2026 EDITION

THE CRYPTO AND WEB3 USER MISTAKES PREVENTION GUIDEBOOK

DO'S

DON'TS

Avoiding Costly Mistakes: A Practical Guide to Protecting Your Blockchain-Based Assets

JUAN PABLO RENEDO

Guía de prevención de errores de usuario en cripto y Web3

Cómo evitar errores costosos: guía práctica para proteger tus activos basados en blockchain

Edición 2026

Juan Pablo Renedo

CryptoSafetyFirst.com

Derechos de autor y aviso legal

Edición 2026 (versión 2026.1, contenido revisado en octubre de 2026). Primera edición: 2025.

Copyright © 2025–2026 Juan Pablo Renedo. Todos los derechos reservados.

Publicado por Juan Pablo Renedo, c/o Block Services, Stuttgarter Str. 106, 70736 Fellbach, Alemania · contact@cryptosafetyfirst.com

Ninguna parte de esta publicación puede modificarse, venderse, incluirse en productos o servicios de pago, ni reproducirse en extractos sin el permiso previo por escrito del editor. Puedes compartir esta guía de forma gratuita, completa y sin modificaciones, incluido este aviso de derechos de autor. Cualquier otra reproducción, distribución o modificación de esta obra, incluida la copia de imágenes, textos u otros materiales, puede infringir los derechos del autor según la Ley alemana de derechos de autor (UrhG) y puede tener consecuencias legales, incluidos requerimientos con costas y reclamaciones de daños y perjuicios según los §§ 97, 97a UrhG. Las excepciones legales, como la cita (§ 51 UrhG), no se ven afectadas. Esta guía se ofrece como descarga gratuita en CryptoSafetyFirst.com, donde siempre está disponible la versión actual.

Exención de responsabilidad. El autor y el editor no ofrecen declaraciones ni garantías sobre la exactitud, integridad o actualidad de la información contenida en este libro. Aunque se ha hecho todo lo posible para garantizar su fiabilidad, en la medida permitida por la ley no se asume ninguna responsabilidad por daños, pérdidas o consecuencias directos o indirectos derivados del uso de la información presentada. Esto no se aplica en casos de dolo, negligencia grave o daños a la vida, la integridad física o la salud.

Este libro tiene fines exclusivamente educativos e informativos. Las opiniones expresadas reflejan la perspectiva personal del autor y no constituyen asesoramiento financiero, recomendaciones de inversión ni asesoramiento jurídico. Nada de esta publicación constituye asesoramiento financiero, fiscal, jurídico o de inversión en ningún marco regulatorio, incluida la Ley alemana del mercado de valores (WpHG). Los lectores deben investigar por su cuenta y consultar a un profesional cualificado antes de tomar decisiones financieras o de inversión.

Esta publicación puede hacer referencia a sitios web, productos y servicios de terceros. El autor y el editor no son responsables de su contenido, disponibilidad o exactitud, y una mención no es una recomendación. Las marcas comerciales y los nombres de marca pertenecen a sus respectivos propietarios. Los escenarios de este libro son ilustrativos salvo que se indique lo contrario; cualquier parecido con personas concretas es pura coincidencia.

Índice

Derechos de autor y aviso legal 3
Índice 4
Sobre esta edición 7
Cómo usar este libro 9
Si algo acaba de salir mal 11
Configuración de billeteras y elección de custodia 15
1.1 Quién tiene las claves 16
1.2 Divide tus fondos según su uso: The Three-Wallet Model® 17
1.3 Errores de configuración que debes conocer 17
1.4 Cuando el problema es la plataforma 19
1.5 Escenario ilustrativo: la billetera del airdrop 19
1.6 Reglas CSF de este capítulo 20
1.7 Si esto te acaba de pasar 21
Frase semilla y copias de seguridad 23
2.1 Frase semilla, clave privada y passphrase explicadas de forma sencilla 24
2.2 Errores con la copia de la frase semilla que debes conocer 25
2.3 Métodos de copia de seguridad comparados 26
2.4 Cantidades mayores: cuando una sola frase semilla no basta 27
2.5 Escenario ilustrativo: la mudanza 28
2.6 Cómo proteger la copia de tu frase semilla 28
2.7 Reglas CSF de este capítulo 29
2.8 Si esto te acaba de pasar 30
Contraseñas, PIN, 2FA y dispositivos 32
3.1 Las capas de acceso alrededor de tu billetera 33
3.2 Errores de acceso que debes conocer 34
3.3 Escenario ilustrativo: el teléfono nuevo 35
3.4 Cómo proteger tu acceso 36

3.5 Reglas CSF de este capítulo 37
3.6 Si esto te acaba de pasar 38
Dirección equivocada 40
4.1 Lo que tu billetera puede detectar y lo que no 41
4.2 Errores con direcciones que debes conocer 42
4.3 Escenario ilustrativo: la dirección del año pasado 44
4.4 Una rutina de envío para cada transferencia 44
4.5 Reglas CSF de este capítulo 45
4.6 Si esto te acaba de pasar 46
Red, token o memo equivocados 48
5.1 Qué errores todavía tienen solución 49
5.2 Errores de red, token y memo que debes conocer 50
5.3 Escenario ilustrativo: la red más barata 52
5.4 Comprueba la red, el token y el memo antes de cada transferencia 52
5.5 Reglas CSF de este capítulo 53
5.6 Si esto te acaba de pasar 54
Errores en transacciones: comisiones, transacciones atascadas y deslizamiento 56
6.1 Los términos de comisiones y transacciones que importan 57
6.2 Errores en transacciones que debes conocer 58
6.3 Escenario ilustrativo: el pago doble 60
6.4 Antes de confirmar una transacción 60
6.5 Reglas CSF de este capítulo 61
6.6 Si esto te acaba de pasar 62
Actualizaciones y mantenimiento 64
7.1 Un único calendario de revisión para tu configuración 65
7.2 Errores de mantenimiento que debes conocer 66
7.3 Mantenlo lo bastante simple para usarlo bajo estrés 67
7.4 Escenario ilustrativo: la actualización que pedía las palabras 68

7.5 Reglas CSF de este capítulo 69
7.6 Si esto te acaba de pasar 69
Herencia y acceso de emergencia 72
8.1 Lo que tu familia necesita y lo que todavía no debe tener 73
8.2 Errores de herencia que debes conocer 74
8.3 Opciones de acceso compartido o diferido 75
8.4 Un plan en cinco pasos 76
8.5 Escenario ilustrativo: dos tipos de cripto 77
8.6 Reglas CSF de este capítulo 78
8.7 Si esto te acaba de pasar 79
Registros e impuestos 81
9.1 Los registros que vale la pena conservar 82
9.2 Errores al llevar registros que debes conocer 83
9.3 Escenario ilustrativo: el exchange que cerró 84
9.4 Reglas CSF de este capítulo 85
9.5 Si esto te acaba de pasar 86
Índice de reglas CSF 88
Sigue aprendiendo 90

Sobre esta edición

La primera edición de esta guía describía once errores comunes. Desde entonces, CryptoSafetyFirst ha recopilado y clasificado cada semana pérdidas reales comunicadas por usuarios de cripto, y la mayoría no necesitó ningún hacker: una copia de seguridad perdida, una red equivocada, un plan que no existía. La Edición 2026 se ha reconstruido en torno a lo que muestra ese trabajo.

Novedades

- **Nueve capítulos en tres grupos** (acceso y copias de seguridad, transacciones, mantenimiento y planificación), según la taxonomía de incidentes de CSF, para que el libro, el sitio web y las reglas CSF usen las mismas categorías.
- **Una sección "Empieza aquí"** para quien acaba de cometer un error. Te dice qué hacer según lo que realmente pasó: red equivocada, dirección equivocada, transacción atascada, acceso perdido o una copia de seguridad que falta.
- **Capítulos nuevos** sobre red, token o memo equivocados (a menudo recuperables) y sobre registros e impuestos.
- **Reglas CSF en cada capítulo,** con una regla principal por error y las reglas complementarias que la respaldan.
- **Consejos corregidos y actualizados,** entre ellos dos copias sin conexión (offline) en lugar de una, copias de seguridad de la 2FA que no dependen de un solo teléfono y un único calendario de revisión cada tres meses.

Cómo se tratan los ejemplos y los datos

- Los escenarios son ilustrativos salvo que se indique claramente lo contrario. Muestran patrones reales sin nombrar personas, proyectos ni cifras de pérdidas reales.
- El libro no contiene estadísticas de incidentes, así que sus consejos siguen siendo válidos aunque cambien las cifras.
- Esta edición usa las Reglas CSF v2, publicadas en CryptoSafetyFirst.com.
- Las herramientas y los servicios se mencionan solo como ejemplos y se comprobaron en octubre de 2026. Los servicios cambian; si tienes dudas, entra tú mismo en el sitio web oficial del proveedor.

- El capítulo 9 explica qué registros conservar. No es asesoramiento fiscal: las normas fiscales varían según el país. Comprueba las normas de donde vives o consulta a un asesor fiscal.

Cómo usar este libro

Si…	Ve a
acabas de cometer un error: red equivocada, dirección equivocada, transacción atascada o acceso perdido	Empieza aquí: Si algo acaba de salir mal; después, el capítulo de tu situación.
estás configurando tus billeteras	Capítulos 1–3 y la guía de The Three-Wallet Model (Modelo de Tres Billeteras), gratuita en CryptoSafetyFirst.com. Este libro usa sus términos: Bóveda, billetera de Uso Frecuente y billetera Desechable.
envías cripto con regularidad	Capítulos 4–6: direcciones, redes y transacciones.
guardas cripto a largo plazo	Capítulos 7–9: mantenimiento, herencia y registros.

Por dónde empezar

Cómo funciona cada capítulo

Todos los capítulos siguen la misma estructura, para que encuentres rápido lo que necesitas: una infografía de un vistazo, los errores que debes conocer, un escenario ilustrativo, cómo protegerte, las reglas CSF para ese error y Si esto te acaba de pasar, con las primeras acciones de ese capítulo. Cada capítulo termina con un enlace a su página en CryptoSafetyFirst.com. Los nueve capítulos forman tres grupos: Errores de acceso y copias de seguridad (1–3), Errores en transacciones (4–6) y Errores de mantenimiento y planificación (7–9).

Los enlaces de esta guía llevan a CryptoSafetyFirst.com, que de momento está en inglés. Puedes leer cualquier página en español con la traducción automática de tu navegador (por ejemplo, en Chrome o Edge: clic derecho → «Traducir al español»; en Safari, el botón de traducción de la barra de direcciones).

Cap.	Capítulo	Suele combinarse con	Regla CSF principal
1	Configuración de billeteras y elección de custodia	2, 7; guía de estafas (aplicaciones falsas)	GR-008
2	Frase semilla y copias de seguridad	3, 7, 8	OR-002
3	Contraseñas, PIN, 2FA y dispositivos	2, 7; guía de hackeos (SIM swap)	OR-006
4	Dirección equivocada	5, 6; guía de estafas (envenenamiento de direcciones)	OR-005
5	Red, token o memo equivocados	4, 6	OR-005
6	Errores en transacciones: comisiones, transacciones atascadas y deslizamiento	4, 5	GR-006
7	Actualizaciones y mantenimiento	2, 3, 8	OR-001
8	Herencia y acceso de emergencia	2, 7, 9	OR-007
9	Registros e impuestos	8	Hábito clave

Mapa de capítulos: cómo se relacionan los errores

Los errores rara vez llegan solos. Una configuración sin plan lleva a perder copias de seguridad; una copia perdida deja a los herederos sin acceso; una transferencia hecha con prisa acaba en la red o la dirección equivocadas. El mapa de capítulos muestra las combinaciones más comunes, para que puedas leer los capítulos que van juntos.

EMPIEZA AQUÍ

Si algo acaba de salir mal

Lo que debes hacer a continuación depende de lo que realmente pasó. Enviar por la red equivocada no es lo mismo que enviar a la dirección equivocada; una transacción atascada no es lo mismo que una fallida; perder el teléfono no es lo mismo que perder la frase semilla (frase de recuperación). Algunas de estas situaciones todavía tienen solución, pero solo si no las empeoras antes.

Busca la fila que corresponde a lo que pasó. Cada fila indica qué hacer ahora y lo que esa acción no soluciona.

Qué pasó	Qué hacer ahora	Lo que esto no soluciona
Enviaste cripto por la red equivocada, elegiste la versión equivocada del token u omitiste un memo o una etiqueta (tag)	Detente y no envíes más. Busca la transacción en el explorador de la red que usaste realmente y guarda el hash de la transacción. Si controlas la dirección receptora, añade esa red en tu billetera: a menudo los fondos ya están ahí. Si se envió a un exchange (plataforma de intercambio), abre una solicitud de soporte (ticket) a través de su app o sitio web oficial con el hash, la red y el memo. Consulta el capítulo 5.	La recuperación depende de quien controle la dirección receptora. Un exchange puede negarse o cobrar una comisión; ningún servicio externo puede hacerlo por ti.
Enviaste cripto a la dirección equivocada	Guarda el hash de la transacción. Comprueba si la dirección te pertenece (otra billetera o cuenta), si es de un exchange (ponte en contacto con él a través de su sitio web oficial) o si es un contrato. Consulta el capítulo 4.	Una transferencia confirmada no se puede revertir. Nadie puede recuperarla a cambio de una comisión.
Tu transacción está atascada como pendiente	No vuelvas a enviar el mismo pago. Usa “acelerar” o “cancelar” en la billetera desde la que lo enviaste. Si no te queda gas, añade primero una pequeña cantidad del token nativo de la red. Consulta el capítulo 6.	Acelerar o cancelar solo funciona mientras la transacción sigue pendiente.

Qué pasó	Qué hacer ahora	Lo que esto no soluciona
Un swap (intercambio de tokens) devolvió muchos menos tokens, o una transacción fallida costó igualmente una comisión	Comprueba la configuración de deslizamiento (slippage) y el “mínimo recibido” en tu próximo swap. Usa la comisión sugerida y mantén un pequeño saldo de gas. Consulta el capítulo 6.	Las comisiones de las transacciones fallidas y las pérdidas por deslizamiento no se pueden reembolsar.
Tu billetera todavía se abre, pero no encuentras la frase semilla	Actúa ahora, mientras el dispositivo todavía funciona: crea una billetera nueva, anota su nueva frase semilla dos veces y guarda las copias en lugares separados; después, mueve tus fondos a ella. Consulta el capítulo 2.	Si el dispositivo falla antes de que lo hagas, los fondos no se pueden recuperar.
Tu teléfono, tu equipo o tu billetera de hardware (hardware wallet) se perdió, se rompió o se restableció	Restaura la billetera con tu frase semilla (y tu passphrase [frase de contraseña adicional], si configuraste una) en un dispositivo nuevo o restablecido. En una billetera de hardware, introduce las palabras solo en la propia pantalla del dispositivo; en una billetera de software, solo en su app oficial. Comprueba que aparecen las mismas direcciones. Consulta los capítulos 2 y 3.	Sin la frase semilla, ninguna empresa puede restaurar una billetera de autocustodia (self-custody).
Olvidaste tu PIN, o una billetera de hardware se restableció tras varios intentos fallidos	Restaura el dispositivo con tu frase semilla (y tu passphrase). Después, guarda el nuevo PIN donde puedas encontrarlo. Consulta el capítulo 3.	Sin la frase semilla, una billetera de hardware restablecida no se puede recuperar.
Perdiste el teléfono de tu 2FA o no puedes iniciar sesión en un exchange	Usa tus códigos de respaldo de 2FA. Si no tienes ninguno, usa la recuperación de cuenta oficial del exchange, solo a través de su propio sitio web o app. Protege primero tu cuenta de correo electrónico. Consulta el capítulo 3.	La recuperación oficial puede tardar días o semanas. Cualquiera que te ofrezca una vía más rápida es un estafador.

