EDICIÓN 2026

# GUÍA DE PREVENCIÓN DE HACKEOS EN CRIPTO Y WEB3

Cómo mantener tus criptomonedas y activos digitales a salvo de los hackers

JUAN PABLO RENEDO

# Guía de prevención de hackeos en cripto y Web3

Cómo mantener tus criptomonedas y activos digitales a salvo de los hackers

**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 crees que te han hackeado ..... 10
Cómo suelen empezar los hackeos ..... 11
1.1 ¿Hackeo o estafa? La pregunta que lo decide ..... 12
1.2 Dónde suelen empezar los hackeos ..... 13
1.3 Por qué importan las capas ..... 13
1.4 Escenario ilustrativo: la billetera vaciada ..... 14
1.5 Reglas CSF de este capítulo ..... 15
1.6 Si esto te acaba de pasar ..... 15
Malware e infostealers ..... 17
2.1 Qué busca el malware en un usuario de cripto ..... 18
2.2 Cómo llega hoy el malware a tu dispositivo ..... 19
2.3 Señales de que un dispositivo puede estar comprometido ..... 20
2.4 Escenario ilustrativo: la prueba de programación ..... 21
2.5 Cómo protegerte del malware ..... 22
2.6 Reglas CSF de este capítulo ..... 24
2.7 Si esto te acaba de pasar ..... 25
Cadena de suministro y fallos en el software de billeteras ..... 26
3.1 Cómo son los ataques a la cadena de suministro ..... 27
3.2 Un caso real: dispositivos con implantes de un revendedor ..... 27
3.3 Cómo comprar y configurar una billetera de hardware de forma segura ..... 28
3.4 Software de billeteras y bibliotecas comprometidos ..... 29
3.5 Escenario ilustrativo: el dispositivo de oferta ..... 30
3.6 Reglas CSF de este capítulo ..... 31

3.7 Si esto te acaba de pasar ..... 32
Robo de cuentas: correo electrónico, SIM swap, contraseñas y 2FA.... 33
4.1 Tu correo electrónico es la llave maestra ..... 34
4.2 SIM swap: cuando te roban el número de teléfono ..... 35
4.3 Contraseñas y llaves de acceso ..... 35
4.4 Autenticación de dos factores: no toda la 2FA es igual..... 36
4.5 Sesiones robadas: por qué la 2FA no siempre basta..... 36
4.6 Ajustes del exchange que evitan que un robo de cuenta acabe en pérdida ..... 37
4.7 Cuentas de mensajería: robos que llegan a tus contactos..... 37
4.8 Escenario ilustrativo: el SIM swap nocturno ..... 38
4.9 Reglas CSF de este capítulo ..... 39
4.10 Si esto te acaba de pasar ..... 40
Ataques de red y wifi público..... 41
5.1 Los riesgos reales hoy ..... 42
5.2 Lo que sigue importando ..... 42
5.3 Escenario ilustrativo: el inicio de sesión en el aeropuerto..... 43
5.4 Reglas CSF de este capítulo ..... 44
5.5 Si esto te acaba de pasar ..... 45
Brechas en plataformas y ataques internos ..... 46
6.1 Dos tipos de brecha en plataformas ..... 47
6.2 Ataques internos ..... 47
6.3 Cómo limitar tu exposición..... 48
6.4 Escenario ilustrativo: el aviso de brecha ..... 48
6.5 Reglas CSF de este capítulo ..... 49
6.6 Si esto te acaba de pasar ..... 50
Coacción física (ataques de llave inglesa) ..... 51
7.1 Cómo se convierte alguien en objetivo..... 52
7.2 Privacidad: la mejor protección..... 52
7.3 Organiza tus cripto para que haya poco que llevarse ..... 53

7.4 Si ocurre ..... 53
7.5 Reglas CSF de este capítulo ..... 54
7.6 Si esto te acaba de pasar ..... 55
Protección avanzada ..... 56
8.1 Un dispositivo dedicado a cripto ..... 57
8.2 Multisig: más de una clave ..... 57
8.3 Otras opciones comparadas ..... 58
8.4 Hábitos de firma que importan en cualquier nivel ..... 58
8.5 Reglas CSF de este capítulo ..... 59
Si te han hackeado ..... 61
9.1 La primera hora ..... 62
9.2 Encuentra la causa probable ..... 63
9.3 Denúncialo ..... 63
9.4 Reconstruye de forma segura ..... 64
9.5 Reglas CSF de este capítulo ..... 65
Índice de reglas CSF ..... 67
Sigue aprendiendo ..... 69

# Sobre esta edición

La primera edición de esta guía, publicada en enero de 2025 como “How to Keep Your Crypto and Digital Assets Safe from Hackers” (“Cómo mantener tus criptomonedas y activos digitales a salvo de los hackers”), se construyó en torno a cuatro tipos de ataque. Desde entonces, CryptoSafetyFirst ha recopilado y clasificado cada semana pérdidas reales comunicadas por usuarios de cripto. Resultó que la mayoría de los hackeos contra particulares empezaban en el propio dispositivo o en las cuentas del usuario, no en una blockchain vulnerada. La Edición 2026 se ha reconstruido en torno a lo que muestra ese trabajo.

### Novedades

- **Nueve capítulos construidos en torno a la taxonomía de incidentes de CSF,** además de protección avanzada y qué hacer después de un hackeo, para que el libro, el sitio web y las reglas CSF usen las mismas categorías.
- **Capítulos nuevos** sobre ataques a la cadena de suministro, robo de cuentas, brechas en plataformas, coacción física y qué hacer después de un hackeo.
- **Una separación clara con la guía de estafas:** este libro trata lo que ocurre cuando un atacante consigue acceso. El phishing, la suplantación de identidad y las aplicaciones falsas se tratan en la Guía de prevención de estafas y se enlazan aquí.
- **Reglas CSF en cada capítulo,** con una regla principal por capítulo y las reglas de apoyo que la respaldan.
- **Consejos corregidos y actualizados,** incluido lo que realmente demuestran un candado y una comprobación de autenticidad, y por qué el PIN de la tarjeta SIM no detiene un SIM swap (duplicado fraudulento de la tarjeta SIM).

### Cómo se tratan los ejemplos y los datos

- Los escenarios son ilustrativos salvo que se indique claramente lo contrario. Los casos reales se describen con su mes y año, sin nombrar a las empresas ni a las personas implicadas.
- 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.

