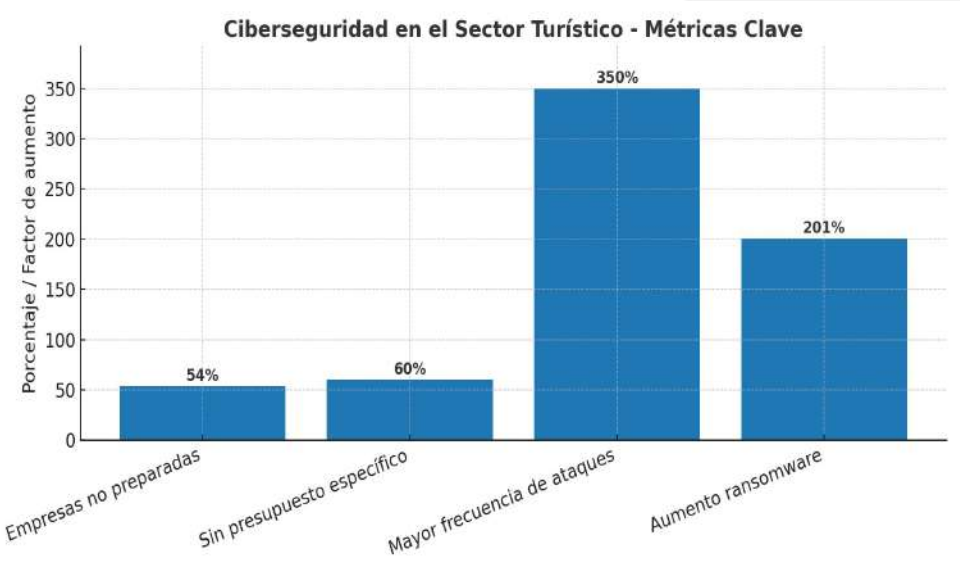
IRONCHIP

Casos de Uso de Ironchip para el sector turístico

Fortaleciendo la Ciberseguridad con tecnología Identity Threat Detection and Response (ITDR)

Un aumento de ataques al sector turístico sin precedentes



PROTECCIÓN AVANZADA DE IDENTIDADES

El sector turístico sigue rezagado en ciberseguridad: el 54 % de las empresas no está preparado para un ciberataque y solo el 40 % cuenta con presupuesto específico. **Sufre 3,5 veces más ataques que otros sectores y los incidentes de ransomware han crecido un 201 % en el último año**.

Casos como **EasyJet, con 9 millones de clientes afectados y más de 2 200 con datos bancarios comprometidos**, o los ataques de ransomware a Carnival y MisterFly, muestran la magnitud del problema. En 2024 se registraron 5 263 ataques graves de ransomware, con rescates medios de 5,2 millones de dólares y picos de hasta 100 millones.

El silencio de las víctimas y la falta de colaboración agravan el riesgo. **Sin inversión y actualización continua, el turismo se convertirá en un objetivo permanente para ciberdelincuentes**: “esto es solo el comienzo”.

¿Por qué Ironchip? Versatilidad , Seguridad y cumplimiento normativo

La gestión de información crítica dentro del sector turístico, bien sean Agencias de Viajes, Touroperadores, hoteles etc.. manejando datos de clientes, expedientes,datos de reservas, exige una protección inquebrantable, a menudo con recursos limitados y equipos muy diversos. Ironchip es el aliado estratégico que ofrece soluciones sin contraseñas, robustas, versátiles y seguras.
Una de las características importantes de la tecnología Ironchip es que está certificada en **LINCE Nivel Alto** y gracias a ellos en el catálogo **CPSTIC** del **CCN** , imprescindible para el cumplimiento del **ENS .**Cumple con los estándares de **ISO/IEC 27001** y buenas prácticas de ciberseguridad.**Alineado con NIS2** (Directiva Europea de Ciberseguridad), clave para entornos críticos.

Versatilidad en Métodos de Autenticación:

- USB, Smart Cards NFC.
- Equipos portátiles y de sobremesa (Windows, Linux, Mac).
- Móviles: Android e iOS.

Naturaleza Totalmente Passwordless: Elimina contraseñas, neutralizando phishing, keylogging y fuerza bruta.

Identity Threat Detection and Response (ITDR): Detección y neutralización automática de robos de cuenta y accesos no autorizados mediante inteligencia de localización y análisis de comportamiento. Frustra ataques de ingeniería social y falsificación de biometría.

IRONCHIP

FINANCIADA POR ENISA

MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

Fortaleciendo la Gobernanza Digital en el sector turismo

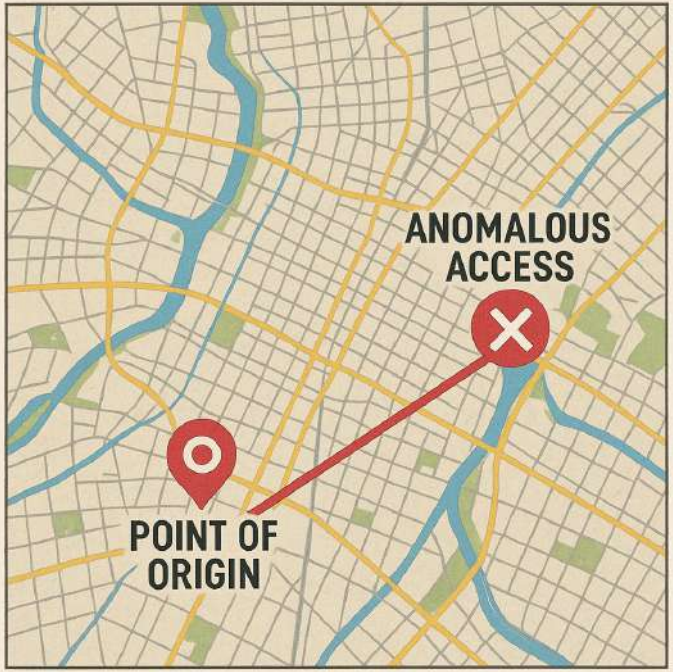
PROTECCIÓN AVANZADA DE IDENTIDADES

Autenticación sin contraseñas, eliminando el riesgo de robo de credenciales. Evitando el 65% del cibercrimen proveniente de toda clase de ingenierías sociales.