Qué pasó	Qué hacer ahora	Lo que esto no soluciona
Puede que alguien haya visto o fotografiado tu frase semilla, o que la hayas introducido en un sitio web	Considera la billetera comprometida. En un dispositivo de confianza, crea una billetera nueva con una frase semilla nueva y mueve todos los fondos a ella ahora. Consulta el capítulo 2.	Cambiar un PIN o una contraseña no hace que una frase semilla expuesta vuelva a ser segura.
Restauraste una billetera y muestra saldo cero	No te asustes: normalmente los fondos siguen ahí. Comprueba la passphrase, la app de la billetera y la ruta de derivación (derivation path), la red, y las palabras exactas y su orden. Consulta los capítulos 2 y 7.	Una sola palabra equivocada puede abrir otra billetera distinta y vacía. Nadie puede “encontrar” los fondos por ti.
Alguien ha fallecido o no puede actuar, y la familia necesita acceso	No publiques detalles y no pagues a nadie que se ofrezca a recuperar los fondos. Reúne los documentos. Ponte en contacto con los exchanges a través de su proceso oficial para clientes fallecidos o de recuperación de cuentas. En el caso de la autocustodia, sigue el plan de recuperación si existe. Consulta el capítulo 8.	Sin la información de recuperación, nadie puede abrir una billetera de autocustodia.
Un exchange cerró o falta tu historial de transacciones al llegar la declaración de impuestos	Exporta lo que todavía esté disponible, usa exploradores de bloques para el historial on-chain y reconstruye el resto con tus registros bancarios. Consulta a un asesor fiscal. Consulta el capítulo 9.	Los datos perdidos de un exchange normalmente no se pueden recuperar. Este libro no es asesoramiento fiscal.
Alguien se ofrece a recuperar tus cripto	Trátalo como una estafa. No pagues comisiones por adelantado, no compartas tu frase semilla y no instales software de acceso remoto. Denuncia el contacto.	Nadie puede revertir una transferencia confirmada ni recuperar una frase semilla perdida a cambio de una comisión.

Tabla 1: Qué hacer a continuación, según lo que pasó

Si se aplica más de una situación

Sigue primero la respuesta para la situación más grave. Por ejemplo, si se rompió tu teléfono y además no encuentras la frase semilla, nada más importa hasta que sepas dónde está la frase semilla. Si tu frase semilla puede haber estado expuesta, mueve los fondos antes de ocuparte de cualquier otra cosa.

DÓNDE CONSEGUIR AYUDA

Quienes ayudan de forma legítima nunca te piden tu frase semilla, tu clave privada, acceso remoto a tu dispositivo ni una comisión por adelantado para recuperar fondos.

- El soporte oficial del proveedor de tu billetera, al que llegas escribiendo tú mismo su sitio web oficial, nunca a través de enlaces en mensajes o anuncios patrocinados.
- El exchange o servicio involucrado, a través de su app o sitio web oficial.
- Para pérdidas causadas por estafas o robos: la policía local o el servicio nacional de denuncia de ciberdelitos. Enlaces por país: **cryptosafetyfirst.com/how-to-report-a-crypto-scam/ (en inglés)**

CUIDADO CON LAS ESTAFAS DE RECUPERACIÓN

Después de un error o una pérdida, es posible que se pongan en contacto contigo personas que dicen poder rastrear, desbloquear o recuperar tus cripto. Trata toda oferta de recuperación no solicitada como una estafa. No compartas tu frase semilla ni tu clave privada, y no pagues a nadie que diga que hace falta una comisión para liberar tus fondos. Consulta **Estafas de recuperación** en la **Guía de prevención de estafas**.

Lo que estas acciones no pueden deshacer

- Nadie puede revertir una transferencia confirmada.
- Acelerar o cancelar solo funciona mientras una transacción sigue pendiente.
- Un PIN o una contraseña nuevos no hacen que una frase semilla expuesta vuelva a ser segura.
- Ninguna empresa puede recuperar una frase semilla perdida de una billetera de autocustodia.

CAPÍTULO 1

Configuración de billeteras y elección de custodia

“Una sola billetera, una mala firma y todo desapareció.”

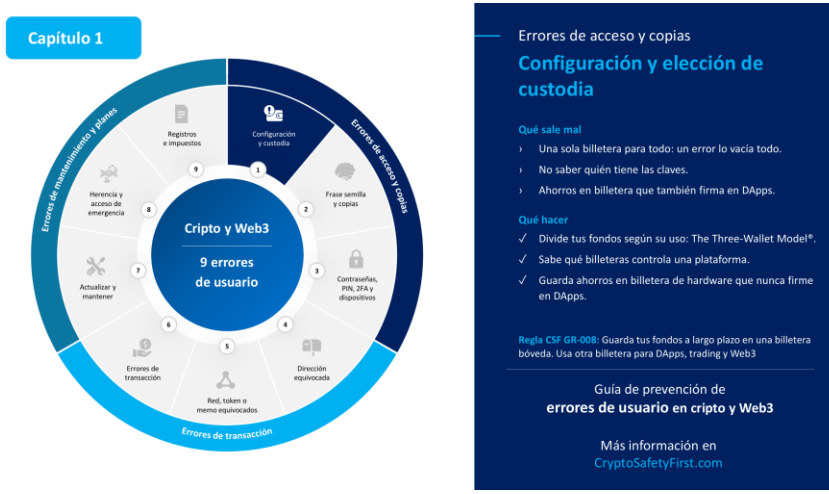

Figura 1.1: Configuración de billeteras y elección de custodia de un vistazo

Antes de cualquier estafa, hackeo o errata, hay una decisión que la mayoría de las personas nunca toma de forma consciente: dónde están sus cripto y quién las controla. Una sola billetera para todo, ahorros dejados en un exchange (plataforma de intercambio) o una billetera a largo plazo que también firma en cada app nueva: cada una de estas opciones convierte un solo error en una pérdida total.

Este capítulo trata las dos decisiones de configuración que determinan cuánto puede costar cualquier error posterior: quién tiene las claves y cómo se dividen tus fondos según su uso. El método completo está en la guía gratuita **Three-Wallet Model®** (Modelo de Tres Billeteras); este capítulo trata los errores.

EN ESTE CAPÍTULO

- 1.1 Quién tiene las claves
- 1.2 Divide tus fondos según su uso: The Three-Wallet Model®
- 1.3 Errores de configuración que debes conocer
- 1.4 Cuando el problema es la plataforma
- 1.5 Escenario ilustrativo: la billetera del airdrop
- 1.6 Reglas CSF de este capítulo
- 1.7 Si esto te acaba de pasar

1.1 Quién tiene las claves

Cada lugar donde guardas cripto es una cuenta custodiada, donde una plataforma tiene las claves, o una billetera de autocustodia (self-custody), donde las tienes tú. Ninguna es segura por defecto; fallan de formas distintas:

Pregunta	Cuenta custodiada (exchange, app)	Billetera de autocustodia
¿Quién tiene las claves?	La plataforma (**billetera custodiada**)	Tú, mediante tu frase semilla (frase de recuperación); es una **billetera no custodiada** (non-custodial)
Si pierdes el acceso	Recuperación de la cuenta con la plataforma: correo electrónico, 2FA, verificaciones de identidad	Solo tu frase semilla restaura la billetera (**capítulo 2**)
¿Quién puede bloquear tus fondos?	La plataforma: congelaciones, bloqueos por verificación de identidad, retiradas de cotización (delisting), insolvencia	Nadie, pero tampoco nadie puede ayudarte
Qué debes respaldar	Contraseña, códigos de respaldo de 2FA, la cuenta de correo electrónico (**capítulo 3**)	Frase semilla (y passphrase [frase de contraseña adicional]), datos de la billetera
Si el proveedor desaparece	Los fondos pueden congelarse o perderse en una insolvencia	Tu frase semilla funciona en otras aplicaciones de billetera compatibles

Tabla 1.1: Cuenta custodiada frente a billetera de autocustodia

1.2 Divide tus fondos según su uso: The Three-Wallet Model®

The Three-Wallet Model® separa las cripto según su uso, para que los riesgos de la actividad diaria nunca lleguen a tus ahorros. Los pasos de configuración y las listas de comprobación están en la guía gratuita **Three-Wallet Model®** y en el **artículo de configuración**.

Billetera	Úsala para	Reglas prácticas
Billetera Bóveda	Ahorros a largo plazo	Una **billetera de hardware (hardware wallet)** comprada al fabricante. Se usa poco, nunca se conecta a DApps y la copia de su frase semilla se guarda sin conexión (offline).
Billetera de Uso Frecuente	Transferencias diarias y las aplicaciones en las que confías	Solo tiene lo que necesitas para tu actividad actual. Revisa sus aprobaciones con regularidad.
Billetera Desechable	DApps nuevas, mints, airdrops y cualquier cosa desconocida	Saldo casi nulo. Sustitúyela en lugar de dejar que crezca; dala de baja cuando haya cumplido su función.
Cuenta en un exchange	Comprar, vender y hacer trading	Un punto de tránsito, no un hogar: retira lo que no estés usando activamente para operar.

Tabla 1.2: The Three-Wallet Model® de un vistazo

1.3 Errores de configuración que debes conocer

1. Una sola billetera para todo

La mayoría de las personas empieza con una sola aplicación de billetera y la usa para los ahorros, el trading, los NFT y cada aplicación nueva. Cada conexión y cada aprobación exponen todo lo que hay en ella. Divide tus fondos según su uso para que una firma equivocada solo alcance a la billetera que la hizo.

2. No saber quién tiene las claves

Un saldo en un exchange, una “billetera” dentro de la aplicación de un exchange y una billetera de autocustodia se parecen en pantalla, pero funcionan de forma muy distinta. Ten claro, para cada una, si tú tienes la frase semilla o si la plataforma tiene las claves: eso decide cómo haces la copia de seguridad y quién puede bloquearla.

3. Dejar los ahorros a largo plazo en un exchange

Los exchanges son útiles para comprar y vender. Como lugar para guardar a largo plazo, añaden un riesgo que no puedes controlar: retiros congelados, bloqueos por verificación de identidad, monedas retiradas de cotización o una insolvencia. Guarda en un exchange solo lo que estés usando activamente para operar.

4. Una billetera Bóveda que firma en DApps

La billetera que guarda tus ahorros no debe conectarse a aplicaciones nuevas, hacer mint de NFT ni reclamar airdrops. En cuanto firma una sola transacción o aprobación maliciosa, los ahorros quedan expuestos. Reserva la billetera Bóveda para transferencias poco frecuentes y deliberadas.

5. Una billetera de hardware de origen equivocado

Una billetera de hardware comprada en un mercado en línea, a un revendedor o a un vendedor de segunda mano puede estar manipulada o venir con una frase semilla ya configurada, y quien preparó esa frase semilla controla la billetera. Cómprala directamente al fabricante y crea tú mismo la frase semilla. Consulta **Aplicaciones y billeteras falsas**.

6. Muchas billeteras sin un registro

Dividir los fondos es bueno; olvidar dónde están, no. Las billeteras de teléfonos antiguos, de configuraciones de prueba y de airdrops acumulan pequeños saldos que nadie vigila. Mantén una sola lista de billeteras con la función de cada una, su dispositivo y el lugar donde está su copia de seguridad.

7. Una billetera Desechable que crece

Una billetera pensada para experimentos acumula poco a poco tokens, NFT y aprobaciones hasta que guarda un valor real. Mueve todo lo que

valga la pena conservar a tu billetera de Uso Frecuente o a tu billetera Bóveda, y sustituye la billetera Desechable en lugar de dejar que crezca.

8. Creer que la autocustodia significa que nada puede salir mal

La autocustodia elimina el riesgo de la plataforma, no todos los riesgos. Las aplicaciones de billetera pueden dejar de ofrecerse (en ese caso, tu frase semilla funciona en otra aplicación compatible) y algunas billeteras usan sus propios métodos de recuperación en lugar de una frase semilla estándar. Averigua cómo se recupera tu billetera antes de poner fondos en ella.

1.4 Cuando el problema es la plataforma

Los usuarios de cuentas custodiadas pierden el acceso de formas que los usuarios de autocustodia nunca ven: retiros pausados por "mantenimiento", una verificación de identidad que nunca termina, una moneda retirada de cotización o una plataforma que quiebra.

- Retira a tu propia billetera lo que no estés usando activamente para operar.
- Activa una **lista blanca de retiros** para que los fondos solo puedan ir a tus propias direcciones.
- Protege la cuenta y su correo electrónico con una **llave de seguridad de hardware**.
- Descarga tu historial de transacciones con regularidad: desaparece con la plataforma (**capítulo 9**).
- En la UE, los proveedores de servicios de criptoactivos necesitan autorización según el Reglamento MiCA; comprueba la plataforma en el registro oficial antes de depositar.

1.5 Escenario ilustrativo: la billetera del airdrop

Este es un escenario ilustrativo, no un caso concreto denunciado.

Daniel guarda sus ahorros y su trading diario en la misma billetera de navegador. Una noche reclama un airdrop de tokens anunciado en redes sociales y firma lo que parece una aprobación rutinaria. En pocos minutos, todos los tokens de la billetera desaparecen.

Qué pasó

El airdrop falso era una estafa. Lo que lo convirtió en una pérdida total fue la configuración: la billetera que firmó la aprobación también guardaba sus ahorros. Con una billetera Desechable para reclamarlo, no habría perdido casi nada.

Conclusiones clave

- Guarda los ahorros en una billetera Bóveda que nunca se conecte a DApps.
- Usa una billetera Desechable para los airdrops y las aplicaciones nuevas.
- Trata por defecto como sospechosos los airdrops inesperados.

1.6 Reglas CSF de este capítulo

REGLA PRINCIPAL · GR-008

Guarda tus fondos a largo plazo en una billetera bóveda. Usa otra billetera para DApps, trading y Web3.

Divide tus fondos según su uso para que un error nunca pueda alcanzar tus ahorros.

Regla	Enunciado	Por qué se aplica aquí
GR-003	Usa siempre una billetera de hardware para guardar cripto a largo plazo o de alto valor	La billetera Bóveda mantiene sus claves fuera del equipo y del teléfono que usas a diario.
TSR-004	Usa autenticación de dos factores basada en hardware	La cuenta del exchange y su correo necesitan un **inicio de sesión resistente al phishing**.
TSR-005	Activa las listas blancas de retiros en los exchanges	Una **lista blanca de retiros** limita los retiros a tus propias billeteras, aunque alguien se apodere de la cuenta.

Tabla 1.3: Reglas CSF complementarias

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

1.7 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
guardas tus ahorros a largo plazo en un exchange	Configura una billetera Bóveda con una billetera de hardware comprada al fabricante, guarda una copia de su frase semilla sin conexión, envía una pequeña transacción de prueba y después mueve los ahorros.
usas una sola billetera para los ahorros y las DApps	Crea una nueva billetera Bóveda para los ahorros y usa la antigua solo para el día a día, o dala de baja. Elimina las aprobaciones antiguas de la billetera antigua.
firmaste algo sospechoso en una billetera con fondos reales	Desde un dispositivo de confianza, crea una billetera nueva con una frase semilla nueva y mueve los fondos ahora. Después, revisa las aprobaciones de la antigua. Consulta **Contratos y aprobaciones maliciosos**.
ves que un exchange retrasa o congela los retiros	No envíes más fondos. Sigue solo los anuncios oficiales de la plataforma, guarda tus registros (**capítulo 9**) y no hagas caso a nadie que te ofrezca retiros más rápidos a cambio de una comisión. Las plataformas que exigen una comisión para retirar siguen un patrón de estafa: consulta **Plataformas de inversión falsas**.
compraste una billetera de hardware usada o preconfigurada	No la uses para guardar fondos y nunca uses una frase semilla que venía con el dispositivo. Compra una nueva al fabricante y configúrala tú mismo.
no sabes cuántas billeteras tienes	Haz una lista de billeteras: nombre, función, dispositivo o aplicación y dónde está la copia de seguridad. Da de baja las que ya no necesites.