- No se recomiendan productos ni servicios por su nombre. Cuando se describe un ajuste, consulta el sitio web oficial del proveedor para ver los pasos actuales.

# Cómo usar este libro

| Si… | Ve a |
|---|---|
| acabas de perder fondos y no sabes cómo | Capítulo 9: Si te han hackeado (lista de la primera hora). |
| quieres entender dónde empiezan los hackeos | Capítulo 1. |
| quieres proteger tus dispositivos y billeteras | Capítulos 2, 3 y 8, y la guía gratuita del Three-Wallet Model (Modelo de Tres Billeteras). |
| quieres proteger tus cuentas | Capítulo 4, luego los capítulos 5 y 6. |
| te preocupa tu seguridad personal | Capítulo 7. |

*Por dónde empezar*

### Cómo funciona cada capítulo

La mayoría de los capítulos siguen la misma estructura: una imagen resumen, cómo funciona el ataque, un escenario ilustrativo, cómo protegerte, las reglas CSF de ese capítulo y los primeros pasos si te acaba de pasar. Cada capítulo termina con un enlace a su página, o a la página de la guía, en CryptoSafetyFirst.com.

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).

EMPIEZA AQUÍ

# Si crees que te han hackeado

Mueve lo que te queda antes de investigar. Ve ahora al **capítulo 9**: enumera en orden los pasos de la primera hora —billetera nueva, proteger el correo electrónico, bloquear los exchanges (plataformas de intercambio), llamar a tu operador móvil, revocar las aprobaciones— y explica cómo encontrar después la causa probable.

**CUIDADO CON LAS ESTAFAS DE RECUPERACIÓN**

Después de un hackeo, es posible que te contacten 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 (frase de recuperación) ni tu clave privada, y no pagues a nadie que diga que hace falta una comisión para liberar tus fondos. Consulta **Estafas de recuperación**.

CAPÍTULO 1

# Cómo suelen empezar los hackeos

*“Nunca compartí mi frase semilla. ¿Cómo entraron?”*

*Figura 1.1: Cómo suelen empezar los hackeos de un vistazo*

Ningún sistema está libre de riesgos, ni en las finanzas tradicionales ni en cripto. Pero quienes tienen cripto son objetivos más atractivos que la mayoría: los fondos pueden moverse en minutos, las transferencias no se pueden revertir y una sola billetera o cuenta suele guardar gran parte de los ahorros de una persona. Por eso las cripto necesitan más cuidado que la banca en línea, no menos.

La buena noticia es que los hackeos contra usuarios individuales siguen un número reducido de patrones. Cada uno tiene defensas que funcionan y, combinadas en capas, evitan que un solo punto débil te cueste todo. Este capítulo explica qué se considera un hackeo, dónde suelen empezar los hackeos y cómo se organiza el resto de este libro en torno a ellos.

EN ESTE CAPÍTULO


- 1.1 ¿Hackeo o estafa? La pregunta que lo decide
- 1.2 Dónde suelen empezar los hackeos
- 1.3 Por qué importan las capas
- 1.4 Escenario ilustrativo: la billetera vaciada
- 1.5 Reglas CSF de este capítulo
- 1.6 Si esto te acaba de pasar


## 1.1 ¿Hackeo o estafa? La pregunta que lo decide

Las guías de CryptoSafetyFirst clasifican las pérdidas según una pregunta: **¿quién realizó la acción que movió los fondos o accedió a la cuenta?**

- **Una estafa:** te convencieron para que actuaras tú mismo y enviaras cripto, firmaras una transacción, conectaras tu billetera o compartieras tu frase semilla (frase de recuperación). Se trata en la **Guía de prevención de estafas**.
- **Un hackeo:** un atacante obtuvo acceso a tu dispositivo, tu cuenta o tu billetera y actuó sin tu aprobación. Se trata en este libro.
- **Un error de usuario:** nadie te atacó; falló una copia de seguridad, una dirección o un ajuste. Se trata en la **Guía de prevención de errores de usuario**.

Muchos hackeos empiezan con un engaño (una descarga falsa, un enlace, un mensaje) y luego continúan sin ti. Este libro empieza donde termina el engaño: en el momento en que un atacante obtiene acceso.

## 1.2 Dónde suelen empezar los hackeos

| Punto de entrada | Qué obtiene el atacante | Capítulo |
|---|---|---|
| Un programa, una extensión o un comando que te convencieron de ejecutar | El control de tu dispositivo, de los archivos de tu billetera y de las cuentas en las que tienes la sesión iniciada | 2 |
| Un dispositivo manipulado o una app o biblioteca de billetera comprometida | Tu frase semilla o tus transacciones, antes de que uses la billetera | 3 |
| Tu correo electrónico, tu número de teléfono o tus contraseñas | Tus cuentas de exchange (plataforma de intercambio) y de billetera, mediante restablecimientos de contraseña y sesiones robadas | 4 |
| Una red que no controlas | Tráfico redirigido y páginas de inicio de sesión falsas | 5 |
| Una plataforma que guarda tus cripto o tus datos | Tus fondos en esa plataforma, o tu nombre y tu dirección postal | 6 |
| Tu casa y tu perfil público | Presión física sobre ti o tu familia | 7 |

*Tabla 1.1: Los puntos de entrada habituales y dónde los trata este libro*

Las páginas de phishing, el soporte falso, la suplantación de identidad y las apps falsas son el primer paso más común. Se tratan en detalle en la guía de estafas: **Estafas de ingeniería social**, **Estafas de phishing** y **Aplicaciones y billeteras falsas**.

## 1.3 Por qué importan las capas

Todas las defensas de este libro tienen un punto débil. Una billetera de hardware (hardware wallet) no impide que apruebes una transacción maliciosa; la 2FA no detiene una sesión robada; una contraseña segura no sirve de nada si te roban el correo electrónico. Lo que funciona son varias capas, para que un solo fallo no baste:

- **Separa tus cripto:** los ahorros en una billetera Bóveda que nunca se conecta a sitios web, y la actividad diaria en otra billetera

(consulta **The Three-Wallet Model [Modelo de Tres Billeteras]**).

- **Protege el dispositivo:** solo software oficial, un dispositivo o una cuenta aparte para cripto, y las claves en una billetera de hardware (capítulos 2 y 3).
- **Protege las cuentas:** un correo aparte para cripto, 2FA basada en hardware y listas blancas de retiros (**capítulo 4**).
- **Protégete a ti mismo:** mantén en privado tus fondos y planifica para el día en que algo salga mal (capítulos 7 y 9).

