Battle **card**

IRONCHIP CYBERSECURITY / yubico

Seguridad: Protección activa, inteligencia contextual y resistencia al fraude

Ironchip

Identity Platform + ITDR

+ **Protección activa (Plugin):** Bloquea AitM, Quishing, VNC y Typosquatting en tiempo real antes de que el usuario firme.
+ **Inteligencia ITDR:** Detecta robos de sesión por ubicación, cambio de SIM y señales RF. Bloqueo automático y reporte al SOC.
+ **Zero-Trust real:** Sin contraseña en el mapa. Autenticación mutua e inteligencia de ubicación como factor contextual.
+ **Sin secreto compartido:** Nada que interceptar, filtrar ni reutilizar. La identidad es contextual, no un dato estático.
+ **Bloqueo automático:** Acceso cortado de inmediato ante cualquier anomalía, sin intervención manual.

Yubico (YubiKey/fido)

Hardware Token

+ **Protección pasiva:** El YubiKey firma cualquier solicitud, incluso sitios fraudulentos. No distingue si el destino es legítimo.
+ **Sin inteligencia contextual:** Si el atacante tiene el hardware, entra sin más contexto. No hay detección de anomalías.
+ **Token robado usable:** Sin PIN configurado, o si el PIN es robado, el token da acceso en cualquier equipo.
+ **Fraude autorizado invisible:** No detecta si el usuario legítimo firma bajo coacción o engaño. Sin validación de intención.
+ **Sin reporte al SOC:** No genera alertas de comportamiento anómalo. La operación de seguridad queda ciega.

Flexibilidad, Enrollment y Compatibilidad: Omnicanalidad, integraciones, movilidad y mantenimiento

Ironchip

Identity Platform + ITDR

+ **Omnicanal:** App móvil, Desktop agent, USB, NFC, SMS y Email. El usuario elige según contexto sin perder seguridad.
+ **Recuperación remota:** El administrador recupera el acceso desde la consola de forma inmediata, sin enviar hardware.
+ **Integraciones totales:** SAML, OIDC, RADIUS, LDAP, SSH, RDP. Cubre apps cloud modernas y sistemas legacy on-premise.
+ **Mobileless nativo:** Funciona sin móvil corporativo. Válido para BYOD y sectores donde no se reparten terminales.
+ **Mantenimiento software:** Actualizaciones instantáneas y gratuitas. Sin desplazamientos ni sustitución de hardware.

Yubico (YubiKey/fido)

Hardware Token

+ **Omnicanalidad nula:** Solo USB físico y NFC. Si el usuario no tiene el token a mano, no puede autenticarse.
+ **Recuperación inexistente:** Requiere 2 llaves físicas registradas de antemano. Sin backup, el acceso queda bloqueado días.
+ **Integraciones limitadas:** Solo WebAuthn / FIDO2 nativo. Sistemas legacy (RADIUS, LDAP, RDP) quedan fuera sin middleware adicional.
+ **Dependencia de hardware:** Sin el token en mano no hay acceso. La movilidad queda condicionada al objeto físico.
+ **Mantenimiento hardware:** Cada fallo requiere sustitución física, envío, re-enrollamiento y tiempo de inactividad.

Coste, Custodia y Certificaciones: TCO, logística ENS, stock y modelo de adquisición

Ironchip

Identity Platform + ITDR

+ **Sin stock físico:** No hay hardware que comprar, almacenar, inventariar ni asegurar físicamente.
+ **Logística ENS digital:** Sin custodia de dispositivos sensibles. Cumple ENS Alto sin gestionar 'plásticos'.
+ **Modelo OpEx (pago por uso):** Coste predecible y escalable. Sin inversión inicial ni costes ocultos de reposición.
+ **Recuperación sin coste extra:** Acceso remoto y gratuito. Sin envío de hardware de repuesto ni tiempo de inactividad.
+ **ENS Alto por diseño:** Segundo factor contextual. Sin degradar el nivel de seguridad en recuperación de cuenta.

Yubico (YubiKey/fido)

Hardware Token

+ **Stock crítico (200–300% extra):** Para cubrir pérdidas, roturas y la regla 1+1 del ENS, hay que comprar el doble o triple.
+ **Logística ENS inviable:** Inventario físico y custodia bajo controles específicos del ENS (op.pl.4). Coste operativo muy alto.
+ **Modelo CAPEX elevado:** Compra inicial + reposición + gestión y custodia. El TCO real supera con creces la alternativa software.
+ **Regla 1+1 obligatoria:** ENS exige mínimo 2 llaves por usuario. Sin backup la recuperación obliga a métodos más débiles.
+ **Sustitución recurrente:** Cada llave perdida o dañada implica compra, envío, re-enrollamiento y tiempo del equipo de IT.

IRONCHIP
Identity Security Platform

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

+34 944 075 954
www.ironchip.com