Trazabilidad total en cuentas compartidas (recepciones, backoffice), garantizando saber *quién* realizó cada acción en tiempo real, aunque la cuenta esté compartida por varios usuarios, o aunque la cuenta sea única en un dispositivo que usan varias personas a la vez.

Prevención de bloqueos de usuarios en puestos compartidos, reduciendo incidencias y costes operativos, evitando que los cambios de usuario provoquen contraseñas equivocadas que generen bloqueos, dado que puede evitarse el uso de las contraseñas

Control inteligente de Ubicación



VERIFICACIÓN UBICACIONES Y DETECCIÓN DE ROBOS DE CUENTA

Verificación de ubicaciones de acceso: garantiza que cada reserva se realiza desde un origen válido, y facilita el conocimiento exacto de la ubicación de reserva.

Detección proactiva de robos de cuenta (evita reservas falsas o accesos sospechosos desde IPs anómalas). Y además facilita ubicación del defraudador para facilitarla a la autoridad y actuar contra ellos.

Oportunidad de marketing: información valiosa de **desde dónde se hacen las reservas** para estrategias comerciales y segmentación geográfica. Capacidad de conocer los puntos calientes de consumo para realizar acciones promocionales dirigidas.

Experiencia de Usuario Simplificada

FLEXIBILIDAD DE MÉTODOS DE AUTENTICACIÓN

Acceso inmediato con **USB, TARJETA NFC o móvil**, sin recordar contraseñas.

Reducción de fricciones en la operativa diaria del personal.

Facilidad de acceso inmediato sin uso de contraseñas que eviten ser robadas y que eviten olvidos bloqueos o necesidad de cambios continuos de actualización con sus problemas administrativos y de gestión.

IRONCHIP

Caso de uso

Eliminación del riesgo por gestión de contraseñas en puestos de alta rotación

En el sector hotelero, los puestos con alta rotación —como recepcionistas, personal de reservas o temporales— suponen un gran reto para la gestión de credenciales.

El uso de contraseñas tradicionales implica procesos complejos: creación, almacenamiento seguro, reseteos constantes y, en muchos casos, riesgo de contraseñas compartidas o anotadas.

Ironchip elimina este problema al ofrecer autenticación sin contraseñas, reduciendo la carga administrativa, eliminando vulnerabilidades asociadas a credenciales y garantizando una experiencia fluida para cada nuevo empleado desde el primer acceso.

Caso de uso

Autenticación de recepcionistas sin móviles

En muchos hoteles, los recepcionistas no disponen de dispositivos corporativos y el uso de móviles o números personales para autenticación multifactor es una práctica que entra en conflicto con la legislación laboral y con el RGPD.

Esto supone un riesgo importante para la protección de accesos a sistemas internos.

Con Ironchip, los hoteles pueden implementar autenticación segura sin depender de móviles, utilizando dispositivos USB o tarjetas NFC inteligentes que cumplen con los estándares normativos y permiten una experiencia rápida y sin fricciones para el usuario.

IRONCHIP

Caso de uso

Detección de ataques de ingeniería social a empleados del hotel

Los ataques de ingeniería social siguen siendo una amenaza crítica para el sector.

Un escenario común es el vishing, donde un ciberdelincuente suplanta la voz de un directivo para convencer al equipo de TI de enviar un proceso de recuperación de cuenta a un correo personal.

Ironchip, gracias a su tecnología ITDR (Identity Threat Detection and Response), analiza el contexto del acceso y detecta anomalías en la petición, bloqueando automáticamente la acción sospechosa antes de que comprometa las credenciales o los sistemas del hotel.

IRONCHIP

Conclusión: AHORRO Y RETORNO DE INVERSIÓN

Con la tecnología de Ironchip, no solo se alcanzan y superan las exigencias normativas del Esquema Nacional de Seguridad (ENS), y otros reglamentos específicos del sector, sino que las empresas transforman su postura de ciberseguridad de manera proactiva. La solución totalmente passwordless elimina los riesgos inherentes a las contraseñas, como el phishing o la ingeniería social, ofreciendo una flexibilidad inigualable en los métodos de autenticación, adaptándose a cualquier entorno sin depender de aplicaciones móviles corporativas.

Gracias a su avanzada capacidad de Identity Threat Detection and Response (ITDR), Ironchip no solo detecta, sino que bloquea en tiempo real el robo de cuentas y los accesos no deseados, incluso frente a la falsificación de biometría. Esto se traduce en un fortalecimiento integral de la Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad (CITAD) de la información. La confianza en los servicios que el cliente está utilizando hace que la imagen de marca se vea fortalecida con respecto a otros actores.

Your next generation identity

Julio Alfaro- julio.alfaro@ironchip.com
Maria Cobas- maria.cobas@ironchip.com

Paseo de la Castellana , 200 Madrid
Beurko Berria, 17. Barakaldo
info@ironchip.com