## 1.4 Escenario ilustrativo: la billetera vaciada

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

Sam se despierta con la billetera vacía. Nunca compartió su frase semilla ni firmó nada fuera de lo normal. Cambia su contraseña, pero al día siguiente también le vacían la cuenta del exchange.

### Qué pasó

Una “herramienta de trading gratuita” que Sam había instalado semanas antes era un infostealer (malware que roba información). Copió los datos de su billetera y la sesión iniciada de su exchange. Cambiar la contraseña en el mismo equipo infectado no sirvió de nada: el atacante ya estaba dentro.

### Conclusiones clave

- Si te vacían la billetera sin que hayas firmado nada, normalmente significa que tu dispositivo o tu frase semilla están comprometidos.
- Actúa desde un dispositivo limpio y mueve los fondos antes de investigar.
- **El capítulo 9** tiene la lista de la primera hora para exactamente esta situación.

## 1.5 Reglas CSF de este capítulo

**REGLA PRINCIPAL · TSR-007**

### Tómate tu tiempo antes de hacer clic o instalar.

La mayoría de los hackeos dependen de un solo clic, una instalación o un comando hechos con prisa.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | La mayoría de los hackeos empiezan con un mensaje, un enlace o un archivo que no pediste. |
| SDR-009 | Verifica todos los enlaces antes de iniciar sesión | Una página de inicio de sesión copiada le entrega al atacante tu contraseña y tu código 2FA. |
| GR-005 | Nunca sigas instrucciones urgentes de soporte o seguridad. Sal del canal y vuelve a entrar por la app o la URL oficial | Las alertas de seguridad falsas son una forma habitual de conseguir que instales algo o inicies sesión. |
| GR-008 | Guarda tus fondos a largo plazo en una billetera bóveda. Usa otra billetera para DApps, trading y Web3 | Un hackeo de tu billetera de uso diario no debería llegar a tus ahorros. |

*Tabla 1.2: Reglas CSF para el primer paso de un hackeo*

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

## 1.6 Si esto te acaba de pasar

Si han salido fondos de tu billetera o de tu cuenta y no sabes por qué, ve directamente al **capítulo 9**: Si te han hackeado. Actúa desde un dispositivo limpio y mueve lo que quede antes de investigar.

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para rastrear o recuperar las cripto robadas. Nadie puede revertir una transferencia confirmada a cambio de una comisión. Consulta **Estafas de recuperación** y denuncia el robo: **Cómo denunciar una estafa cripto**.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

Todos los capítulos, novedades y guías relacionadas están en la página de la guía (en inglés):

**cryptosafetyfirst.com/keep-your-crypto-safe-from-hackers/**

CAPÍTULO 2

# Malware e infostealers

*“Solo ejecuté el script de instalación de la prueba de programación.”*

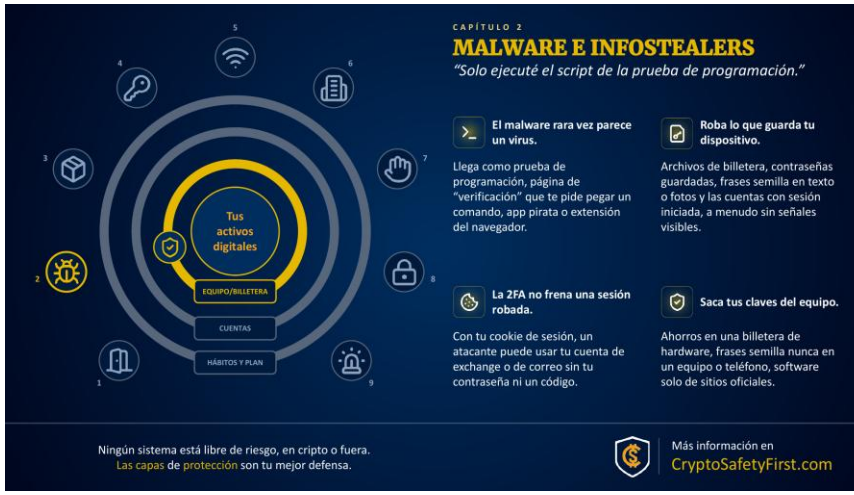


*Figura 2.1: Malware e infostealers de un vistazo*

La mayoría de los hackeos contra usuarios individuales de cripto no rompen ningún cifrado. Empiezan en el propio dispositivo del usuario: un programa que parece útil, una extensión del navegador, un paso de “verificación” o un archivo de un contacto nuevo. Una vez que el malware se ejecuta, puede leer lo que escribes y guardas, cambiar lo que pegas y usar las cuentas en las que tienes la sesión iniciada, a menudo sin ninguna señal visible.

Este capítulo explica qué roba el malware a los usuarios de cripto, cómo llega hoy a los equipos y teléfonos, las señales de que un dispositivo puede estar comprometido y los hábitos que evitan que un solo dispositivo infectado te cueste todo.

EN ESTE CAPÍTULO


- 2.1 Qué busca el malware en un usuario de cripto
- 2.2 Cómo llega hoy el malware a tu dispositivo
- 2.3 Señales de que un dispositivo puede estar comprometido
- 2.4 Escenario ilustrativo: la prueba de programación
- 2.5 Cómo protegerte del malware
- 2.6 Reglas CSF de este capítulo
- 2.7 Si esto te acaba de pasar


## 2.1 Qué busca el malware en un usuario de cripto

El malware cripto no necesita “hackear” una blockchain. Busca todo lo que haya en tu dispositivo que pueda mover tus fondos o acceder a tus cuentas.

| Tipo | Qué roba | Por qué hace daño |
|---|---|---|
| Infostealer (malware que roba información) | Archivos de billeteras y datos de extensiones del navegador, contraseñas guardadas, frases semilla (frases de recuperación) guardadas como texto, fotos o notas, y cookies de sesión del navegador | Las cookies de sesión permiten a un atacante usar una cuenta en la que ya tienes la sesión iniciada, sin tu contraseña ni tu código 2FA. |
| Clipboard swapper (malware que reemplaza lo que copias en el portapapeles) | Nada al principio: espera a que copies una dirección cripto y la reemplaza por la del atacante | La transferencia parece normal y se confirma. Los fondos van al atacante y no se pueden revertir. |
| Troyano de acceso remoto (RAT) | El control de todo el equipo: pantalla, teclado, archivos y apps abiertas | El atacante puede actuar como si fuera tú, en un momento en que no estás mirando. |
| App de billetera falsa o aviso de actualización falso | Tu frase semilla, escrita en una ventana que se parece a tu software de billetera | Escribir una sola vez tu frase semilla entrega todas las cuentas de esa billetera, en todas las redes. |

*Tabla 2.1: Qué roba el malware cripto*

Los PC con Windows no son el único objetivo. Los Mac son cada vez más atacados, y también los teléfonos: apps de billetera falsas, apps que leen las capturas de pantalla de tu galería de fotos y teléfonos de segunda mano que ya vienen con malware instalado.