Tabla 1.4: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Después de que vacíen una billetera o un exchange congele los fondos, aparecen falsos servicios de recuperación y falsos agentes de “soporte” que se ponen en contacto contigo. Nadie legítimo te pide tu frase semilla, acceso remoto ni una comisión. Consulta **Estafas de recuperación**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/unsafe-crypto-wallet-setup-risks/

CAPÍTULO 2

Frase semilla y copias de seguridad

“Lo anoté. Solo que no encuentro dónde.”

Figura 2.1: Frase semilla y copias de seguridad de un vistazo

Tu frase semilla (frase de recuperación) es la copia de seguridad maestra de una billetera de autocustodia (self-custody). Con ella, puedes reconstruir la billetera en cualquier dispositivo compatible. Sin ella, un teléfono perdido, una billetera de hardware (hardware wallet) rota o una aplicación restablecida pueden significar perder para siempre todo lo que hay en la billetera. Ninguna empresa, línea de soporte ni restablecimiento de contraseña puede recuperarla.

La mayoría de las frases semilla no se roban. Se pierden: nunca se anotaron, se anotaron una vez y se tiraron por accidente, se guardaron en un lugar que luego falló o se escondieron de forma tan ingeniosa que nadie puede volver a encontrarlas. Este capítulo explica cómo fallan las copias y cómo crear una que siga funcionando dentro de muchos años, para ti o para alguien que actúe en tu nombre.

EN ESTE CAPÍTULO

- 2.1 Frase semilla, clave privada y passphrase explicadas de forma sencilla
- 2.2 Errores con la copia de la frase semilla que debes conocer
- 2.3 Métodos de copia de seguridad comparados
- 2.4 Cantidades mayores: cuando una sola frase semilla no basta
- 2.5 Escenario ilustrativo: la mudanza
- 2.6 Cómo proteger la copia de tu frase semilla
- 2.7 Reglas CSF de este capítulo
- 2.8 Si esto te acaba de pasar

2.1 Frase semilla, clave privada y passphrase explicadas de forma sencilla

Tus cripto no se guardan en tu teléfono ni en tu billetera de hardware. Están en la blockchain. Tu billetera guarda las claves que te permiten moverlas.

- **Frase semilla.** Una lista de 12, 18 o 24 palabras que tu billetera crea cuando la configuras. Puede recrear todas las claves y direcciones de la billetera. Quien la tenga controla tus fondos; si la pierdes, nadie puede recrearla por ti. Consulta **Frase semilla** en el Glosario de CSF.
- **Clave privada.** La clave de una sola dirección. Tu frase semilla genera las claves privadas de todas las cuentas creadas a partir de ella, así que no necesitan una copia aparte. Excepción: una cuenta que importaste con una clave privada no está cubierta por la frase semilla; haz una copia de esa clave por separado o mueve sus fondos a una cuenta creada a partir de tu frase semilla. No las exportes salvo que tengas un motivo concreto.
- **Passphrase (frase de contraseña adicional, opcional).** Algunas billeteras te permiten añadir una palabra o frase extra además de la frase semilla. Crea una billetera completamente distinta. Si restauras la frase semilla sin la passphrase exacta, obtienes una billetera válida pero vacía, sin ningún mensaje de error. Si usas una passphrase, necesita su propia copia, guardada por separado de la frase semilla. Consulta **Passphrase**.

Hay un detalle más que importa al restaurar: distintas aplicaciones de billetera pueden usar distintas rutas de derivación (derivation path) o tipos de dirección. Si restauras una frase semilla correcta en otra aplicación y ves saldo cero, normalmente tus fondos siguen ahí; la aplicación está mirando otras direcciones. Anota la aplicación de billetera o el dispositivo que usaste con tu copia, y consulta **Ruta de derivación** antes de intentar cualquier otra cosa.

Una frase semilla parece una lista numerada de palabras sencillas: palabra 1, palabra 2 … palabra 24. Esta guía no muestra ningún ejemplo real. Hay herramientas automáticas que vigilan las frases semilla publicadas en cualquier lugar, y a veces la gente reutiliza lo que ve.

2.2 Errores con la copia de la frase semilla que debes conocer

1. Ninguna copia de seguridad

La billetera ofrece mostrar la frase semilla “más tarde”, y ese momento nunca llega. Meses después, un restablecimiento del teléfono, un dispositivo roto o una aplicación borrada se llevan la única copia. Nunca pongas fondos en una billetera antes de que la copia esté anotada y comprobada.

2. Una copia digital

Las capturas de pantalla, las notas del teléfono, el almacenamiento en la nube, los borradores de correo, los mensajes de chat a ti mismo y las aplicaciones de contraseñas parecen seguros porque siempre están a mano. Fallan de dos maneras: se pierde la cuenta o el dispositivo, o alguien más consigue entrar. Las fotos y las notas además se sincronizan con la nube por sí solas. Una frase semilla debe guardarse solo sin conexión (offline), sin excepciones para los archivos cifrados.

3. Una sola copia en papel

Una sola hoja de papel puede desaparecer con un incendio, una fuga de agua, una mudanza o una limpieza. El papel, además, se decolora y puede leerse mal. Guarda al menos dos copias en lugares separados, y usa un material resistente para cantidades mayores.

4. Una copia que nunca probaste

Una palabra que falta, un error de ortografía o el orden equivocado inutilizan toda la copia, y solo te enteras cuando la necesitas. Lo mismo ocurre con una passphrase o un PIN que olvidaste anotar. Prueba la copia una vez, justo después de crearla, sin fondos en riesgo: en una billetera de hardware, usa su comprobación de copia integrada o restáurala en una segunda billetera de hardware; en una billetera de software, restáurala en la aplicación oficial en un dispositivo de confianza. Nunca escribas la frase semilla de una billetera de hardware en un teléfono o un equipo.

5. Un lugar olvidado o un método de ocultación “ingenioso”

Una frase semilla escondida en un libro, dividida en un acertijo, escrita con tinta invisible o ultravioleta, o cifrada con una clave que nadie más conoce puede perderse con el tiempo o porque tú mismo olvides dónde está. Las tintas invisibles se borran, y tu familia no sabrá que tiene que buscarla. Lo simple y documentado gana a lo ingenioso: anota dónde están las copias, en un lugar aparte, sin las palabras.

6. Etiquetas que le dicen a quien la encuentre qué es

Un sobre con la etiqueta “frase semilla”, “palabras de recuperación” o con una marca de billetera es una invitación para cualquiera que lo encuentre. Usa una etiqueta neutra que solo signifique algo para ti y para las personas de tu plan.

7. Una frase semilla expuesta

Escribir las palabras en un sitio web “para verificar” la billetera, mostrárselas al “soporte” o leerlas en voz alta durante una llamada las expone. Lo mismo ocurre con una foto que se sincronizó con la nube. En cuanto una frase semilla pueda haber sido vista, trátala como comprometida, aunque todavía no haya pasado nada.

2.3 Métodos de copia de seguridad comparados

Método	Riesgo principal	Úsalo para
Una sola copia en papel	Fuego, agua, tinta que se borra, tirada por error	Solo a corto plazo, hasta que hagas una segunda copia

Método	Riesgo principal	Úsalo para
Dos o más copias en papel en lugares separados	Cada copia la puede leer quien la encuentre	Cantidades pequeñas y medianas
Copia en acero o en otro metal	Aún se puede encontrar y leer; coste	Ahorros y fondos a largo plazo (**cómo guardar una frase semilla en acero**)
Solo en la memoria	Olvido, enfermedad, accidentes; nadie más puede recuperarla	Nunca como única copia
Foto, archivo, nube, correo o aplicación de contraseñas	Pérdida de la cuenta, pérdida del dispositivo, hackeo, sincronización automática	Nunca

Tabla 2.1: Métodos de copia de la frase semilla comparados

2.4 Cantidades mayores: cuando una sola frase semilla no basta

Para ahorros que piensas mantener durante años, una sola frase semilla es un punto único de fallo: si alguien encuentra una copia, lo pierdes todo; si pierdes una copia, puede que todo desaparezca. Dos configuraciones reducen este riesgo, a cambio de más complejidad:

- **Multisig (multifirma):** varias claves, cada una en su propio dispositivo, de las que se necesita un número determinado para mover los fondos (por ejemplo, 2 de 3). Si pierdes una clave, no pierdes los fondos, y encontrar una clave no basta para llevárselos. Pero guarda el archivo de configuración de la billetera (descriptor) con cada copia de las claves, o puede que las claves solas no basten para restaurarla.
- **Copias divididas (Shamir):** la copia se divide en varios fragmentos, y un número determinado de fragmentos reconstruye la billetera. Algunas billeteras de hardware admiten este método.

Ambas añaden pasos que tú, y cualquiera que herede tus cripto, deben entender. Configúralas solo si vas a documentarlas con claridad y a probar la recuperación. Para ver cómo encaja esto con tu billetera Bóveda, consulta **The Three-Wallet Model®** (Modelo de Tres

Billeteras); para dejar instrucciones a otras personas, consulta el **capítulo 8: Herencia y acceso de emergencia**.

2.5 Escenario ilustrativo: la mudanza

Este es un escenario ilustrativo, no un caso concreto denunciado.

Mira configuró una billetera de hardware hace tres años y escribió sus 24 palabras en la tarjeta que venía en la caja. Guardó la tarjeta en una carpeta con la documentación del dispositivo. Durante una mudanza, la carpeta acabó en una caja de papeles viejos. Más tarde, el contenido de la caja acabó en el contenedor de reciclaje.

El mes pasado, la billetera de hardware dejó de encenderse. Mira compró un dispositivo nuevo, abrió la carpeta para restaurar la billetera y no encontró nada. Las monedas siguen en la blockchain. Nadie puede moverlas.

Qué pasó

Había una sola copia, guardada con los papeles normales, y nunca se probó ni se anotó en ningún sitio. El fallo del dispositivo no era el problema; los dispositivos fallan. El problema era una sola copia, archivada con los papeles normales.

Conclusiones clave

- Una billetera de hardware no es más segura que su copia.
- Guarda al menos dos copias en lugares separados, lejos de los papeles del día a día.
- Anota dónde están las copias y revísalas de forma periódica.

2.6 Cómo proteger la copia de tu frase semilla

- Escribe la frase semilla a mano cuando crees la billetera, antes de enviarle fondos.
- Guarda al menos dos copias en lugares separados y seguros, para que un solo incendio, inundación o robo no pueda llevarse ambas.
- Usa un material resistente, como una **copia en acero**, para ahorros y fondos a largo plazo.
- Guarda la frase semilla solo sin conexión: nada de fotos, archivos, nube, correo, chat ni aplicaciones de contraseñas.

- Prueba la copia una vez sin fondos en riesgo (en una billetera de hardware, con su comprobación de copia integrada) y comprueba cada tres meses que todavía se puede leer (calendario de revisión en el capítulo 7).
- Anota qué aplicación de billetera o dispositivo la creó, y cualquier passphrase, por separado de las palabras.
- Usa etiquetas neutras. Nunca escribas “frase semilla” ni la marca de la billetera en el sobre o el contenedor.
- Anota dónde están las copias, sin las palabras, e inclúyelo en tu **plan de emergencia (capítulo 8)**.

2.7 Reglas CSF de este capítulo

REGLA PRINCIPAL · OR-002

Nunca dependas de una sola copia de tu frase semilla.

Guarda al menos dos copias sin conexión en lugares separados, y prueba que funcionan.

Regla	Enunciado	Por qué se aplica aquí
GR-001	Nunca compartas tu frase semilla	Quien vea las palabras controla la billetera, incluidos el “soporte” y los servicios de recuperación.
GR-007	Nunca guardes tu frase semilla en la nube, en el correo ni en capturas de pantalla	Las copias digitales se pierden con la cuenta o las encuentra quien consigue entrar en ella.
OR-004	Nunca guardes tu frase semilla solo en formato digital	Una copia que solo existe en un dispositivo falla cuando falla el dispositivo.
OR-001	Prueba la recuperación de tu billetera antes de confiar en ella	Una copia sin probar puede ocultar durante años una palabra que falta o está mal escrita.

Regla	Enunciado	Por qué se aplica aquí
OR-003	Documenta cómo se creó tu billetera	La aplicación de billetera, el dispositivo, la passphrase y la ruta de derivación determinan si una restauración muestra tus fondos.

Tabla 2.2: Reglas CSF complementarias

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

2.8 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
perdiste la copia, pero la billetera todavía se abre	Crea una billetera nueva, haz bien la copia de su frase semilla (dos copias, probadas) y mueve todos los fondos a ella ahora. No borres ni restablezcas la aplicación antigua hasta que los fondos hayan llegado.
perdiste la copia y la billetera ya no se abre	Busca en todos los lugares donde pueda estar y comprueba si tienes otro dispositivo o aplicación donde la misma billetera siga instalada. Sin la frase semilla o una copia de la billetera que funcione, nadie puede restaurarla.
crees que alguien vio tu frase semilla	Dala por comprometida. Crea una billetera nueva con una frase semilla nueva y mueve todo ahora. Añadir una cuenta en la misma billetera no basta.
tienes una copia dañada o incompleta	No escribas las palabras en ningún sitio web ni se las des a nadie. Si la billetera todavía se abre, mueve primero los fondos a una billetera nueva con una copia bien hecha. A veces, unas pocas palabras ilegibles se pueden deducir sin conexión con herramientas de recuperación especializadas: pide ayuda solo a alguien que conozcas personalmente y nunca compartas las palabras.

Si…	Haz esto ahora
restauraste las palabras correctas pero ves una billetera vacía	Comprueba la passphrase y después la aplicación de billetera y la ruta de derivación antes de dar por perdidos los fondos. Consulta **Ruta de derivación** en el Glosario CSF.

Tabla 2.3: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Es probable que recibas ofertas para “recuperar” tu frase semilla o tu billetera. Nadie puede recuperar una frase semilla perdida a cambio de una comisión, y quien te pida tus palabras se llevará los fondos. Consulta **Estafas de recuperación**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/lost-seed-phrase-crypto-web3/

CAPÍTULO 3

Contraseñas, PIN, 2FA y dispositivos

“Las monedas estaban a salvo. Solo que no podía acceder a ellas.”

Figura 3.1: Contraseñas, PIN, 2FA y dispositivos de un vistazo

Tu frase semilla (frase de recuperación) puede estar a salvo y aun así puedes quedarte sin acceso. Alrededor de cada billetera hay un anillo de llaves más pequeñas: el PIN de una billetera de hardware (hardware wallet), la contraseña de una aplicación de billetera, el inicio de sesión y la autenticación de dos factores (2FA) de una cuenta en un exchange (plataforma de intercambio), la dirección de correo electrónico que puede restablecerlos todos, y el teléfono o el equipo donde están.

Si pierdes uno de ellos sin una copia de seguridad, el resultado es el mismo que perder la frase semilla: fondos que puedes ver pero no puedes mover. Este capítulo explica cómo la gente se queda sin acceso por su cuenta y las copias sencillas que te permiten volver a entrar.

EN ESTE CAPÍTULO

- 3.1 Las capas de acceso alrededor de tu billetera
- 3.2 Errores de acceso que debes conocer
- 3.3 Escenario ilustrativo: el teléfono nuevo
- 3.4 Cómo proteger tu acceso
- 3.5 Reglas CSF de este capítulo
- 3.6 Si esto te acaba de pasar

3.1 Las capas de acceso alrededor de tu billetera

Una frase semilla restaura una billetera de autocustodia (self-custody). No sirve de nada para una cuenta en un exchange, tu correo o tu gestor de contraseñas. Cada capa necesita su propia forma de volver a entrar:

Capa	Qué te deja sin acceso	La copia que te permite volver a entrar
Billetera de autocustodia (aplicación o billetera de hardware)	Dispositivo perdido, roto o restablecido; PIN o contraseña de la aplicación olvidados	Tu frase semilla (y la passphrase [frase de contraseña adicional], si configuraste una): consulta el **capítulo 2**
Exchange u otra cuenta custodiada	Dispositivo de 2FA perdido, contraseña olvidada, correo bloqueado	Códigos de respaldo de la 2FA o una segunda llave de seguridad; acceso al correo de la cuenta
Cuenta de correo electrónico	Contraseña olvidada, número de teléfono perdido, 2FA perdida	Sus propios códigos de recuperación y una segunda llave de seguridad: esta cuenta restablece las demás
Gestor de contraseñas	Contraseña maestra olvidada, dispositivo perdido	La contraseña maestra escrita o el kit de emergencia del gestor, guardados sin conexión (offline)
Teléfono o equipo	Pérdida, robo, daños, un PIN del dispositivo olvidado	Nada en el dispositivo que exista solo allí

Tabla 3.1: Las capas de acceso alrededor de tu billetera

El malware, los keyloggers (registradores de teclas) y las herramientas de acceso remoto también pueden tomar el control de un dispositivo. Eso es un ataque, no un error, y se trata en la guía de hackeos. Este capítulo trata del acceso que pierdes por tu cuenta.

