



Manual Técnico: Configuración Segura de Hardware Wallets y Conectividad Web3

Guía oficial de derivación de claves BIP-32/BIP-44, passphrases ocultas, Clear Signing y conexión a MetaMask, Rabby y Sparrow.

OBJETO Y ALCANCE TÉCNICO

Protocolo de laboratorio para inicialización determinista de hardware wallets, aislamiento de claves privadas y mitigación de ataques de drenado de contratos inteligentes.

1. Protocolo Criptográfico de Derivación y Aislamiento

La generación de claves deterministas jerárquicas (BIP-32 / BIP-44) permite derivar infinitas direcciones públicas y privadas a partir de una única semilla de 256 bits generada por el TRNG de silicio seguro.

El estándar de propósito m/44'/60'/0'/0 (Ethereum) y m/84'/0'/0' (Bitcoin Native SegWit) garantiza que el signer físico solo estampe firmas en curvas elípticas secp256k1 sin emitir jamás las claves maestras.

La técnica de la Passphrase (palabra 25) crea una cuenta señuelo con el PIN primario y una bóveda oculta independiente ante asaltos físicos.

2. Matriz de Conectividad con Clientes Web3 y Suites Oficiales

Software Cliente	Protocolo Conexión	Redes Principales	Ventaja Crítica de Seguridad
Rabby Wallet	WebHID / USB-C Directo	Ethereum, Arbitrum, EVM	Simulación previa de saldos y alerta de contratos maliciosos
Sparrow Wallet	USB-C / Tor / Nodo Local	Bitcoin Core / Liquid	Control exhaustivo de UTXOs y transacciones PSBT
Phantom Wallet	Bluetooth BLE / WebHID	Solana, Ethereum, Bitcoin	Filtro anti-spam de tokens y confirmación física obligatoria
Trezor Suite	Trezor Bridge / WebUSB	Multichain (+9.000 tokens)	Código 100% abierto auditable y soporte Shamir SLIP-39

3. Lista de Verificación Obligatoria para Firmas Web3

- ☐ **Conectar la hardware wallet seleccionando exclusivamente "Connect Hardware Wallet" en la extensión.**
Jamás escribas tus 12 o 24 palabras en un formulario web o extensión del navegador.
- ☐ **Cotejar en la pantalla física la dirección completa y la función de contrato antes de pulsar aprobar.**
Neutraliza ataques de inyección en portapapeles y sitios web de phishing que suplantan interfaces.
- ☐ **Auditar periódicamente y revocar aprobaciones infinitas (Token Allowances) en contratos desusados.**
Utiliza herramientas como Revoke.cash para cerrar puertas traseras en contratos antiguos.
- ☐ **Respalidar las 24 palabras en cápsulas de acero inoxidable AISI 303 o placas de titanio (1.400 °C).**
Elimina el punto único de fallo de la celulosa frente a incendios e inundaciones domésticas.

MARCO NORMATIVO Y BIBLIOGRAFÍA DE REFERENCIA

- * **BIP-0039 / BIP-0044:** Multi-Account Hierarchy for Deterministic Wallets & Mnemonic Codes — Bitcoin Core
- * **EIP-712:** Ethereum Typed Structured Data Hashing and Signing — Ethereum Foundation
- * **NIST SP 800-57:** Recommendation for Key Management — Cryptographic Key Generation — NIST

RECURSOS Y ASISTENCIA TÉCNICA:

[Consultar Asesor IA en Telegram](#)

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