## 2.2 Cómo llega hoy el malware a tu dispositivo

El malware rara vez llega como un virus evidente. Normalmente es algo que te convencieron de ejecutar tú mismo.

### 1. Entrevistas de trabajo y pruebas de programación falsas

Un reclutador o una "empresa Web3" te ofrece un trabajo remunerado y luego te pide que clones un repositorio de código, ejecutes un script de instalación, instales una app de reuniones o abras un archivo de proyecto. El script instala malware. Los desarrolladores y los community managers son los principales objetivos. La parte de la estafa de empleo se trata en el **capítulo 11 de la Guía de prevención de estafas**.

### 2. Páginas de "verificación" que te piden pegar un comando

Una página muestra un CAPTCHA falso, una "verificación humana" o un mensaje de error y te pide que presiones una combinación de teclas, pegues algo en el cuadro Ejecutar o en Terminal y presiones Enter. Ningún sitio web real necesita esto nunca. El comando descarga malware con tus propios permisos.

### 3. Anuncios patrocinados, sitios de descarga que imitan al real y enlaces de chatbots

Los anuncios patrocinados en buscadores, los anuncios en redes sociales y las páginas de descarga copiadas ofrecen apps de billetera, herramientas de trading o software de uso diario con malware dentro. Los enlaces que sugieren los chatbots de IA pueden llevar a los mismos sitios que imitan al real. Descarga software solo desde la dirección del sitio web oficial del desarrollador, escrita por ti mismo o guardada en tus marcadores.

### 4. Extensiones del navegador y bookmarklets

Las extensiones pueden leer y cambiar todas las páginas que abres, incluidas las pestañas de tu billetera y de tu exchange (plataforma de intercambio). Algunas son maliciosas desde el principio; otras se

vuelven maliciosas con una actualización después de haber reunido usuarios. Los bookmarklets (marcadores que ejecutan código) de “bots de trading” que se comparten en Discord o Telegram ejecutan código dentro de la página en la que tienes la sesión iniciada. Las extensiones de billetera falsas se tratan en el **capítulo 4 de la Guía de prevención de estafas**.

### 5. Software pirata, trucos para juegos y “herramientas gratuitas”

Los programas pirata, los trucos para juegos, las “herramientas de IA” gratuitas y las aplicaciones de minería son una vía habitual para distribuir infostealers. Si algo de pago se ofrece gratis desde una fuente no oficial, da por hecho que el precio son tus datos.

### 6. Archivos e invitaciones de contactos nuevos

Un contacto que conociste en línea te envía un documento, un archivo de proyecto “cifrado”, un juego para probar en su servidor o un enlace a una reunión que requiere una aplicación especial. Las semanas de conversación amistosa son parte del método, no una prueba de confianza.

## 2.3 Señales de que un dispositivo puede estar comprometido

Muchas infecciones no muestran ninguna señal. Si aparece alguna de estas, deja de usar el dispositivo para cripto y sigue los pasos del final de este capítulo.

- Una dirección pegada es distinta de la que copiaste.
- El software de tu billetera te pide de repente que escribas tu **frase semilla**, que “vuelvas a verificar” la billetera o que corrijas un error de firmware. Las aplicaciones de billeteras de hardware (hardware wallets) no te piden que escribas tu frase semilla en una ventana emergente o de “verificación”. Una recuperación real es algo que inicias tú mismo, siguiendo las instrucciones oficiales del fabricante.
- Extensiones, programas o ajustes del navegador que no añadiste, como un proxy cambiado o un nuevo buscador predeterminado.

- Alertas de inicio de sesión, dispositivos nuevos o sesiones activas en tus cuentas de correo electrónico o de exchange que no son tuyos.
- Las cuentas cambian solas: mensajes enviados desde tus perfiles de redes sociales, claves API (API keys) nuevas, ajustes de retiro modificados.

La ausencia de señales de alerta no significa que el dispositivo esté limpio. Un infostealer puede copiarlo todo en segundos sin dejar nada visible.

## 2.4 Escenario ilustrativo: la prueba de programación

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

Un reclutador de una startup Web3 contacta a Daniel, un desarrollador independiente, a través de una red profesional. Después de dos llamadas amistosas, le envían un repositorio para una breve prueba de programación remunerada y le piden que ejecute el script de instalación antes de la siguiente entrevista.

El script se ejecuta en segundo plano mientras Daniel trabaja en la tarea. Dos días después, su billetera del navegador está vacía y alguien ha iniciado sesión en su cuenta del exchange desde otro país, sin su contraseña ni su código 2FA.

### Qué pasó

El script de instalación instaló un infostealer. Copió los datos de su billetera del navegador y la cookie de sesión de su cuenta del exchange. El atacante no tuvo que romper nada: el equipo entregó lo que contenía.

### Conclusiones clave

- En el equipo que usas para cripto, nunca ejecutes código, scripts ni instaladores enviados por alguien que conociste en línea.
- Un dispositivo que ejecuta software desconocido no es lugar para billeteras ni para inicios de sesión en exchanges.
- Una billetera de hardware habría mantenido las claves de los ahorros de Daniel fuera del equipo.