3.2 Errores de acceso que debes conocer

1. Un PIN o una contraseña de billetera olvidados

Las billeteras de hardware y las aplicaciones de billetera protegen tus claves con un PIN o una contraseña. Muchas billeteras de hardware se restablecen solas después de un número determinado de PIN incorrectos: comprueba cuántos permite tu dispositivo. Un restablecimiento no hace daño si tu frase semilla está a salvo y completa, y es definitivo si no lo está.

2. Una passphrase que nadie anotó

Una **passphrase** opcional crea una billetera distinta. Si la olvidas, la frase semilla sola abre una billetera vacía. Necesita su propia copia escrita, guardada por separado de la frase semilla (capítulo 2).

3. La 2FA en un solo teléfono

Con una aplicación de autenticación (authenticator app) en un solo teléfono, basta con perder, romper o cambiar ese teléfono para quedarte sin acceso. Lo mismo pasa con las llaves de acceso (passkeys) guardadas solo en ese teléfono. La mayoría de los servicios te dan códigos de respaldo cuando activas la 2FA; mucha gente nunca los guarda, y un teléfono nuevo sin migrar los códigos la deja sin acceso.

4. El SMS como único segundo factor

Los códigos por mensaje de texto fallan cuando cambias de número, viajas o pierdes tu SIM, y alguien puede apoderarse de ellos con un SIM swap (duplicado fraudulento de la tarjeta SIM). Usa en su lugar una aplicación de autenticación o una llave de seguridad física (hardware security key), y deja el SMS solo como último recurso cuando un servicio lo exija. Consulta **Estafas de SIM swap**.

5. Una cuenta de correo electrónico que puede restablecerlo todo

La mayoría de los exchanges te permiten restablecer una contraseña a través del correo. Eso convierte tu correo en la llave maestra de tus cuentas cripto: si lo pierdes, te quedas sin acceso a todas; si dejas entrar a otra persona, puede restablecerlas. Protégelo con su propia contraseña segura y una llave de seguridad física, y guarda sus códigos de recuperación sin conexión.

6. Un gestor de contraseñas sin forma de volver a entrar

Un gestor de contraseñas es un buen lugar para las contraseñas, y un punto único de fallo si su contraseña maestra solo existe en tu cabeza. Anota la contraseña maestra o el kit de emergencia del gestor y guárdalo sin conexión. Una frase semilla no debe estar en un gestor de contraseñas (capítulo 2).

7. Todo en un mismo dispositivo

Tener la aplicación de billetera, la de autenticación, el gestor de contraseñas y el correo en el mismo teléfono significa que un solo robo o una sola pantalla rota te quita todo a la vez. Repártelos: una segunda llave de seguridad, códigos de respaldo en papel y al menos otro dispositivo que pueda iniciar sesión en tu correo.

8. Un dispositivo de segunda mano o preconfigurado

Una billetera de hardware comprada de segunda mano, o que llega con un PIN o una frase semilla ya configurados, puede estar controlada por otra persona. Cómprala directamente al fabricante y crea siempre tú mismo una frase semilla nueva. Los dispositivos manipulados son un ataque, y se tratan en la **guía de hackeos**.

3.3 Escenario ilustrativo: el teléfono nuevo

Este es un escenario ilustrativo, no un caso concreto denunciado.

Tom cambia de teléfono y entrega el antiguo en la tienda. Una semana después intenta iniciar sesión en su cuenta del exchange. La contraseña funciona; el código de 2FA no. Su aplicación de autenticación está en el teléfono antiguo y nunca guardó los códigos de respaldo.

El proceso de recuperación del exchange exige una verificación de identidad y un período de espera. Mientras tanto, no puede vender, retirar ni cambiar la configuración. Un mensaje del “soporte” le ofrece acelerar el proceso si instala una aplicación de acceso remoto. Está a punto de hacerlo.

Qué pasó

La aplicación de autenticación estaba en un solo dispositivo, sin códigos de respaldo y sin un segundo método. El cambio de teléfono en sí no hizo daño; el error fue cambiar sin migrar los códigos de 2FA. El mensaje del “soporte” era una estafa dirigida a personas que se han quedado sin acceso.

Conclusiones clave

- Guarda los códigos de respaldo en el momento en que actives la 2FA.
- Pasa la 2FA al teléfono nuevo antes de entregar el antiguo.
- El soporte real nunca te pide acceso remoto ni tu frase semilla.

3.4 Cómo proteger tu acceso

- Guarda en papel los códigos de respaldo de la 2FA cuando la actives, y consérvalos con tus otros documentos de recuperación.
- Usa una **llave de seguridad física** o una **aplicación de autenticación** en lugar del SMS, y registra una segunda llave o un segundo dispositivo de reserva.
- Protege la cuenta de correo vinculada a tus cuentas cripto con su propia contraseña segura, una llave de seguridad y códigos de recuperación guardados sin conexión.
- Anota la contraseña maestra o el kit de emergencia de tu **gestor de contraseñas** y guárdalo sin conexión.
- Registra cómo se configuró cada billetera: dispositivo, aplicación de billetera, reglas del PIN, passphrase (sí o no) y qué correo usa cada cuenta.
- Nunca dejes que un solo teléfono lo tenga todo: ten al menos otro dispositivo que pueda iniciar sesión en tu correo y en tu exchange.
- Pasa la 2FA a un teléfono nuevo antes de borrar, vender o entregar el antiguo.

- Compra las billeteras de hardware directamente al fabricante y configura tú mismo el PIN y la frase semilla.
- Una vez al año, comprueba que puedes acceder a todas tus cuentas y billeteras sin tu teléfono principal (el calendario de revisión está en el capítulo 7).

3.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · OR-006

Mantén el acceso a tus sistemas de autenticación.

Cada PIN, contraseña, método de 2FA y cuenta de correo necesita una copia que no dependa del mismo dispositivo.

Regla	Enunciado	Por qué se aplica aquí
TSR-004	Usa autenticación de dos factores basada en hardware	Una llave de seguridad resiste el phishing y los ataques de SIM swap, y una segunda llave es una reserva lista para usar.
OR-003	Documenta cómo se creó tu billetera	Saber qué dispositivo, app, reglas de PIN y passphrase usaste es lo que hace que una restauración funcione.
OR-001	Prueba la recuperación de tu billetera antes de confiar en ella	Una recuperación que ya practicaste una vez no te fallará bajo estrés.
TSR-006	Separa dispositivos y cuentas para el uso de cripto	Repartir la billetera, el autenticador y el correo entre distintos dispositivos y cuentas hace que una pérdida nunca sea total.

Tabla 3.2: Reglas CSF complementarias

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

3.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
perdiste el teléfono con tu aplicación de autenticación	Inicia sesión con tus códigos de respaldo de 2FA o con tu segunda llave de seguridad y registra un dispositivo nuevo. Sin ellos, inicia la recuperación oficial de la cuenta en cada servicio; es probable que te pidan verificaciones de identidad y que haya un tiempo de espera.
olvidaste el PIN de una billetera de hardware	Detente después de uno o dos intentos. Comprueba cuántos intentos permite tu dispositivo antes de restablecerse. Si se restablece, restáuralo desde tu frase semilla en el mismo dispositivo o en uno nuevo.
te quedaste sin acceso a una cuenta de un exchange	Usa solo el enlace de recuperación dentro de la app o el sitio web oficial al que llegues desde tu propio marcador. Nunca uses un enlace ni un número de teléfono que venga de un mensaje, un anuncio o un resultado de búsqueda.
perdiste el acceso a tu cuenta de correo electrónico	Recupera primero el correo, con sus propios códigos de recuperación o llaves de seguridad. Después, revisa cada cuenta cripto que use esa dirección de correo y cambia sus contraseñas.
olvidaste la contraseña maestra de tu gestor de contraseñas	Busca el kit de emergencia o la contraseña maestra escrita. Sin ellos, la mayoría de los gestores de contraseñas no pueden recuperar la bóveda del gestor; reconstruye el acceso cuenta por cuenta.
perdiste un dispositivo o te lo robaron	Desde otro dispositivo, cambia las contraseñas de tus cuentas de correo y de exchange, elimina el dispositivo perdido de tus cuentas y mueve los fondos de cualquier billetera cuya frase semilla o app estuviera en él sin protección.

Tabla 3.3: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Las personas que se quedan sin acceso son un objetivo favorito de los falsos servicios de soporte y de “desbloqueo”. Ningún servicio legítimo te pide tu frase semilla, acceso remoto ni una comisión para restaurar el acceso. Consulta **Estafas de recuperación**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/locked-out-crypto-wallet/

CAPÍTULO 4

Dirección equivocada

“La blockchain hace exactamente lo que le dices, incluso cuando se lo dices mal.”

Figura 4.1: Dirección equivocada de un vistazo

Enviar cripto lleva unos segundos. Deshacerlo suele ser imposible. Una vez confirmada una transacción, no hay banco al que llamar, ni contracargo, ni servicio de soporte que pueda revertirla.

La mayoría de las pérdidas por dirección equivocada no son hackeos. Vienen de pequeños hábitos: copiar una dirección del historial, comprobar solo unos pocos caracteres, editar una dirección a mano o usar una dirección que ya no es la correcta. Este capítulo trata esos hábitos y las comprobaciones que los evitan. El envío en la red, el token o el memo equivocados se trata en el **capítulo 5**.

EN ESTE CAPÍTULO

- 4.1 Lo que tu billetera puede detectar y lo que no
- 4.2 Errores con direcciones que debes conocer
- 4.3 Escenario ilustrativo: la dirección del año pasado
- 4.4 Una rutina de envío para cada transferencia
- 4.5 Reglas CSF de este capítulo
- 4.6 Si esto te acaba de pasar

4.1 Lo que tu billetera puede detectar y lo que no

Una **dirección de billetera** es una larga cadena de letras y números. Las billeteras comprueban que tenga un formato válido antes de enviar. Eso detecta muchas erratas, pero nunca una dirección válida que simplemente es la equivocada:

El error	¿La billetera lo detecta?	Qué pasa
Una errata en una dirección de Bitcoin	Casi siempre: la dirección tiene una suma de verificación (checksum) integrada	La billetera la rechaza antes de enviar
Una errata en una dirección de tipo Ethereum escrita con mayúsculas y minúsculas	Normalmente: la mayoría de las billeteras comprueban las mayúsculas como suma de verificación	La billetera la rechaza o te avisa
Una errata en una dirección de tipo Ethereum escrita todo en minúsculas	No: las direcciones en minúsculas no llevan suma de verificación	Las cripto van a una dirección que nadie controla
Una dirección válida de la persona equivocada	Nunca	Las cripto van a esa persona
Una dirección antigua tuya cuya frase semilla (frase de recuperación) se perdió	Nunca	Las cripto se ven en la blockchain, pero no se pueden mover

El error	¿La billetera lo detecta?	Qué pasa
La dirección del contrato de un token	A veces: algunas billeteras avisan	Los tokens normalmente quedan atascados para siempre

Tabla 4.1: Lo que tu billetera puede detectar y lo que no

El malware del portapapeles que cambia direcciones y las direcciones parecidas que se colocan en tu historial son ataques, no errores. Se tratan en la **guía de hackeos** y en **Estafas de envenenamiento de direcciones**. La rutina de envío de este capítulo protege contra ambos.

4.2 Errores con direcciones que debes conocer

1. Copiar una dirección del historial de transacciones

La dirección a la que enviaste el mes pasado está ahí mismo, en el historial, a un toque. Pero el historial también muestra direcciones que nunca pensabas volver a usar, y direcciones parecidas que los estafadores colocan ahí con transferencias diminutas. Copia direcciones solo de tu propia libreta de direcciones guardada, nunca del historial. Cómo funciona el truco de las direcciones parecidas: **Estafas de envenenamiento de direcciones**.

2. Comprobar solo los primeros y los últimos caracteres

La mayoría de las personas comprueba el principio y el final de una dirección. Los estafadores lo saben y crean direcciones que coinciden en ambos. Compara la dirección completa en grupos de cuatro caracteres, con tu copia guardada o con la dirección que muestra la pantalla de tu billetera de hardware (hardware wallet).

3. Escribir o editar una dirección a mano

Las direcciones de Bitcoin, y las direcciones de tipo Ethereum escritas con mayúsculas y minúsculas, llevan una suma de verificación, así que la mayoría de las erratas se rechazan. Una dirección de tipo Ethereum escrita todo en minúsculas no la lleva: un solo carácter equivocado puede crear una dirección válida que nadie controla. Nunca escribas una dirección a mano, nunca “corrijas” una editándola y nunca envíes a una dirección que te hayan dictado por teléfono.

4. Usar una dirección que ya no es la correcta

Las direcciones sobreviven al motivo por el que las guardaste. Un amigo se pasa a una billetera nueva, un exchange (plataforma de intercambio) cambia tu dirección de depósito, una factura tiene dos años. Antes de enviar a una dirección guardada que no has usado desde hace tiempo, confírmala con el destinatario por otro canal.

5. Elegir la entrada equivocada de la libreta de direcciones

Una libreta de direcciones solo ayuda si sus etiquetas son claras. “Billetera 2” y “Billetera nueva” se parecen en una pantalla pequeña. Pon a cada entrada un nombre claro, elimina las direcciones que ya no uses y comprueba la etiqueta y la dirección antes de confirmar.

6. Enviar a una billetera cuya frase semilla ya no existe

Enviar a tu propia billetera antigua solo es seguro si todavía tienes su frase semilla. Muchas personas envían a una dirección que usaron hace años, de una billetera que restablecieron o perdieron. Los fondos llegan y se quedan ahí para siempre. Antes de enviar a una dirección antigua tuya, confirma que todavía puedes acceder a esa billetera.

7. Enviar tokens a la dirección de un contrato

Cada token tiene su propia dirección de contrato, que a menudo aparece en sitios web y en exploradores de bloques junto a direcciones de billetera. Los tokens enviados a la propia dirección del contrato normalmente quedan atascados para siempre. Envía los tokens a una dirección de billetera, nunca al propio contrato del token.

8. Fiarse de un nombre en lugar de la dirección

Los servicios de nombres te permiten enviar a un nombre legible en lugar de a una dirección larga. Una errata de una sola letra en el nombre apunta a la billetera de otra persona, y un desconocido puede registrar los nombres caducados. Comprueba la dirección a la que apunta el nombre antes de confirmar.

4.3 Escenario ilustrativo: la dirección del año pasado

Este es un escenario ilustrativo, no un caso concreto denunciado.

Lena le debe dinero a su hermano por unas vacaciones compartidas. Abre su billetera, encuentra en el historial una transferencia a él del año pasado, copia esa dirección y envía la cantidad. La billetera la acepta; la transacción se confirma en minutos.

Su hermano nunca la recibe. Se había pasado a una billetera nueva hacía meses y había restablecido su teléfono antiguo sin anotar la frase semilla de esa billetera. Los fondos están en su dirección antigua, visibles en la blockchain, sin que nadie pueda moverlos.

