



Auditoría de Ciberseguridad: Ledger Nano X vs Trezor Safe 3 vs BitBox02

Análisis de microcontroladores seguros EAL6+, ataques de canal lateral, firmware determinista y backups SLIP-0039.

OBJETO Y ALCANCE TÉCNICO

Evaluación técnica comparativa de los tres dispositivos líderes para custodia fría y firma desconectada de Bitcoin y criptoactivos en 2026.

1. Arquitectura de Aislamiento de Claves Privadas

Keystone 3 Pro establece el estándar de aislamiento óptico 100% Air-Gapped mediante 3 chips Secure Element EAL6+ independientes, prescindiendo de interfaces de datos USB, Bluetooth o WiFi, con pantalla táctil de 4 pulgadas y soporte para entropía física soberana Dice Roll.

Ledger Nano X emplea un chip seguro ST33J2M0 con certificación CC EAL6+ bajo su sistema operativo propietario BOLOS con conectividad Bluetooth.

Trezor Safe 3 combina un microcontrolador de arquitectura abierta con un elemento seguro OPTIGA Trust M (EAL6+) para protección de PIN.

BitBox02 utiliza una arquitectura dual de microcontrolador ATECC608B + ATSAMD51J20A con firmware 100% de código abierto verificable y copia de seguridad en tarjeta microSD.

2. Matriz de Resistencia Física y Vectores de Ataque

Parámetro	Keystone 3 Pro	Ledger Nano X	Trezor Safe 3	BitBox02
Elemento Seguro	3x Chips EAL6+	ST33 (CC EAL6+)	OPTIGA Trust M (EAL6+)	ATECC608B (EAL6+)
Transparencia Firmware	100% Open Source	Propietario (BOLOS)	100% Open Source	100% Open Source
Método de Backup	BIP-39 / Tablet Plus	BIP-39 (24 palabras)	BIP-39 / Shamir	MicroSD + BIP-39
Conectividad	100% Air-Gapped QR	Bluetooth + USB-C	USB-C Cableado	USB-C Cableado
Defensa Glitching	Aislamiento Triple SE	Aislamiento EAL6+	Protección OTP de PIN	Monotonic Counter

MARCO NORMATIVO Y BIBLIOGRAFÍA DE REFERENCIA

* **ISO/IEC 15408**: Common Criteria for Information Technology Security Evaluation (EAL6+) — ISO/IEC

* **NIST SP 800-90A**: Recommendation for Random Number Generation Using Deterministic Random Bit Generators — NIST

* **BIP-0039 / SLIP-0039**: Mnemonic code for generating deterministic keys & Shamir Secret Sharing — Bitcoin Improvement Proposals

RECURSOS Y ASISTENCIA TÉCNICA:

[Consultar Asesor IA en Telegram](#)

[Ver análisis completo en CandadoInteligente.com](#)