## 2.5 Cómo protegerte del malware

- **Instala software cripto solo desde fuentes oficiales.** Escribe tú mismo la dirección del sitio web del desarrollador o usa un marcador; nunca sigas anuncios, resultados de búsqueda, enlaces de chats ni sugerencias de chatbots para descargar nada.
- **Mantén tus cripto en un dispositivo o una cuenta de usuario separados.** Usa un equipo, o al menos una cuenta y un perfil del navegador separados, solo para billeteras y exchanges, sin juegos, software pirata, código de prueba ni extensiones al azar.
- **Guarda tus ahorros en una billetera de hardware.** Sus claves nunca salen del dispositivo, así que el malware del equipo no puede copiarlas. Comprueba cada dirección e importe en la propia pantalla de la billetera de hardware antes de aprobar.
- **Nunca guardes una frase semilla en un dispositivo.** Nada de archivos de texto, fotos, notas, gestores de contraseñas ni unidades en la nube. Escríbela en papel o metal (consulta el **capítulo 2 de la Guía de prevención de errores de usuario**).
- **Nunca pegues un comando que te pida un sitio web.** Cierra la página.
- **Usa el mínimo de extensiones.** Elimina las que ya no uses y desconfía de cualquier extensión que de repente pida permisos nuevos.
- **Actualiza tu sistema, tu navegador y tus aplicaciones de billetera.** Instala las actualizaciones desde la propia aplicación o el propio sistema, nunca desde una ventana emergente ni desde un enlace.
- **Considera el software de seguridad una base, no una garantía.** El antivirus integrado ayuda contra el malware conocido; no detecta todo lo nuevo. Consulta **Herramientas de seguridad** para ver qué cubre cada herramienta.

| Defensa | Qué evita | Qué no evita |
|---|---|---|
| Billetera de hardware | Que el malware copie tus claves privadas | Que tú apruebes una transacción o una dirección maliciosas en su pantalla |
| Dispositivo o cuenta separados para cripto | Que una infección del uso diario llegue a tus billeteras | El malware que tú mismo instales en ese dispositivo |
| Comprobar la dirección completa en la pantalla del dispositivo | Clipboard swappers | Una dirección equivocada que elegiste tú mismo |
| Antivirus y actualizaciones | Malware conocido y fallos de seguridad conocidos | Malware nuevo y cualquier cosa que ejecutes a propósito |

*Tabla 2.2: Qué cubre cada defensa*

## 2.6 Reglas CSF de este capítulo

REGLA PRINCIPAL · TSR-002

### Da por hecho que tu dispositivo puede estar comprometido.

Comprueba las direcciones y las transacciones en la pantalla de la billetera de hardware y mantén los secretos fuera del equipo.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| TSR-001 | Nunca instales software cripto de fuentes no oficiales | Las billeteras, extensiones y herramientas de trading falsas son la vía más común por la que llega el malware. |
| TSR-006 | Separa dispositivos y cuentas para el uso de cripto | Un dispositivo infectado no debería exponer todas tus cripto a la vez. |
| TSR-007 | Tómate tu tiempo antes de hacer clic o instalar | Casi todas las infecciones empiezan por instalar, hacer clic o pegar un comando con prisa. |
| GR-003 | Usa siempre una billetera de hardware para guardar cripto a largo plazo o de alto valor | El malware del equipo no puede copiar las claves de una billetera de hardware. |
| GR-007 | Nunca guardes tu frase semilla en la nube, en el correo ni en capturas de pantalla | Los infostealers buscan exactamente estos archivos y fotos. |

*Tabla 2.3: Reglas CSF para malware e infostealers*

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

## 2.7 Si esto te acaba de pasar

Para ver la lista completa de la primera hora, consulta el **capítulo 9**: Si te han hackeado. Los pasos específicos para malware:

| Si… | Haz esto ahora |
|---|---|
| ejecutaste un archivo, script o comando sospechoso | Desconecta el dispositivo de internet. No vuelvas a escribir contraseñas ni frases semilla en él. Desde un dispositivo limpio, mueve los fondos de todas las billeteras que se hayan usado alguna vez en él a billeteras nuevas con frases semilla nuevas. |
| ves que cambia una dirección pegada | No envíes nada. Deja de usar el dispositivo para cripto hasta que lo hayas borrado por completo y reinstalado. |
| escribiste tu frase semilla en una aplicación o ventana | Considera la frase semilla comprometida. En un dispositivo limpio, crea una billetera nueva y mueve todo ahora, también desde cualquier billetera de hardware que use la misma frase semilla. |
| ves inicios de sesión o cambios que no hiciste | Desde un dispositivo limpio: cambia primero la contraseña del correo electrónico, cierra todas las sesiones, revoca las claves API, revisa las listas blancas de retiros y después cambia las contraseñas de los exchanges. |

*Tabla 2.4: Primeros pasos después de una infección de malware*

Borrar por completo y reinstalar va al final, cuando los fondos ya estén a salvo: un sistema limpio no hace que una frase semilla comprometida vuelva a ser segura.

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para rastrear o recuperar las cripto robadas. Nadie puede revertir una transferencia confirmada a cambio de una comisión. Consulta **Estafas de recuperación** y denuncia el robo: **Cómo denunciar una estafa cripto**.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

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

**cryptosafetyfirst.com/malware-attacks-cryptocurrency/**

CAPÍTULO 3

# Cadena de suministro y fallos en el software de billeteras

*“Venía precintado, pasó la comprobación… y a mitad de precio.”*

*Figura 3.1: Cadena de suministro y fallos en el software de billeteras de un vistazo*

Una billetera de hardware (hardware wallet) protege tus claves del equipo al que está conectada. No puede protegerte de un dispositivo que fue manipulado antes de llegar a ti, ni de una aplicación de billetera comprometida en su origen. Estos ataques son más raros que el malware, pero cuando ocurren, afectan a usuarios cuidadosos que hicieron bien todo lo demás.

Este capítulo trata las dos caras del riesgo de la cadena de suministro (supply chain) —el dispositivo que compras y el software que ejecutas— y los hábitos sencillos de compra y actualización que eliminan la mayor parte de ese riesgo.

EN ESTE CAPÍTULO


- 3.1 Cómo son los ataques a la cadena de suministro
- 3.2 Un caso real: dispositivos con implantes de un revendedor
- 3.3 Cómo comprar y configurar una billetera de hardware de forma segura
- 3.4 Software de billeteras y bibliotecas comprometidos
- 3.5 Escenario ilustrativo: el dispositivo de oferta
- 3.6 Reglas CSF de este capítulo
- 3.7 Si esto te acaba de pasar


## 3.1 Cómo son los ataques a la cadena de suministro

- **Una billetera de hardware manipulada:** un dispositivo modificado entre la fábrica y tú, vendido casi siempre por un revendedor o por un vendedor de un marketplace (tienda en línea de terceros), a veces por debajo del precio normal.
- **Un dispositivo con una frase semilla (frase de recuperación) preconfigurada:** una billetera que llega con una frase semilla ya impresa en una tarjeta, o con instrucciones para usar una frase semilla proporcionada en lugar de crear una nueva.
- **Una aplicación o actualización de billetera comprometida:** un atacante modifica el software oficial, o una biblioteca de código que este usa, para que robe claves o cambie direcciones.
- **Datos de clientes filtrados:** una brecha en un vendedor expone los nombres y direcciones postales de los compradores, que luego se usan para phishing, envíos falsos de “dispositivos de reemplazo” y amenazas (capítulos 6 y 7).