Qué pasó

La dirección era válida y en su día perteneció a la persona correcta. Simplemente ya no se usaba. Al copiarla del historial, se saltó la única pregunta que importaba: ¿sigue siendo esta la dirección correcta?

Conclusiones clave

- Envía solo a direcciones de tu propia libreta de direcciones, no del historial.
- Confirma por otro canal una dirección que no has usado desde hace tiempo.
- Para cantidades mayores, envía una pequeña prueba y espera a que el destinatario la confirme.

4.4 Una rutina de envío para cada transferencia

- Guarda cada dirección habitual una sola vez, en la libreta de direcciones de tu billetera o en la **lista blanca de retiros** de un exchange, después de confirmarla con el destinatario.
- Copia direcciones solo de esa lista guardada o directamente del destinatario, nunca del historial, de chats ni de correos antiguos.
- Compara la dirección completa en grupos de cuatro caracteres, no solo el principio y el final.
- En una billetera de hardware, compara la dirección en la pantalla del dispositivo antes de aprobar.

- Para cantidades mayores o una dirección nueva, **envía primero una pequeña prueba**, espera a que el destinatario la confirme y después envía el resto, de nuevo desde tu libreta de direcciones.
- Nunca escribas, edites ni dictes una dirección. Si el destinatario está contigo, escanea el código QR en la pantalla de su propia billetera.
- Antes de enviar a una dirección antigua tuya, asegúrate de que todavía puedes acceder a esa billetera.
- Envía tokens solo a direcciones de billeteras, nunca a la dirección del contrato de un token.
- Detente y vuelve a comprobarlo siempre que sientas prisa: con la urgencia es cuando te saltas la rutina.

4.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · OR-005

Verifica siempre el destino antes de enviar cripto.

Comprueba la dirección completa con una copia guardada de confianza, cada vez, antes de aprobar.

Regla	Enunciado	Por qué se aplica aquí
GR-006	Envía siempre una pequeña transacción de prueba antes de transferir grandes cantidades de cripto	Una prueba demuestra que la dirección es correcta y que los fondos llegan, mientras solo arriesgas una pequeña cantidad.
TSR-005	Activa las listas blancas de retiros en los exchanges	Así, el exchange solo envía a direcciones que aprobaste antes, lo que también bloquea una errata o una dirección equivocada que hayas pegado.
SDR-010	Nunca pagues a nadie para recuperar criptomonedas perdidas	Las personas que enviaron a una dirección equivocada son uno de los principales objetivos de los servicios de recuperación falsos.

Tabla 4.2: Reglas CSF complementarias

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

4.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
no sabes qué pasó	Pega el ID de la transacción en un **explorador de bloques** de esa red. Comprueba el estado y la dirección de destino carácter por carácter.
ves que la transacción sigue pendiente	En algunas redes, una transacción pendiente se puede reemplazar o cancelar desde la misma billetera (consulta el **capítulo 6**). Una vez confirmada, ya no.
enviaste a una dirección de depósito de un exchange que no es tuya	Ponte en contacto con ese exchange a través de su sitio web o app oficial, con el ID de la transacción. Algunos pueden ayudar cuando la dirección pertenece a uno de sus clientes; no hay garantía.
enviaste a alguien que conoces, a una dirección antigua o equivocada	Pregúntale. Si la dirección pertenece a una billetera que todavía controla, puede devolvértelo. Si perdió la frase semilla de esa billetera, nadie puede.
enviaste a una dirección antigua tuya	Busca la frase semilla de esa billetera y restáurala en una app de billetera: los fondos siguen ahí (consulta el **capítulo 2**).
enviaste tokens a la dirección del contrato de un token	Ponte en contacto con el proyecto solo a través de su sitio web oficial. La mayoría de los proyectos no pueden devolverlos. Nunca pagues a nadie que se ofrezca a hacerlo.
notaste que la dirección pegada es distinta de la que copiaste	Deja de usar ese dispositivo para cripto. Que una dirección cambie al pegarla es señal de malware (consulta la **guía de hackeos**).

Tabla 4.3: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Nadie puede revertir una transacción confirmada ni “rastrear y devolver” fondos a cambio de una comisión. Las personas que enviaron cripto a una dirección equivocada son uno de los objetivos favoritos de los servicios de recuperación falsos. Consulta **Estafas de recuperación**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/crypto-wrong-wallet-address/

CAPÍTULO 5

Red, token o memo equivocados

“Dirección correcta, red equivocada, y de repente el saldo muestra cero.”

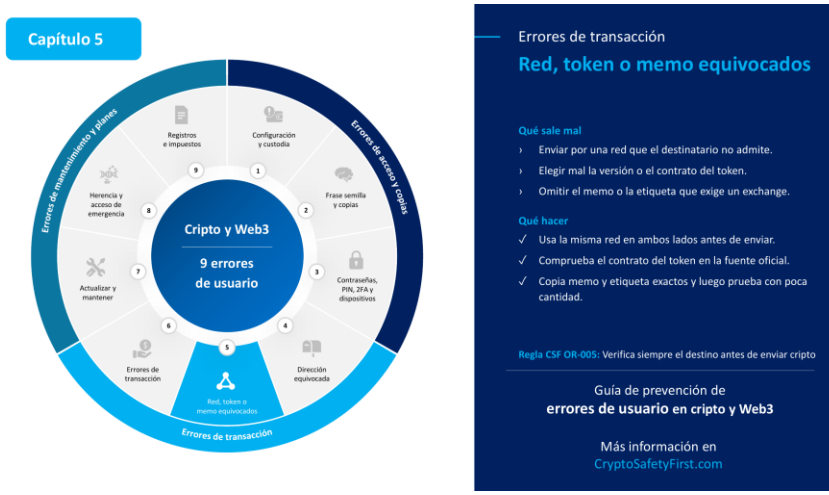

Figura 5.1: Red, token o memo equivocados de un vistazo

Puedes copiar la dirección correcta y aun así perder la pista de tus cripto. El mismo formato de dirección se usa en muchas redes, el mismo nombre de token existe en varias versiones y algunos exchanges (plataformas de intercambio) necesitan un memo o una etiqueta (tag) junto a la dirección para saber de quién es el depósito.

La buena noticia: muchos de estos errores no son definitivos. Las cripto enviadas por la red equivocada a menudo quedan en una dirección que tú o el destinatario todavía controlan. Este capítulo muestra cómo ocurren estos errores, cuáles tienen solución y las comprobaciones que los evitan. Las direcciones equivocadas se tratan en el **capítulo 4**.

EN ESTE CAPÍTULO

- 5.1 Qué errores todavía tienen solución
- 5.2 Errores de red, token y memo que debes conocer
- 5.3 Escenario ilustrativo: la red más barata
- 5.4 Comprueba la red, el token y el memo antes de cada transferencia
- 5.5 Reglas CSF de este capítulo
- 5.6 Si esto te acaba de pasar

5.1 Qué errores todavía tienen solución

A diferencia de una dirección equivocada, una red equivocada o un memo que falta a menudo dejan las cripto contigo o en el exchange. Que las recuperes depende de quién controla la dirección receptora en esa red:

Qué pasó	¿Tiene solución?	Cómo
Tokens enviados por otra red de tipo Ethereum a tu propia billetera de autocustodia (self-custody)	Normalmente sí	Añade esa red en tu billetera. Misma frase semilla (frase de recuperación), misma dirección: los fondos aparecen. Necesitas el token de gas de esa red para moverlos.
Depósito en un exchange sin el memo o la etiqueta obligatorios	Normalmente sí	Abre una solicitud de soporte (ticket) a través de la app o el sitio web oficial, con el ID de la transacción. Puede llevar tiempo y algunos exchanges cobran una comisión.
Depósito en un exchange por una red o una versión del token que no admite	A veces	Solo el exchange puede actuar. Pregunta a su soporte; no hay garantía.
Envío a una billetera multisig (multifirma) o de contrato inteligente en una red donde nunca se configuró	Depende de la billetera	Pregunta al proveedor de la billetera a través de su sitio web oficial. Algunos pueden configurar la misma dirección en esa red; otros no.

Qué pasó	¿Tiene solución?	Cómo
Tokens enviados directamente a la dirección del contrato de un token o de un puente (bridge)	Rara vez	Ponte en contacto con el proyecto solo a través de su sitio web oficial. Normalmente los tokens quedan atascados.
La billetera muestra cero, pero el explorador muestra la transferencia a tu dirección	No se ha perdido nada	Tu billetera todavía no muestra esa red o ese token. Añade la red o el contrato del token.

Tabla 5.1: Qué errores tienen solución

Una solución casi siempre pasa por ti (tu propia billetera y tu frase semilla) o por el soporte oficial del exchange o del proveedor de la billetera. Nunca por alguien que se pone en contacto contigo, y nunca compartiendo tu frase semilla.

5.2 Errores de red, token y memo que debes conocer

1. Elegir la red más barata en lugar de la correcta

Los exchanges ofrecen varias redes de retiro para la misma moneda, a menudo con la más barata arriba. Es posible que la billetera o el exchange de destino solo admita una de ellas. Elige la red que indique el destinatario, nunca solo por la comisión.

2. Dar por hecho que el mismo token está en la misma red

USDT en Ethereum, en Tron y en BNB Smart Chain comparten nombre, pero son tokens distintos en redes distintas. Un **estándar de token** como ERC-20 o BEP-20 te indica en qué red está un token. Haz coincidir siempre la red y el token en ambos lados.

3. Omitir el memo o la etiqueta de destino

Para monedas como XRP, XLM o ATOM, los exchanges suelen usar una única dirección de depósito compartida y un memo, una etiqueta o un comentario para identificarte. Sin él, el depósito llega, pero no se acredita en tu cuenta. Copia el memo exactamente, cada vez; tu propia billetera de autocustodia normalmente no lo necesita.

4. Enviar un token o una red que el exchange no admite

La dirección de depósito de un exchange solo acepta las monedas y redes que aparecen en su página de depósito. Es posible que los tokens que no admite nunca se acrediten. Comprueba en la página de depósito la moneda y la red exactas antes de enviar.

5. Elegir la versión equivocada de un token

Muchos tokens existen en una versión nativa y otra puenteada (bridged) en la misma red, y los tokens falsos copian nombres y logotipos reales. Comprueba la dirección del contrato del token en el sitio web oficial del proyecto, no en los resultados de búsqueda ni en una lista de tokens. Las versiones falsas son una estafa: consulta **Estafas con tokens**.

6. Dar por hecho que una multisig funciona en todas las redes

Una dirección de billetera normal funciona en todas las redes de tipo Ethereum. Una billetera multisig o de contrato inteligente solo existe en las redes donde se configuró. Los fondos enviados a la misma dirección en otra red pueden quedar fuera de tu alcance.

7. Enviar tokens directamente a un puente o a un contrato

Mover tokens entre redes se hace a través de la propia app del puente, nunca enviando tokens a la dirección de su contrato. Los tokens enviados directamente a un contrato normalmente quedan atascados. Los puentes también tienen sus propios riesgos, así que mueve solo lo que necesites.

8. Creer que los fondos se perdieron cuando la billetera simplemente no los muestra

Las billeteras solo muestran las redes y los tokens que tienen configurados. Una transferencia en otra red puede estar segura en tu dirección y aun así mostrar cero. Comprueba el explorador antes de entrar en pánico: el pánico es justo lo que buscan los servicios de recuperación falsos. Los tokens inesperados que no enviaste tú son un caso distinto: no los toques (**Estafas de airdrops**).

5.3 Escenario ilustrativo: la red más barata

Este es un escenario ilustrativo, no un caso concreto denunciado.

Sam retira USDT de un exchange a su billetera de hardware (hardware wallet). Pega su dirección de Ethereum y el exchange le ofrece varias redes. BNB Smart Chain es mucho más barata que Ethereum, así que la elige. El retiro se confirma, pero su billetera no muestra ningún USDT.

Publica un mensaje en un foro cripto. En cuestión de minutos, un "agente de soporte" le envía un mensaje privado: una "herramienta de sincronización" puede recuperar los fondos si introduce su frase semilla.

Qué pasó

No se perdió nada. Los USDT llegaron a la misma dirección en BNB Smart Chain. En cuanto añadió esa red en su billetera y recibió un poco de BNB para las comisiones, pudo moverlos. El "agente" del foro era una estafa de recuperación: el único riesgo real de toda la historia.

Conclusiones clave

- Elige la red que admite el destinatario, no la más barata.
- Consulta el explorador antes de entrar en pánico: puede que los fondos estén a salvo en tu dirección.
- Nadie que se ponga en contacto contigo puede "sincronizar" ni recuperar fondos. Y nunca escribas tu frase semilla en una herramienta.

5.4 Comprueba la red, el token y el memo antes de cada transferencia

- Pregunta al destinatario qué red y qué token acepta, o lee la página de depósito del exchange. Después, selecciona exactamente esa red.
- Compara el nombre de la red en ambos lados: la pantalla de retiro y la página de depósito deben indicar lo mismo.
- Comprueba el contrato del token con el sitio web oficial del proyecto, no con resultados de búsqueda ni listas de tokens.
- Copia el memo, la etiqueta o el comentario exactamente cada vez que la página de depósito muestre uno.

- Guarda cada dirección habitual en la libreta de direcciones de tu billetera o en la **lista blanca de retiros** de un exchange, junto con su red y su memo.
- Envía primero una **pequeña prueba** cada vez que la red, el token o el memo sean nuevos para ti.
- Mantén una pequeña cantidad del token de gas de cada red allí donde tengas fondos en esa red.
- Usa un puente solo a través de su propia aplicación, y solo para lo que necesites mover.
- Si el saldo aparece en cero después de una transferencia, consulta el explorador antes de hacer cualquier otra cosa.

5.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · OR-005

Verifica siempre el destino antes de enviar cripto.

El destino es la dirección, la red, el token y el memo: comprueba los cuatro antes de aprobar.

Regla	Enunciado	Por qué se aplica aquí
GR-006	Envía siempre una pequeña transacción de prueba antes de transferir grandes cantidades de cripto	Una pequeña prueba en una red, un token o un memo nuevos demuestra que la configuración funciona antes de mover la cantidad completa.
TSR-005	Activa las listas blancas de retiros en los exchanges	Una entrada de la lista blanca guarda la dirección junto con su red y su memo, así que los eliges una sola vez, con cuidado.
SDR-010	Nunca pagues a nadie para recuperar criptomonedas perdidas	Las personas cuyas cripto “desaparecieron” en la red equivocada son uno de los principales objetivos de los falsos servicios de recuperación.

Tabla 5.2: Reglas CSF complementarias

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

5.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
no sabes qué red usaste	Abre los detalles del retiro o de la transacción en la aplicación desde la que enviaste. Busca el ID de la transacción en un **explorador de bloques** de esa red.
enviaste a tu propia billetera en otra red de tipo Ethereum	Añade esa red en la misma billetera (o restaura la frase semilla en una billetera que la admita, consulta el **capítulo 2**). Compra o recibe un poco del token de gas de esa red para mover los fondos.
olvidaste el memo o la etiqueta en un depósito en un exchange	Abre una solicitud de soporte a través de la aplicación o el sitio web oficial del exchange: ID de la transacción, cantidad, dirección de depósito y tu cuenta. Nunca respondas al “soporte” que se pone en contacto contigo primero.
enviaste un token o una red que el exchange no admite	Pregunta al exchange, a través de su soporte oficial, si puede acreditar o devolver el depósito. No envíes nada más a esa dirección.
enviaste a una billetera multisig o de contrato inteligente en la red equivocada	No pruebes soluciones de foros. Pregunta al proveedor de la billetera, a través de su sitio web oficial, qué es posible en esa red.
ves un saldo cero después de una transferencia a tu propia billetera	Consulta primero el explorador. Si la transferencia aparece, añade la red o el contrato del token desde el sitio web oficial del proyecto: los fondos no se han perdido.

