REF: DOC-CI-2026-YUBIKEY
EDICIÓN: Rev. 2026 Oficial
ÁREA: Ciberseguridad & Identidad Digital

Manual de Despliegue de Llaves de Seguridad FIDO2 / WebAuthn

Autenticación multifactor por hardware, protección antiphishing y configuración en cuentas críticas.

OBJETO Y ALCANCE TÉCNICO

Directrices técnicas para la implementación de llaves criptográficas de hardware (YubiKey 5 Series) en cuentas de Google, Apple ID, gestores de contraseñas y entornos corporativos.

1. Principio Criptográfico Challenge-Response FIDO2

FIDO2 y WebAuthn eliminan las contraseñas compartidas mediante criptografía asimétrica de clave pública (ECC P-256):

• La clave privada reside en el chip de hardware seguro de la llave y jamás abandona el dispositivo ni se transmite por internet.

• Resistencia total al phishing: La firma criptográfica incluye el origen del dominio web (TLS Origin Binding), imposibilitando que una web falsa capture el token.

2. Protocolo de Configuración de Llave Principal y Llave de Respaldo

- [ ] **Vincular siempre dos llaves físicas simultáneas por cada cuenta crítica.**
  Una llave de uso diario (llavero) y una llave de respaldo guardada en caja fuerte.
- [ ] **Configuración de PIN de hardware de 6 a 8 dígitos en la llave.**
  Protege contra accesos no autorizados en caso de pérdida física de la llave.
- [ ] **Registro en gestor de contraseñas principal (Bitwarden, 1Password) y Apple/Google.**
  Desactivar métodos débiles de recuperación por SMS.

MARCO NORMATIVO Y BIBLIOGRAFÍA DE REFERENCIA

* **FIDO2 / WebAuthn Level 3:** Web Authentication: An API for accessing Public Key Credentials — W3C / FIDO Alliance
* **NIST SP 800-63B:** Digital Identity Guidelines: Authentication and Lifecycle Management (AAL3) — NIST

RECURSOS Y ASISTENCIA TÉCNICA: Consultar Asesor IA en Telegram — Ver análisis completo en CandadoInteligente.com