## 3.2 Un caso real: dispositivos con implantes de un revendedor

En octubre de 2026, un importante fabricante de billeteras de hardware confirmó que los dispositivos vendidos a través de un revendedor del sudeste asiático, que varios fabricantes tenían en su lista de revendedores autorizados, contenían un implante de hardware añadido. El implante leía la **frase semilla** que aparecía en la pantalla del

dispositivo durante la configuración y la enviaba a través de una conexión móvil (LTE) integrada. Los compradores que configuraron estos dispositivos descubrieron más tarde que les habían vaciado los fondos. Según se informó, también se vendieron unidades en marketplaces en línea a cerca de la mitad del precio normal. Un gran minorista europeo de electrónica suspendió brevemente las ventas tras el aviso de un cliente; el fabricante dijo después que no había encontrado existencias manipuladas en Europa.

El fabricante señaló que su comprobación de autenticidad no puede detectar un implante añadido cuando el chip seguro original está intacto. Dicho de otro modo: **un resultado de "auténtico" confirma el chip, no el dispositivo completo.**

Ese mismo mes, otro fabricante de billeteras de hardware informó de que un atacante había robado datos de clientes y de envíos de su tienda en línea, junto con la clave que usaba su verificación en línea de dispositivos, lo que significa que dispositivos falsificados podían superar esa verificación. El fabricante anunció que destruiría sus existencias sin vender y emitiría dispositivos con una clave nueva. Las frases semilla y las claves privadas no se vieron afectadas, y los dispositivos entregados antes de la intrusión siguieron siendo seguros.

Las lecciones de ambos casos: **superar una comprobación de autenticidad no es prueba suficiente por sí sola, un canal autorizado reduce el riesgo pero no lo elimina y, después de cualquier filtración, es probable que recibas cartas, paquetes y mensajes dirigidos específicamente a ti, aunque hayas comprado directamente al fabricante.**

## 3.3 Cómo comprar y configurar una billetera de hardware de forma segura

- **Compra directamente en la tienda oficial del fabricante,** escribiendo tú mismo su dirección. Ese es el canal más seguro. Un revendedor autorizado, que aparezca en el sitio web del fabricante, reduce el riesgo pero no lo elimina.
- **Nunca compres dispositivos de segunda mano, devueltos, de "caja abierta" o inusualmente baratos,** y nunca aceptes uno como regalo de alguien a quien conociste en línea.

- **Comprueba el embalaje y el dispositivo** con la descripción del fabricante. Si hay cualquier señal de apertura, un peso distinto o una pieza suelta, no lo configures.
- **Crea siempre una frase semilla nueva en el propio dispositivo.** Un dispositivo que llega con una frase semilla, o que te indica que uses una frase semilla incluida en lugar de crear una nueva, ha sido manipulado.
- **Escribe la frase semilla solo en papel o metal,** nunca en un equipo ni en un teléfono.
- **Actualiza el firmware solo a través de la app oficial del dispositivo,** nunca desde un enlace, un correo o una ventana emergente.
- **Prueba primero con una cantidad pequeña** y después envía más.

## 3.4 Software de billeteras y bibliotecas comprometidos

Las apps de billetera, las extensiones del navegador y los sitios web de las aplicaciones descentralizadas se construyen sobre bibliotecas de código compartidas. Cuando un atacante toma el control de una de ellas (por ejemplo, mediante una cuenta de desarrollador robada), el cambio puede llegar a muchas apps a la vez. Entre los casos pasados están una biblioteca de código usada por muchos sitios web de dApps, alterada en diciembre de 2023, y paquetes de desarrollo muy utilizados, alterados en septiembre de 2025 para cambiar direcciones cripto en los navegadores.

No puedes auditar este código por tu cuenta. Lo que sí puedes hacer:

- Comprueba cada dirección y cada importe en la propia pantalla de tu billetera de hardware antes de aprobar. Una app comprometida puede mostrar una cosa en el equipo y enviar otra.
- Evita la firma a ciegas (blind signing): si el dispositivo no puede mostrar lo que estás aprobando, no lo apruebes con tus ahorros.
- Cuando se informe de que una billetera, una extensión o una dApp que usas está comprometida, deja de usarla hasta que el canal oficial del desarrollador diga que la corrección ya está disponible. Consulta el sitio web o la cuenta oficial, no los mensajes que te lleguen.

- Guarda los fondos a largo plazo en una billetera Bóveda que no se conecte nunca a dApps, para que una interfaz (front end) de dApp comprometida no pueda alcanzarla.

## 3.5 Escenario ilustrativo: el dispositivo de oferta

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

Lena quiere sacar sus ahorros de un exchange (plataforma de intercambio). Encuentra la billetera de hardware que ha elegido en un gran marketplace muy por debajo del precio habitual, precintada y con buenas valoraciones del vendedor. La configuración funciona, la comprobación de autenticidad se supera y transfiere sus ahorros. Tres semanas después, han desaparecido.

### Qué pasó

El dispositivo había sido abierto y modificado antes de volver a precintarlo y venderlo. La frase semilla se capturó durante la configuración. Nada de lo que Lena hiciera después podría haberlo evitado.

### Conclusiones clave

- Una billetera de hardware solo es tan fiable como el lugar donde la compraste.
- Un precio bajo en un dispositivo de seguridad es una advertencia, no una oferta.
- Una comprobación de autenticidad confirma el chip, no que no se haya añadido nada.