Tabla 5.3: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Los falsos “agentes de soporte” y servicios de recuperación vigilan foros y redes sociales en busca de personas cuyos fondos desaparecieron. Ningún servicio legítimo necesita tu frase semilla, acceso remoto ni un pago por adelantado. Consulta **Estafas de recuperación**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/crypto-sent-wrong-network/

CAPÍTULO 6

Errores en transacciones: comisiones, transacciones atascadas y deslizamiento

“La transacción no desapareció. Estaba esperando, y pagué dos veces intentando arreglarlo.”

Figura 6.1: Errores en transacciones de un vistazo

Cada transacción tiene un precio y una serie de ajustes: la comisión de red, la cantidad y, en los swaps (intercambios de tokens), el deslizamiento (slippage) que aceptas. La mayoría de las veces, las sugerencias de la billetera están bien. Cuando no lo están, una transacción se queda colgada durante horas, falla y aun así cuesta la comisión, o un swap devuelve mucho menos de lo esperado.

Estos errores rara vez hacen perder todo de golpe, pero son frecuentes, y el pánico que provocan es lo que busca el falso “soporte”. Este capítulo explica los ajustes que importan y qué hacer cuando una transacción sale mal.

EN ESTE CAPÍTULO

- 6.1 Los términos de comisiones y transacciones que importan
- 6.2 Errores en transacciones que debes conocer
- 6.3 Escenario ilustrativo: el pago doble
- 6.4 Antes de confirmar una transacción
- 6.5 Reglas CSF de este capítulo
- 6.6 Si esto te acaba de pasar

6.1 Los términos de comisiones y transacciones que importan

No necesitas entender cómo una blockchain pone precio a su espacio en los bloques. Necesitas conocer unos pocos términos que te muestra tu billetera, y lo que significa cada uno cuando algo sale mal:

Término	Qué significa	Por qué importa
Comisión de red (gas)	Lo que pagas a la red para que procese una transacción. Las billeteras suelen ofrecer lenta, normal y rápida.	Si es demasiado baja, la transacción espera; si es demasiado alta, pagas de más. Consulta **gas**.
Token de gas	La moneda propia de la red con la que se paga la comisión: ETH en Ethereum y en la mayoría de sus redes de capa 2 (layer 2), BNB en BNB Smart Chain, POL en Polygon, SOL en Solana.	Sin él no puedes mover ningún token en esa red.
Pendiente	Enviada, pero todavía no incluida en un bloque.	Todavía se puede acelerar o cancelar. Una vez confirmada, ya no.
Fallida (revertida)	Incluida en un bloque, pero la acción no se realizó.	Tus fondos se quedan donde estaban, pero la comisión se gasta.

Término	Qué significa	Por qué importa
Nonce (redes de tipo Ethereum)	El número correlativo de cada transacción desde tu dirección.	Una transacción atascada bloquea todas las posteriores desde la misma dirección hasta que se confirma o se reemplaza.
“Acelerar” / “cancelar” (replace-by-fee)	Una nueva versión de la transacción pendiente con una comisión más alta.	La forma segura de arreglar una transacción atascada, en lugar de volver a enviarla.
Tolerancia al deslizamiento	Cuánto peor que el precio cotizado aceptas en un swap.	Una tolerancia alta puede devolverte muchos menos tokens. Consulta **deslizamiento**.
Mínimo recibido	Lo mínimo que puede devolver el swap con tu ajuste de deslizamiento.	Léelo antes de confirmar: es el peor caso real.

Tabla 6.1: Términos de comisiones y transacciones que importan

Los retiros desde un exchange (plataforma de intercambio) funcionan de otra manera: el exchange fija la comisión y envía la transacción él mismo. No puedes acelerarla ni cancelarla. Si un retiro se queda colgado, ponte en contacto con el exchange a través de su aplicación o su sitio web oficial.

6.2 Errores en transacciones que debes conocer

1. Poner una comisión demasiado baja

Una comisión inferior a la que la red necesita en ese momento deja la transacción pendiente, a veces durante horas o días. En las redes de tipo Ethereum, además, bloquea todas las transacciones posteriores desde la misma dirección. Usa la comisión normal o sugerida de la billetera, salvo que sepas por qué necesitas otra.

2. Volver a enviar el pago en lugar de acelerarlo

La reacción más cara ante una transacción atascada es volver a enviar el mismo pago. La primera sigue siendo válida y puede confirmarse más tarde, y entonces habrás pagado dos veces. Usa “acelerar” o “cancelar”

en la billetera desde la que la enviaste: reemplazan la transacción pendiente en lugar de añadir una nueva.

3. Pagar de más sin comprobar la comisión en dinero

Las billeteras que usan “rápida” por defecto, o una comisión personalizada mal escrita, pueden convertir una transferencia rutinaria en una cara. Antes de confirmar, lee la comisión como una cantidad en tu propia moneda. Si parece incorrecta, probablemente lo sea.

4. No dejar token de gas

Enviar todo tu saldo de ETH, BNB o SOL con “Max” no deja nada para pagar la siguiente transacción. Lo mismo ocurre después de pasar tokens por un puente (bridge) a una red nueva sin su token de gas. Los tokens están a salvo, pero no se pueden mover. Mantén un pequeño saldo del token de gas de cada red allí donde tengas fondos.

5. Forzar una transacción que la billetera dice que fallará

Muchas billeteras simulan la transacción y te avisan cuando es probable que falle. Confirmarla de todos modos suele significar una transacción fallida y una comisión gastada. Averigua primero por qué: saldo insuficiente, una aprobación que falta o un precio que cambió.

6. Poner un deslizamiento demasiado alto

Una tolerancia al deslizamiento alta permite que un swap se ejecute a un precio mucho peor, y da a los bots de trading margen para quedarse con la diferencia. Mantén el valor predeterminado salvo que una operación siga fallando, y lee el “mínimo recibido” cada vez. Un token que solo puedes vender con un deslizamiento muy alto es una señal de alerta: consulta **Estafas con tokens**.

7. Introducir una cantidad equivocada

Un cero de más, una confusión entre la visualización en el token y en moneda fiat, o un botón “Max” que no querías pulsar. Comprueba la cantidad tanto en el token como en tu propia moneda antes de confirmar y, en una billetera de hardware (hardware wallet), compárala en la pantalla del dispositivo.

8. Aprobar un gasto ilimitado “para ahorrar comisiones”

Las aprobaciones de tokens ilimitadas te ahorran una comisión de aprobación la próxima vez y dejan un permiso abierto de forma indefinida. Aprueba solo la cantidad que necesitas y elimina las aprobaciones antiguas (**herramientas de aprobaciones**). Cómo las aprobaciones maliciosas vacían billeteras: **Contratos y aprobaciones maliciosos**.

6.3 Escenario ilustrativo: el pago doble

Este es un escenario ilustrativo, no un caso concreto denunciado.

Mia paga a un trabajador independiente en USDC en Ethereum y elige la comisión más barata. Una hora después, el pago sigue apareciendo como pendiente. Preocupada, vuelve a enviar la misma cantidad con una comisión normal.

El segundo pago espera detrás del primero, porque su billetera procesa en orden las transacciones de una misma dirección. Cuando las comisiones de red bajan esa noche, ambos se confirman. El trabajador independiente ha cobrado dos veces y hay que pedirle que devuelva uno de los pagos.

Qué pasó

Una comisión baja, por sí sola, solo era un retraso. Volver a enviar convirtió el retraso en un pago doble. Usar “acelerar” en la primera transacción la habría sustituido por otra con una comisión más alta y habría mantenido un solo pago.

Conclusiones clave

- Usa la comisión normal de la billetera, salvo que tengas un motivo para no hacerlo.
- Una transacción pendiente no está perdida: acelérala o cancélala, nunca vuelvas a enviarla.
- Comprueba el estado en un explorador de bloques antes de hacer nada.

6.4 Antes de confirmar una transacción

- Lee la comisión como una cantidad en tu propia moneda. Si parece incorrecta, detente.

- Comprueba la cantidad dos veces: en el token y en tu moneda.
- Mantén un pequeño saldo del token de gas de cada red en la que tengas fondos.
- En los swaps, mantén el deslizamiento predeterminado y lee el "mínimo recibido" antes de confirmar (**vista previa de la transacción**).
- Toma en serio las advertencias de la billetera: si dice que la transacción probablemente fallará, averigua primero por qué.
- Si una transacción se queda atascada, usa "acelerar" o "cancelar" en la misma billetera. Nunca vuelvas a enviarla.
- Aprueba solo la cantidad que necesitas y elimina las aprobaciones que ya no uses.
- Para una transferencia grande o poco habitual, **envía primero una pequeña prueba**: muestra la comisión y el tiempo reales antes de que se mueva la cantidad completa.

6.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · GR-006

Envía siempre una pequeña transacción de prueba antes de transferir grandes cantidades de cripto.

Una pequeña prueba muestra la comisión real, la red y el tiempo mientras solo arriesgas una cantidad pequeña.

Regla	Enunciado	Por qué se aplica aquí
GR-004	Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos	Las aprobaciones también son transacciones. Las aprobaciones ilimitadas "para ahorrar comisiones más adelante" siguen abiertas mucho después del swap.
SDR-003	Nunca pagues para desbloquear o retirar fondos	Una "comisión de gas" que debes pagar antes de recibir, liberar o desbloquear cripto es una estafa, no una comisión de red.

Regla	Enunciado	Por qué se aplica aquí
SDR-010	Nunca pagues a nadie para recuperar criptomonedas perdidas	Las transacciones atascadas o fallidas atraen a falsos agentes de soporte que se ofrecen a solucionarlas a cambio de una comisión o de tu frase semilla (frase de recuperación).

Tabla 6.2: Reglas CSF complementarias

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

6.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
tienes una transacción pendiente desde hace mucho tiempo (red de tipo Ethereum)	En la billetera desde la que la enviaste, usa “acelerar” para volver a enviarla con una comisión más alta, o “cancelar” para reemplazarla. No envíes un pago nuevo: se queda en la cola detrás de la transacción atascada y es posible que se procesen las dos.
tienes una transacción de Bitcoin pendiente desde hace mucho tiempo	Si tu billetera ofrece “aumentar la comisión” (bump fee), úsala. Si no, espera: el receptor, o tú con la salida de cambio, puede acelerarla con una transacción posterior. Con el tiempo, los nodos descartan una transacción no confirmada, pero aún puede retransmitirse y confirmarse más tarde; por eso, vuelve a enviarla solo con la función “aumentar la comisión” o “cancelar” de tu billetera, que gasta las mismas monedas. Nunca envíes un segundo pago independiente.
ves una transacción fallida	Tus fondos no se movieron; solo se perdió la comisión. Lee el motivo en un **explorador de bloques** (sin gas, el precio cambió, falta la aprobación) antes de volver a intentarlo.
no puedes mover tokens porque no tienes token de gas	Envía una pequeña cantidad del token de gas de esa red a la misma dirección, desde un exchange u otra billetera que controles.

Si…	Haz esto ahora
recibiste muchos menos tokens de un swap que los cotizados	Comprueba el “mínimo recibido” y el impacto en el precio en los detalles de la transacción. No se puede revertir; reduce tu tolerancia al deslizamiento para la próxima vez y desconfía de los tokens que solo se pueden vender con un deslizamiento muy alto.
enviaste una cantidad equivocada	Si la transacción sigue pendiente, cancélala. Si ya está confirmada, pide al receptor que te devuelva la diferencia.
te dicen que debes pagar una “comisión de gas” para recibir o desbloquear fondos	Detente. Eso es una estafa, no una comisión de red (SDR-003). Consulta **Estafas de regalos y airdrops**.

Tabla 6.3: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Las transacciones atascadas y fallidas son una de las vías favoritas del falso soporte en foros y redes sociales. Ninguna persona legítima que te ayude necesita tu frase semilla, acceso remoto ni una comisión para solucionar una transacción. Consulta **Estafas de recuperación**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/crypto-transactions-gas-fees-mistakes/

CAPÍTULO 7

Actualizaciones y mantenimiento

“La configuración era perfecta… en 2021.”

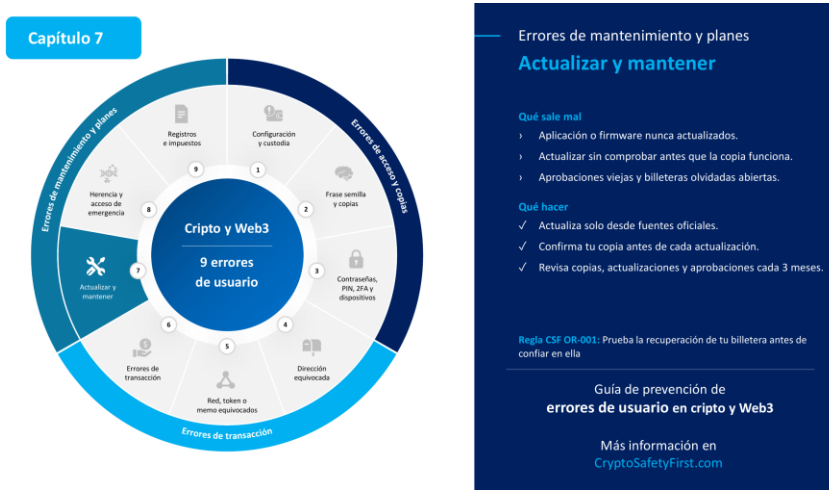

Figura 7.1: Actualizaciones y mantenimiento de un vistazo

La mayoría de las configuraciones cripto no fallan el día en que se crean. Fallan años después: una copia de seguridad que se borró con el tiempo, una actualización de firmware hecha sin una recuperación probada, una aprobación concedida a un proyecto olvidado hace mucho, una billetera que nadie recuerda.

Nada de esto requiere conocimientos técnicos para evitarse, solo una rutina. Este capítulo trata los errores de actualización y mantenimiento que convierten una buena configuración en una débil, y ofrece un único calendario de revisión para toda la guía.

EN ESTE CAPÍTULO

- 7.1 Un único calendario de revisión para tu configuración
- 7.2 Errores de mantenimiento que debes conocer
- 7.3 Mantenlo lo bastante simple para usarlo bajo estrés
- 7.4 Escenario ilustrativo: la actualización que pedía las palabras
- 7.5 Reglas CSF de este capítulo
- 7.6 Si esto te acaba de pasar

7.1 Un único calendario de revisión para tu configuración

Este calendario es el mismo que usa el **Three-Wallet Model® Toolkit** (kit de herramientas) y sustituye los distintos intervalos de la primera edición. Elige fechas fijas (por ejemplo, el primer fin de semana de cada trimestre) y las revisiones te llevarán solo unos minutos:

Cuándo	Qué comprobar	Por qué
Cada 3 meses	Las copias de seguridad siguen siendo legibles y están donde deben estar · aplicaciones de billetera, extensiones y firmware actualizados desde fuentes oficiales · aprobaciones de tokens y conexiones con DApps revisadas · billeteras Desechables dadas de baja cuando ya no se usan	Detecta a tiempo las copias deterioradas, los fallos de seguridad conocidos y los permisos abiertos.
Cada 6 meses	Lista de billeteras y etiquetas al día · cada billetera se sigue usando para su propósito · billeteras nuevas registradas y con copia · información de emergencia todavía fácil de encontrar	Mantiene tus registros al día con lo que realmente usas.
Una vez al año	Simulacro completo de recuperación (billetera de hardware [hardware wallet]: comprobación de copia integrada o una segunda billetera de hardware; nunca escribas la frase semilla [frase de recuperación] en un teléfono ni en un equipo) · ubicaciones de las copias · acceso a todas las cuentas sin tu teléfono principal (**capítulo 3**) · plan de herencia (**capítulo 8**) · dispositivos antiguos y billeteras sin uso dados de baja	Demuestra que toda la configuración funciona cuando la necesitas.
Antes de cada actualización de firmware o de versión principal	Copia de la frase semilla completa y legible · passphrase (frase de contraseña adicional) anotada, si usas una	Una actualización que restablece el dispositivo solo es inofensiva si tienes una buena copia.

