que se tratan los datos o en las finalidades previstas, Ironchip lo comunicará de forma clara y anticipada tanto al Cliente como a los usuarios afectados, permitiendo que conozcan el alcance de los cambios antes de que entren en vigor. De este modo, se asegura que la relación con el Servicio se mantenga siempre bajo condiciones informadas y conforme al marco jurídico aplicable.

Fecha de Última Actualización: Enero 2026