## 3.6 Reglas CSF de este capítulo

**REGLA PRINCIPAL · TSR-001**

### Nunca instales software cripto de fuentes no oficiales.

Lo mismo se aplica al hardware: compra directamente en la tienda oficial del fabricante; un revendedor autorizado reduce el riesgo pero no lo elimina.

| 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 | Sigue siendo la mejor protección para los ahorros, siempre que el propio dispositivo sea de confianza. |
| TSR-002 | Da por hecho que tu dispositivo puede estar comprometido | Verifica las direcciones y los importes en la pantalla de la billetera de hardware, no en el equipo. |
| GR-008 | Guarda tus fondos a largo plazo en una billetera bóveda. Usa otra billetera para DApps, trading y Web3 | Una dApp o una extensión comprometida no puede alcanzar una billetera que nunca se conecta. |

*Tabla 3.1: Reglas CSF para los riesgos de la cadena de suministro*

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

## 3.7 Si esto te acaba de pasar

Para ver la lista completa de la primera hora, consulta el **capítulo 9**. Los pasos específicos para los riesgos de la cadena de suministro:

| Si… | Haz esto ahora |
|---|---|
| compraste una billetera de hardware a un revendedor o en un marketplace y tienes dudas | No la configures. Ponte en contacto con el fabricante a través de su sitio web oficial y pregunta cómo confirmar que es auténtica. |
| recibiste un dispositivo después de que su fabricante informara de una brecha | Antes de configurarlo, consulta el aviso oficial del fabricante para saber si tu dispositivo está afectado. |
| ya usas un dispositivo de un vendedor que, según se ha informado, está comprometido | Compra un dispositivo nuevo directamente al fabricante, crea en él una frase semilla nueva y transfiere a él todos los fondos. No reutilices la frase semilla antigua. |
| usas una app de billetera o una extensión que, según se ha informado, está comprometida | Deja de usarla. Sigue las instrucciones oficiales del desarrollador; si las claves pueden estar expuestas, transfiere los fondos a una billetera nueva con una frase semilla nueva. |
| recibiste una carta, un paquete o un mensaje sobre un “dispositivo de reemplazo” después de una filtración de datos | No le hagas caso y no introduzcas tu frase semilla en ningún sitio. Los fabricantes no envían dispositivos que no hayas solicitado. |

*Tabla 3.2: Primeros pasos ante los riesgos de la cadena de suministro*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para rastrear o recuperar las cripto robadas. Nadie puede revertir una transferencia confirmada a cambio de una comisión. Consulta **Estafas de recuperación** y denuncia el robo: **Cómo denunciar una estafa cripto**.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

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

**cryptosafetyfirst.com/hardware-wallet-supply-chain-attacks/**

CAPÍTULO 4

# Robo de cuentas: correo electrónico, SIM swap, contraseñas y 2FA

*“Mi teléfono se quedó sin servicio. Una hora después, me quedé sin fondos.”*

*Figura 4.1: Robo de cuentas de un vistazo*

Tu cuenta del exchange (plataforma de intercambio), la copia de seguridad en la nube de tu app de billetera y tu herramienta fiscal de cripto solo son tan seguras como las cuentas que hay detrás: tu correo electrónico, tu número de teléfono y tus contraseñas. Los atacantes rara vez entran directamente en un exchange. Toman el control del correo que puede restablecer su contraseña, del número de teléfono que recibe sus códigos o de la sesión del navegador que ya está iniciada.

Este capítulo explica cómo se producen los robos de cuenta (account takeover) —correo comprometido, SIM swap (duplicado fraudulento de la tarjeta SIM), contraseñas reutilizadas, sesiones robadas y cuentas de mensajería secuestradas— y cómo configurar tus cuentas para que una sola contraseña o un solo código robados no basten.

EN ESTE CAPÍTULO


- 4.1 Tu correo electrónico es la llave maestra
- 4.2 SIM swap: cuando te roban el número de teléfono
- 4.3 Contraseñas y llaves de acceso
- 4.4 Autenticación de dos factores: no toda la 2FA es igual
- 4.5 Sesiones robadas: por qué la 2FA no siempre basta
- 4.6 Ajustes del exchange que evitan que un robo de cuenta acabe en pérdida
- 4.7 Cuentas de mensajería: robos que llegan a tus contactos
- 4.8 Escenario ilustrativo: el SIM swap nocturno
- 4.9 Reglas CSF de este capítulo
- 4.10 Si esto te acaba de pasar


## 4.1 Tu correo electrónico es la llave maestra

Casi cualquier cuenta se puede restablecer por correo electrónico. Quien controla tu correo normalmente puede tomar el control de todo lo que está vinculado a él. Trata el correo de tus cuentas cripto como la cuenta más importante que tienes:

- **Usa una dirección de correo distinta solo para las cuentas cripto,** no la que das a tiendas, boletines y redes sociales. Recibirá menos phishing, y una filtración en otro sitio no la revelará.
- **Protege ese correo con una llave de seguridad física (hardware security key) o una llave de acceso (passkey),** y elimina el SMS como opción de inicio de sesión o de recuperación. Encontrarás opciones en nuestra página **Herramientas de seguridad**.
- **Revisa sus ajustes cada tres meses:** correo y teléfono de recuperación, reglas de reenvío, apps conectadas y sesiones activas. Los atacantes suelen añadir una regla de reenvío y pasar desapercibidos.
- **Guarda sus códigos de recuperación sin conexión,** con tus otras copias de seguridad (consulta el **capítulo 3 de la Guía de prevención de errores de usuario**).

## 4.2 SIM swap: cuando te roban el número de teléfono

En un SIM swap, un atacante convence a tu operador móvil (o soborna a alguien que trabaja allí) para que transfiera tu número a una tarjeta SIM o eSIM que él controla. Tu teléfono pierde la señal de repente. A partir de ese momento, cada código por SMS y cada "restablecimiento por mensaje de texto" va al atacante.

El PIN de la tarjeta SIM no protege contra esto: solo bloquea la tarjeta física de tu teléfono. Lo que ayuda:

- **Elimina tu número de teléfono como método de 2FA y como opción de recuperación** en el correo, los exchanges y las apps de billetera, siempre que el servicio lo permita.
- **Pide a tu operador móvil protección para tu cuenta:** un PIN o una contraseña de cuenta independiente y un bloqueo de la portabilidad del número y de los cambios de SIM sin identificación en persona, si lo ofrece.
- **Mantén tu número de teléfono en privado.** Si un servicio insiste en pedirte un número de teléfono, usa un número aparte que utilices solo para eso y que nunca publiques.
- **Trata un "Sin servicio" repentino como una emergencia** si no has cambiado nada: llama a tu operador móvil desde otro teléfono y protege tu correo electrónico desde otro dispositivo.