Cuándo	Qué comprobar	Por qué
Después de cualquier cambio importante	Teléfono nuevo, billetera nueva, mudanza, nueva situación familiar: actualiza los registros, las copias y el plan de emergencia	Los registros que ya no reflejan la realidad fallan en el peor momento.

Tabla 7.1: Un único calendario de revisión para toda la guía

7.2 Errores de mantenimiento que debes conocer

1. Ignorar las actualizaciones

Las aplicaciones de billetera, las extensiones del navegador, el firmware de la billetera de hardware y el teléfono o el equipo en el que funcionan reciben correcciones de seguridad. Usar versiones antiguas mantiene abiertas debilidades conocidas. Activa las notificaciones de actualización y compruébalo en tu revisión trimestral.

2. Actualizar el firmware sin una copia probada

La mayoría de las actualizaciones de firmware van bien. Unas pocas restablecen el dispositivo y, entonces, la frase semilla es la única forma de recuperarlo. Antes de cada actualización de firmware, comprueba que tu copia está completa y es legible, y que conoces tu passphrase, si usas una.

3. Actualizar desde un enlace recibido en un mensaje

Los proveedores de billeteras reales no envían archivos de actualización por correo electrónico, SMS ni ventanas emergentes. Actualiza solo dentro de la aplicación oficial, en la tienda oficial de aplicaciones o, en el caso de las billeteras de hardware, en la aplicación del propio fabricante. Los mensajes de actualización falsos se tratan en **Estafas de phishing**.

4. Tratar todas las actualizaciones igual

Las correcciones de seguridad deben instalarse pronto. Las versiones grandes con nuevas funciones y las versiones principales de firmware pueden esperar unos días hasta que se conozcan los primeros problemas, pero no meses. Lee las notas de la versión en la aplicación o el sitio web oficiales.

5. Dejar abiertas aprobaciones antiguas

Cada aprobación que diste a una DApp sigue siendo válida hasta que la eliminas. Los proyectos se abandonan o los hackean años después, y entonces una aprobación antigua puede usarse para llevarse tokens. Revisa las aprobaciones cada tres meses y elimina las que ya no uses. Cómo se abusa de las aprobaciones: **Contratos y aprobaciones maliciosos**.

6. Olvidar billeteras que todavía tienen fondos

Las billeteras antiguas de airdrops, configuraciones de prueba o un teléfono anterior acumulan pequeños saldos y casi nunca se vigilan. Si se pierde su frase semilla, se pierden los fondos; si se filtró, nadie nota el robo. Mantén una lista de billeteras y da de baja las que ya no necesites.

7. Usar billeteras en dispositivos sin soporte

Un teléfono o un equipo que ya no recibe actualizaciones de seguridad es una base débil, incluso con una app de billetera actualizada. Mueve las billeteras a un dispositivo con soporte y después restablece el antiguo.

8. No probar nunca la recuperación

Una copia solo está probada de verdad cuando ha restaurado una billetera. Pruébala una vez sin fondos en riesgo (en una billetera de hardware con su comprobación de copia integrada o en una segunda billetera de hardware, nunca escribiendo la frase semilla en un teléfono o un equipo) y después haz un simulacro completo de recuperación una vez al año. No des por hecho que las palabras que faltan se podrán “adivinar más tarde”: a veces los especialistas pueden probar sin conexión unas pocas palabras que faltan, pero cualquiera que te pida en línea las palabras restantes va por tus fondos. Consulta **recuperación de billeteras**.

7.3 Mantenlo lo bastante simple para usarlo bajo estrés

Algunas configuraciones se vuelven tan complejas que su propietario no puede seguirlas en una emergencia: frases semilla divididas en varios

lugares, billeteras multisig (multifirma) con titulares de claves poco claros, herramientas de cifrado que nadie más entiende. Una configuración que solo funciona en un buen día es un riesgo en sí misma.

- ¿Puedes seguir tus pasos de recuperación bajo presión, sin tener que buscar nada?
- ¿Podría seguirlos una persona de confianza sin ti?
- ¿Has probado el proceso completo de principio a fin?

Prefiere métodos bien documentados (una billetera de hardware y copias en papel o en acero sin conexión) y añade complejidad solo cuando puedas mantenerla documentada y probada.

7.4 Escenario ilustrativo: la actualización que pedía las palabras

Este es un escenario ilustrativo, no un caso concreto denunciado.

Jonas no ha tocado su billetera de hardware desde hace dos años. La app oficial muestra una actualización de firmware y él la instala. La actualización se detiene a mitad; el dispositivo se reinicia y le pide que lo restaure desde su frase semilla.

Su única copia en papel está en un cajón. Dos palabras se han borrado y cuesta leerlas. Finalmente encuentra la segunda copia que hizo en casa de sus padres y restaura la billetera.

Qué pasó

La actualización hizo lo que a veces hacen las actualizaciones. El verdadero riesgo era una copia que nadie había comprobado desde hacía dos años. La segunda copia lo salvó.

Conclusiones clave

- Comprueba tu copia antes de cada actualización de firmware.
- Guarda una segunda copia en otro lugar.
- Incluye las comprobaciones de la copia en un calendario de revisión fijo.

7.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · OR-001

Prueba la recuperación de tu billetera antes de confiar en ella.

Prueba tu copia una vez (en una billetera de hardware con su comprobación de copia integrada) y haz un simulacro completo de recuperación una vez al año.

Regla	Enunciado	Por qué se aplica aquí
GR-004	Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos	Las aprobaciones antiguas son la puerta abierta más común en una billetera por lo demás bien cuidada.
TSR-001	Nunca instales software cripto de fuentes no oficiales	Las actualizaciones llegan solo a través de la app, la tienda o el sitio web oficiales, nunca desde un enlace en un mensaje.
TSR-002	Da por hecho que tu dispositivo puede estar comprometido	Los teléfonos y equipos antiguos sin soporte ya no reciben correcciones de seguridad; trátalos como corresponde.

Tabla 7.2: Reglas CSF complementarias

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

7.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
recibiste un mensaje de actualización por correo electrónico, SMS o ventana emergente	No hagas clic en el enlace. Abre la aplicación de la billetera o escribe tú mismo la dirección web oficial y compruébalo allí. Las actualizaciones falsas son una estafa: consulta **Aplicaciones y billeteras falsas**.
tienes una billetera de hardware que se restableció durante una actualización	Restáurala desde tu frase semilla (y tu passphrase, si usas una) en el propio dispositivo, siguiendo la app oficial del fabricante. Introduce las palabras solo en la propia pantalla de la billetera de hardware: una app, un sitio web o una ventana emergente que te pida escribirlas es una estafa.
encontraste una copia con palabras ilegibles	Si la billetera todavía se abre, crea una billetera nueva con una frase semilla nueva, haz una copia correcta y mueve los fondos ahora. Si no se abre, usa tu segunda copia (**capítulo 2**). Nunca compartas las palabras restantes con nadie.
encontraste aprobaciones antiguas que ya no necesitas	Elimínalas desde un dispositivo de confianza con la sección de aprobaciones de tu billetera o con una **herramienta de verificación de aprobaciones**. Cada eliminación cuesta una pequeña comisión de red.
encontraste una billetera olvidada con fondos	Comprueba que todavía tienes su frase semilla. Después mueve los fondos a tu configuración actual, registra la billetera antigua como dada de baja y conserva su copia hasta que la billetera esté vacía.
usas un teléfono o un equipo que ya no recibe actualizaciones	Mueve tus apps de billetera a un dispositivo con soporte y después restablece o da de baja el antiguo para que no quede ninguna clave en él.

Tabla 7.3: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Las personas con copias dañadas o dispositivos restablecidos son un objetivo de falsos servicios de “recuperación” y “reparación”. Nadie legítimo te pide tu frase semilla, una parte de ella ni acceso remoto. Consulta **Estafas de recuperación**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/crypto-wallet-software-mistakes/

CAPÍTULO 8

Herencia y acceso de emergencia

“Sabíamos que tenía cripto. Lo que no sabíamos era dónde, ni cómo.”

Figura 8.1: Herencia y acceso de emergencia de un vistazo

La autocustodia (self-custody) significa que nadie más puede quitarte tus cripto. También significa que nadie más puede desbloquearlas (ni tu pareja, ni tus hijos, ni un abogado o un tribunal) a menos que les hayas dejado una forma de acceder.

Este capítulo es el único lugar de la guía dedicado a la herencia y al acceso de emergencia: una enfermedad, un accidente o simplemente un momento en que no puedes actuar tú mismo. Muestra lo que tu familia necesita saber, cómo mantenerlo seguro hasta entonces y los errores que dejan a los herederos sin acceso. No es asesoramiento legal: la ley de herencias varía según el país.

EN ESTE CAPÍTULO

- 8.1 Lo que tu familia necesita y lo que todavía no debe tener
- 8.2 Errores de herencia que debes conocer
- 8.3 Opciones de acceso compartido o diferido
- 8.4 Un plan en cinco pasos
- 8.5 Escenario ilustrativo: dos tipos de cripto
- 8.6 Reglas CSF de este capítulo
- 8.7 Si esto te acaba de pasar

8.1 Lo que tu familia necesita y lo que todavía no debe tener

Un buen plan le da a tu familia un camino que seguir sin entregarle las claves hoy. Piénsalo por capas:

Qué	Quién lo sabe o lo tiene	Dónde se guarda
Que existen cripto, y aproximadamente cuánto	Tu persona de confianza, desde ya	Se lo dices en persona; se menciona en tu testamento sin ninguna clave
Dónde está el plan de recuperación	Tu persona de confianza, desde ya	Un sobre cerrado o el testamento indica dónde está
El plan de recuperación: billeteras, apps, dispositivos, exchanges (plataformas de intercambio), paso a paso	Nadie lo lee hasta que haga falta	Cerrado, en un lugar seguro, separado de la frase semilla (frase de recuperación)
Frases semilla (y passphrases [frases de contraseña adicionales])	Nadie excepto tú	Tus copias de seguridad sin conexión (offline), como en el capítulo 2; nunca en el plan, nunca en el testamento

Qué	Quién lo sabe o lo tiene	Dónde se guarda
Acceso al exchange y al correo electrónico	Nadie excepto tú	Kit de emergencia del gestor de contraseñas o credenciales escritas, guardados sin conexión (capítulo 3)

Tabla 8.1: Lo que tu familia necesita y dónde se guarda

8.2 Errores de herencia que debes conocer

1. Nadie sabe que las cripto existen

Las familias a menudo saben que alguien “tenía cripto”, pero no dónde. Sin al menos ese conocimiento, nadie empieza siquiera a buscar. Tu persona de confianza debe saber que existen cripto, aproximadamente cuánto y dónde está el plan, sin tener las claves.

2. Sin instrucciones, o con instrucciones que solo tú entiendes

Una frase semilla y una billetera de hardware (hardware wallet) no significan nada para alguien que nunca las ha usado. Escribe pasos sencillos: qué dispositivo o app, desde dónde descargarla, dónde está la copia, qué redes y tokens es probable que encuentre. Da por hecho que quien lo lea nunca ha usado cripto.

3. Guardar juntas las instrucciones y la frase semilla

Si el plan y la frase semilla están en el mismo sobre, quien lo encuentre tiene acceso total, tanto un ladrón como un heredero. Guárdalos en lugares separados y deja que el plan indique dónde está la copia.

4. Escribir la frase semilla en el testamento

Los testamentos los leen abogados, notarios, familiares y a veces tribunales, y en algunos países pasan a formar parte de archivos oficiales. Menciona tus cripto en el testamento e indica que existe un plan de recuperación; nunca escribas en él frases semilla, passphrases ni PIN. Pregunta a un abogado o notario cómo funciona esto donde vives.

5. Olvidar las cuentas en exchanges

Los saldos en exchanges normalmente pueden entregarse a los herederos, pero solo si alguien sabe que la cuenta existe. Haz una lista de cada exchange y app que usas, y de la dirección de correo electrónico asociada a cada cuenta. Los registros también ayudan a los herederos con los impuestos y los extractos (**capítulo 9**).

6. Todo detrás de una sola contraseña

Si cada inicio de sesión, nota y código de recuperación está en un gestor de contraseñas cuya contraseña maestra solo existe en tu cabeza, nadie podrá abrir nada cuando ya no estés. Guarda el kit de emergencia o la contraseña maestra sin conexión, y recuerda que la 2FA de tu teléfono necesita su propia copia (**capítulo 3**).

7. Una configuración demasiado compleja para cualquier otra persona

Las billeteras multisig (multifirma), las copias divididas y varios dispositivos pueden ofrecer una buena seguridad, y a la vez resultar imposibles para un heredero sin orientación. Si los usas, documenta cada pieza y quién la tiene, y plantéate designar a una persona con conocimientos técnicos en quien tu heredero pueda confiar.

8. Un plan que nadie ha comprobado

Las billeteras cambian, las copias se trasladan y las personas se mudan. Un plan escrito hace cinco años puede indicar un dispositivo que ya no existe. Revísalo una vez al año junto con tus otras comprobaciones (**capítulo 7**) y recórrelo paso a paso con tu persona de confianza.

8.3 Opciones de acceso compartido o diferido

Para la mayoría de las personas, un plan en sobre cerrado y una copia sin conexión separada son suficientes. Las cantidades mayores a veces justifican algo más, pero cada pieza adicional debe estar documentada y probada:

Opción	Cómo funciona	Ten cuidado con
Plan en sobre cerrado + copia separada	Las instrucciones en un lugar y la copia de la frase semilla en otro; tu persona de confianza sabe dónde están ambas.	Sencillo y robusto. Ambos lugares deben seguir siendo seguros, y el plan debe mantenerse actualizado.
Billetera multisig	Una billetera **multisig** necesita, por ejemplo, 2 de 3 claves. Tú, una persona de confianza y una copia de seguridad tienen una cada uno.	Más piezas en juego. Perder más claves de las que permite el umbral, o el archivo de configuración de la billetera (descriptor), bloquea los fondos; los herederos necesitan instrucciones claras o ayuda.
Copias divididas (tipo Shamir)	Algunas billeteras de hardware dividen la copia en varios fragmentos; un número determinado de ellos restaura la billetera.	Cada fragmento debe estar registrado y poder encontrarse. No todas las billeteras lo admiten.
Servicios de herencia o de acceso diferido	Un proveedor libera el acceso tras un período de espera o un fallecimiento confirmado.	Dependes de que el proveedor siga existiendo y sea honesto. Comprueba quién podría acceder a tus fondos, y nunca entregues una frase semilla.

Tabla 8.2: Opciones de acceso compartido o diferido

8.4 Un plan en cinco pasos

1. Haz una lista de lo que tienes

Cada billetera y su función, cada dispositivo, cada exchange o aplicación, lo que contiene aproximadamente cada uno y la dirección de correo electrónico asociada a cada cuenta. La lista de billeteras del Three-Wallet Model® Toolkit (kit de herramientas) funciona bien para esto.

2. Elige a tu persona de confianza

Tu pareja, un hijo adulto, un amigo o un abogado. No necesita acceso ahora; solo saber que existe un plan y dónde está.

3. Escribe el plan de recuperación

Pasos sencillos para cada billetera y cuenta: qué aplicación o dispositivo, dónde está la copia, si se necesita una passphrase (sin escribirla en el plan) y a quién dirigirse en el caso de las cuentas en exchanges.

4. Guarda el plan y las copias por separado

Por ejemplo, el plan en un sobre cerrado con tus documentos importantes y las copias de la frase semilla en los lugares del capítulo 2. En tu testamento, menciona el plan, no las claves.

5. Revísalo cada año

Actualízalo cada vez que añadas una billetera, cambies de dispositivo o te mudes. Una vez al año, compáralo con tu configuración y recórrelo paso a paso con tu persona de confianza.

8.5 Escenario ilustrativo: dos tipos de cripto

Este es un escenario ilustrativo, no un caso concreto denunciado.

Tras la muerte de su padre, Anna encuentra correos electrónicos de un exchange de cripto y, en el escritorio de él, una pequeña billetera de hardware. El exchange pide un certificado de defunción y los documentos de la herencia, y libera el saldo al cabo de unas semanas.

La billetera de hardware es otra historia. Nadie conoce su PIN y no hay frase semilla en ninguna parte: ni una nota, ni un sobre, ni instrucciones. Un desconocido en un foro en línea se ofrece a “desbloquearla” a cambio de una parte de los fondos.

Qué pasó

La cuenta custodiada tenía un proceso; la billetera de autocustodia solo tenía la frase semilla, y él nunca dejó un camino para llegar a ella. La oferta del foro era una estafa de recuperación: nadie puede saltarse la protección de una billetera de hardware sin su frase semilla.

Conclusiones clave

- Dile a una persona de confianza que tienes cripto y dónde está el plan.
- Guarda el plan y la frase semilla en lugares separados y conocidos.
- Nunca dejes que alguien que se ponga en contacto contigo primero “desbloquee” una billetera.

8.6 Reglas CSF de este capítulo

REGLA PRINCIPAL · OR-007

Planifica la recuperación de tu billetera para emergencias y herencia.

Deja un camino por escrito que tu persona de confianza pueda seguir, guardado aparte de las propias claves.

Regla	Enunciado	Por qué se aplica aquí
OR-003	Documenta cómo se creó tu billetera	Los herederos necesitan saber qué aplicación de billetera, qué dispositivo y qué passphrase se usaron; las palabras por sí solas pueden abrir una billetera vacía.
OR-001	Prueba la recuperación de tu billetera antes de confiar en ella	Un plan que nadie ha recorrido paso a paso es una suposición. Recórrelo una vez al año.
SDR-010	Nunca pagues a nadie para recuperar criptomonedas perdidas	Las familias que buscan cripto son uno de los principales objetivos de los falsos servicios de recuperación.

Tabla 8.3: Reglas CSF complementarias

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

8.7 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
encontraste una billetera de hardware, una frase semilla o notas tras un fallecimiento	Guárdalo todo junto, en privado y sin conexión. Busca primero instrucciones escritas y el testamento. No escribas las palabras en ningún sitio web ni aplicación, y no se las entregues a nadie que te ofrezca ayuda.
sabes que hay cuentas en exchanges	Ponte en contacto con cada exchange a través de su sitio web oficial. Pregunta por su proceso para clientes fallecidos; es probable que te pidan un certificado de defunción y una prueba de que tienes derecho a heredar.
encontraste las palabras pero no sabes de qué billetera son	Busca la aplicación de la billetera en el teléfono o el equipo de la persona, recibos de una billetera de hardware o notas sobre la configuración. Las mismas palabras pueden abrir billeteras distintas según la aplicación y la **passphrase** que se use.
no tienes conocimientos técnicos y la cantidad es importante	Pide a alguien de tu confianza que entienda de cripto que te ayude en persona, en tus propios dispositivos. Nunca aceptes ayuda de alguien que se ponga en contacto contigo primero.
estás planificando para ti	Anota hoy qué billeteras y exchanges usas y dónde están las copias. Dile a una persona de confianza que existe un plan y dónde está.

Tabla 8.4: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Las familias de personas fallecidas son objetivo de falsos servicios de recuperación, falsos abogados y falsos funcionarios que han “encontrado” las cripto. Nadie legítimo te pide una frase semilla, acceso remoto ni una comisión para liberar los fondos. Consulta **Estafas de recuperación** y **Estafas de suplantación de identidad**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/how-to-plan-your-crypto-inheritance-safely/

CAPÍTULO 9

Registros e impuestos

“El exchange había desaparecido, y con él tres años de operaciones.”

Figura 9.1: Registros e impuestos de un vistazo

En muchos países, comprar, vender, hacer swaps (intercambios de tokens) o ganar cripto puede tener consecuencias fiscales. Las normas cambian de un país a otro, y esta guía no las explica. Lo que sí explica es la parte que es casi igual en todas partes: los registros que necesitas y cómo conservarlos antes de que desaparezcan.

La falta de registros es un error de usuario, igual que una copia de seguridad perdida. Un exchange (plataforma de intercambio) cierra, una aplicación deja de funcionar, un equipo portátil se estropea, y años de historial desaparecen con ellos. Este capítulo no es asesoramiento fiscal. Para tu situación concreta, comprueba las normas del lugar donde vives o consulta a un asesor fiscal.

EN ESTE CAPÍTULO

- 9.1 Los registros que vale la pena conservar
- 9.2 Errores al llevar registros que debes conocer
- 9.3 Escenario ilustrativo: el exchange que cerró
- 9.4 Reglas CSF de este capítulo
- 9.5 Si esto te acaba de pasar

9.1 Los registros que vale la pena conservar

Sean cuales sean las **normas fiscales** del lugar donde vives, casi todos los cálculos o consultas parten de los mismos registros:

Registro	Por qué lo necesitas	De dónde sale
Cada compra y venta: fecha, cantidad, precio en tu moneda, comisiones	La base de la mayoría de los cálculos fiscales y la prueba de lo que pagaste	Exportaciones y extractos del exchange; tus propias notas para las operaciones privadas
Swaps entre tokens	En muchos países, un swap cuenta como una venta	Exportaciones del exchange; explorador de bloques para tu dirección
Transferencias entre tus propias billeteras y cuentas	Demuestran que no hubo ninguna venta	Tus propias etiquetas; ID de las transacciones
Ingresos asimilables: recompensas de staking, intereses, airdrops, pagos	A menudo se tratan de forma distinta a las compras	Exportaciones del exchange; historial de la billetera con el valor del día en que se recibieron
Comisiones pagadas	Pueden ser relevantes para el cálculo	Exportaciones del exchange; explorador de bloques
Pérdidas: robos, estafas, plataformas quebradas	Pruebas para las denuncias y, donde se permita, para el tratamiento fiscal	ID de las transacciones, capturas de pantalla, denuncias ante la policía o la plataforma (**cómo denunciar**)
Tu lista de billeteras y cuentas	Para que ni tú ni tus herederos olviden nada	La lista de billeteras que llevas para los capítulos 1 y 8

Tabla 9.1: Los registros que vale la pena conservar

Conserva los registros durante el tiempo que las autoridades de tu país puedan pedirlos, a menudo varios años. Comprueba el plazo del lugar donde vives.

9.2 Errores al llevar registros que debes conocer

1. Ningún registro de lo que pagaste

La blockchain muestra qué se movió y cuándo, pero no el precio en tu moneda. Sin registros de compra, un cálculo posterior tiene que adivinar, y lo que adivina rara vez te favorece. Guarda la fecha de compra, la cantidad, el precio y las comisiones de cada compra.

2. Confiar en que el exchange guarde tu historial

Los exchanges cierran, retiran monedas de cotización (delisting), abandonan países y cierran cuentas. A menudo las exportaciones solo están disponibles mientras todavía puedes iniciar sesión. Descarga tu historial completo con regularidad, no una vez al año.

3. No etiquetar las transferencias entre tus propias billeteras

Mover fondos de un exchange a tu propia billetera de hardware (hardware wallet) no es una venta, pero las herramientas de seguimiento y los extractos pueden mostrarlo como si lo fuera. Etiqueta tus propias transferencias con la billetera a la que fueron y guarda los ID de las transacciones.

4. Olvidar los ingresos asimilables

Las recompensas de staking, los intereses, los airdrops y los pagos en cripto son fáciles de pasar por alto porque no los compraste. En muchos países se tratan de forma distinta a las compras. Registra la fecha y el valor del día en que los recibiste.

5. Perder la pista de tus billeteras

Las billeteras antiguas de teléfonos anteriores, de configuraciones de prueba y de airdrops siguen teniendo historial. Si ya no sabes que existen, tus registros están incompletos. Mantén una única lista de billeteras (**capítulo 1**) y da de baja las billeteras que ya no uses (**capítulo 7**).

6. Dar demasiado acceso a una herramienta de seguimiento

Las herramientas de seguimiento de cartera e impuestos solo necesitan leer. Conéctalas con tus direcciones públicas o con una clave API de solo lectura del exchange; nunca con una clave que pueda operar o retirar, y nunca con tu frase semilla (frase de recuperación). Consulta **herramientas de seguimiento de cartera e impuestos**.

7. Guardar los registros en un solo lugar

Los registros que solo están en una cuenta de exchange, solo en un portátil o solo en una aplicación desaparecen con ella. Guarda una exportación en tu herramienta de seguimiento y una copia sin conexión (offline), y guarda los registros aparte de las copias de tu frase semilla, que nunca deben estar en el mismo archivo ni en la misma carpeta (**capítulo 2**).

8. Esperar al plazo de la declaración

Con la presión del plazo, las exportaciones que faltan ya no existen y los recuerdos se han desvanecido. Exporta cada mes o cada trimestre como parte de tu revisión periódica, y deja que un asesor fiscal se ocupe de las normas.

9.3 Escenario ilustrativo: el exchange que cerró

Este es un escenario ilustrativo, no un caso concreto denunciado.

Kai operó en un exchange pequeño durante tres años y, por el camino, retiró la mayor parte de sus cripto a una billetera de hardware. Entonces el exchange anunció que iba a cerrar. Retiró el resto, pero no descargó su historial de transacciones antes de que el sitio dejara de estar en línea.

Cuando su asesor fiscal le pide los precios de compra, solo tiene sus extractos bancarios y el historial en la blockchain de su billetera de hardware. Reconstruir tres años de operaciones le lleva semanas, y algunas transferencias a su propia billetera parecen ventas.

Qué pasó

Las cripto estaban a salvo; los registros, no. El exchange era el único lugar donde se guardaban sus operaciones, y sus propias transferencias nunca se etiquetaron.

Conclusiones clave

- Exporta el historial de tu exchange con regularidad, y de inmediato cuando una plataforma anuncie cambios.
- Etiqueta las transferencias entre tus propias billeteras.
- Guarda una exportación en tu herramienta de seguimiento y una copia sin conexión.

9.4 Reglas CSF de este capítulo

HÁBITO CLAVE

Mantén un registro completo de cada billetera y cada transacción.

Exporta los historiales con regularidad, etiqueta tus propias transferencias y guarda una copia sin conexión. Esto no es asesoramiento fiscal: comprueba las normas del lugar donde vives o consulta a un asesor fiscal.

Regla	Enunciado	Por qué se aplica aquí
OR-003	Documenta cómo se creó tu billetera	La misma lista de billeteras que te ayuda a restaurar una billetera te indica qué direcciones deben figurar en tus registros.
OR-007	Planifica la recuperación de tu billetera para emergencias y herencia	Tus herederos necesitan tus registros tanto como tu plan de recuperación, para el patrimonio hereditario y para los impuestos.
GR-001	Nunca compartas tu frase semilla	Ninguna herramienta fiscal, ningún asesor contable y ninguna autoridad tributaria necesitan nunca tu frase semilla. Basta con las direcciones públicas o un acceso de solo lectura.

Tabla 9.2: Reglas CSF relacionadas

Las 32 reglas, con lo que previene cada una: **Reglas de seguridad cripto de CSF**.

9.5 Si esto te acaba de pasar

Primero busca tu situación en la tabla “Empieza aquí”, al principio del libro. Después, añade los pasos para tu situación:

Si…	Haz esto ahora
te enteras de que un exchange va a cerrar o a abandonar tu país	Inicia sesión a través de su sitio web oficial y descarga todos los historiales de transacciones, extractos e informes fiscales que ofrezca, en más de un formato si es posible. Después decide qué retirar.
tienes una cuenta que el exchange ha cerrado	Solicita tu historial de transacciones completo a través del canal de soporte oficial. Muchas plataformas están obligadas a conservar los registros durante algunos años y pueden facilitártelos si los pides.
te faltan registros de una billetera	Busca las direcciones de tu billetera en un explorador de bloques de cada red y exporta lo que muestre. Completa los precios con los registros del exchange o del banco de cada compra.
usaste muchas billeteras y no sabes distinguirlas	Haz ahora una lista de billeteras: dirección, red, aplicación de billetera y uso. The Three-Wallet Model® Toolkit (kit de herramientas) incluye una plantilla (**Toolkit**).
te piden pagar impuestos en cripto o “verificar” tu billetera a efectos fiscales	Detente. Las autoridades tributarias reales no cobran impuestos en cripto ni piden acceso a tu billetera. Ponte en contacto con ellas a través de su sitio web oficial. Consulta **Estafas de suplantación de identidad**.
recibiste tokens que nunca pediste	No interactúes con ellos: algunos son estafas que vacían billeteras cuando intentas venderlos. Anótalos si tu asesor lo necesita. Consulta **Estafas de regalos y airdrops**.

Tabla 9.3: Primeras acciones específicas de este capítulo

DESPUÉS DE UNA PÉRDIDA

Si perdiste cripto por un robo o una estafa, tus registros son tu prueba: guarda los ID de las transacciones, las capturas de pantalla y las denuncias. Nadie puede recuperar los fondos a cambio de una comisión. Consulta **Estafas de recuperación**.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo sobre este tema (en inglés):

cryptosafetyfirst.com/crypto-tax-records/

Índice de reglas CSF

Estas son las reglas de CryptoSafetyFirst usadas en este libro, con los capítulos en los que se aplican. El conjunto completo de reglas, con lo que previene cada una, está publicado en **Reglas de seguridad cripto de CSF**. Familias de reglas: GR = Reglas de Oro, OR = Reglas Operativas, SDR = Reglas de Defensa contra Estafas, TSR = Reglas de Seguridad Técnica.

Regla	Enunciado	Capítulos
GR-001	Nunca compartas tu frase semilla	2, 9
GR-003	Usa siempre una billetera de hardware para guardar cripto a largo plazo o de alto valor	1
GR-004	Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos	6, 7
GR-006	Envía siempre una pequeña transacción de prueba antes de transferir grandes cantidades de cripto	4, 5, 6
GR-007	Nunca guardes tu frase semilla en la nube, en el correo ni en capturas de pantalla	2
GR-008	Guarda tus fondos a largo plazo en una billetera bóveda. Usa otra billetera para DApps, trading y Web3	1
OR-001	Prueba la recuperación de tu billetera antes de confiar en ella	2, 3, 7, 8
OR-002	Nunca dependas de una sola copia de tu frase semilla	2
OR-003	Documenta cómo se creó tu billetera	2, 3, 8, 9
OR-004	Nunca guardes tu frase semilla solo en formato digital	2
OR-005	Verifica siempre el destino antes de enviar cripto	4, 5
OR-006	Mantén el acceso a tus sistemas de autenticación	3
OR-007	Planifica la recuperación de tu billetera para emergencias y herencia	8, 9
SDR-003	Nunca pagues para desbloquear o retirar fondos	6

Regla	Enunciado	Capítulos
SDR-010	Nunca pagues a nadie para recuperar criptomonedas perdidas	4, 5, 6, 8
TSR-001	Nunca instales software cripto de fuentes no oficiales	7
TSR-002	Da por hecho que tu dispositivo puede estar comprometido	7
TSR-004	Usa autenticación de dos factores basada en hardware	1, 3
TSR-005	Activa las listas blancas de retiros en los exchanges	1, 4, 5
TSR-006	Separa dispositivos y cuentas para el uso de cripto	3

Reglas CSF usadas en este libro

Sigue aprendiendo

Las billeteras, las redes y las aplicaciones cambian más rápido que cualquier libro. CryptoSafetyFirst.com mantiene viva esta guía entre ediciones:

- **Una página para cada capítulo**, siempre actualizada.
- **The Three-Wallet Model (Modelo de Tres Billeteras)**: una guía y un kit de herramientas gratuitos para configurar billeteras Bóveda, de Uso Frecuente y Desechables.
- Las guías de **estafas** y de **hackeos**, para las pérdidas que no son errores.
- **Herramientas de seguridad prácticas**: lo que previene cada una y lo que no puede hacer.

La mayoría de las pérdidas de cripto no son obra de ningún hacker. Con un plan, una copia probada y una rutina de envío cuidadosa, la mayoría nunca llegan a producirse.

cryptosafetyfirst.com