## 4.3 Contraseñas y llaves de acceso

- **Usa una contraseña distinta para cada cuenta.** Las contraseñas robadas de un sitio filtrado se prueban automáticamente en exchanges y proveedores de correo electrónico.
- **Deja que un gestor de contraseñas de confianza las cree y las guarde.** Contraseñas largas y aleatorias o una frase de contraseña de varias palabras aleatorias; sin datos personales. Consulta **Herramientas de seguridad**.
- **No necesitas cambiar periódicamente las contraseñas seguras y únicas.** Cámbialas cuando un servicio informe de una brecha o sospeches que hay un problema.
- **Usa llaves de acceso donde se ofrezcan.** Una llave de acceso no se puede escribir en un sitio falso, así que resiste el phishing.

Asegúrate de que puedes seguir iniciando sesión si pierdes el teléfono o la cuenta que la guarda.

- **Nunca guardes tu frase semilla (frase de recuperación) en el gestor de contraseñas.** Es para contraseñas, no para las claves de tu billetera.

## 4.4 Autenticación de dos factores: no toda la 2FA es igual

| Método | Protege contra | Principal debilidad |
|---|---|---|
| Llave de seguridad física o llave de acceso | Robo de contraseñas, páginas de phishing, SIM swap | Perderla sin una llave de respaldo ni códigos de recuperación |
| Aplicación de autenticación (authenticator app) | Robo de contraseñas, SIM swap | Un código escrito en un sitio falso; un teléfono perdido sin respaldo |
| Código por correo electrónico | Solo robo de contraseñas | Cae junto con tu cuenta de correo electrónico |
| Código por SMS | Solo robo de contraseñas | SIM swap y códigos robados mediante phishing |

*Tabla 4.1: Métodos de 2FA del más fuerte al más débil*

Usa una llave de seguridad física o una llave de acceso para la **autenticación de dos factores** en tu correo electrónico y en tus cuentas de exchange, con una segunda llave o códigos de recuperación guardados por separado. Si un servicio solo ofrece una aplicación de autenticación, usa esa. Mantén el SMS solo donde no haya otra opción, y nunca como vía de recuperación de tu correo electrónico.

## 4.5 Sesiones robadas: por qué la 2FA no siempre basta

Después de iniciar sesión, tu navegador guarda una cookie de sesión para que no tengas que volver a iniciar sesión. El malware infostealer copia estas cookies (consulta el **capítulo 2**). Con una de ellas, un

atacante puede usar tu cuenta como si fuera tú, sin tu contraseña y sin un código 2FA.

- Cierra sesión en tus cuentas de exchange y de correo electrónico cuando termines, sobre todo en dispositivos compartidos o de uso diario.
- Revisa la lista de sesiones activas y dispositivos en tus cuentas de correo electrónico y de exchange, y cierra las que no reconozcas.
- Si un dispositivo puede estar infectado, cierra todas las sesiones desde un dispositivo limpio y cambia allí las contraseñas, no en el dispositivo infectado.

## 4.6 Ajustes del exchange que evitan que un robo de cuenta acabe en pérdida

- **Lista blanca de retiros:** los fondos solo pueden ir a direcciones que guardaste de antemano, normalmente con un período de espera antes de poder usar una dirección nueva o desactivar la lista blanca. Un atacante que controle tu correo electrónico y tu 2FA aún puede cambiarla, pero el retraso te da tiempo para ver la alerta y congelar la cuenta.
- **Código antiphishing:** una palabra que eliges y que aparece en todos los correos electrónicos auténticos del exchange.
- **Claves API (API keys):** créalas solo para herramientas en las que confíes, nunca con permisos de retiro y limitadas a tu dirección IP cuando sea posible; elimina las claves que ya no uses.
- **Alertas:** activa alertas por correo electrónico o en la app para inicios de sesión, retiros y cambios de seguridad.
- **Mantén en el exchange solo lo que usas para operar.** Tus ahorros deben estar en tu propia billetera Bóveda.

## 4.7 Cuentas de mensajería: robos que llegan a tus contactos

Una cuenta robada de Telegram, WhatsApp, Discord o redes sociales se usa para escribir a tus contactos y pedirles cripto, compartir un enlace malicioso o un “juego para probar”. Los atacantes entran con un código de inicio de sesión robado, una sesión secuestrada o el buzón de voz de

tu número, donde algunos servicios dejan un código de inicio de sesión cuando no contestas.

- Activa la contraseña o el PIN adicional que ofrecen estas apps (verificación en dos pasos).
- Configura un PIN del buzón de voz o desactiva el buzón de voz si no lo usas; pregunta a tu operador móvil cómo hacerlo.
- Nunca reenvíes un código de inicio de sesión a nadie, ni siquiera a un amigo que te lo pida.
- Revisa las sesiones activas y los dispositivos vinculados en cada app.
- Si un amigo te pide cripto o te envía un archivo, confírmalo antes con esa persona por otro canal.

## 4.8 Escenario ilustrativo: el SIM swap nocturno

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

Un sábado por la noche, el teléfono de Ana muestra “Sin servicio”. Ella supone que es un problema de la red y se va a dormir. Mientras duerme, alguien restablece la contraseña de su correo electrónico con un código por SMS, inicia sesión en su cuenta del exchange mediante “¿Olvidaste tu contraseña?” y retira su saldo.

### Qué pasó

Su número se había trasladado a una nueva tarjeta SIM. Su correo electrónico usaba el SMS como método de recuperación, y su exchange dependía de ese correo y de códigos por SMS. Un solo número de teléfono robado desbloqueó todas las cuentas de la cadena.

### Conclusiones clave

- Nunca dejes que un número de teléfono sea lo único que separa a un atacante de tu correo electrónico.
- Las llaves de seguridad físicas y las llaves de acceso no se pueden redirigir a una nueva tarjeta SIM.
- Una lista blanca de retiros, con las alertas activadas, habría retrasado el retiro y le habría dado a Ana tiempo para reaccionar.

## 4.9 Reglas CSF de este capítulo

REGLA PRINCIPAL · TSR-004

### Usa autenticación de dos factores basada en hardware.

Una llave de seguridad física no se puede redirigir a una nueva tarjeta SIM ni introducir en un sitio falso.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| TSR-005 | Activa las listas blancas de retiros en los exchanges | Las nuevas direcciones de retiro quedan en espera, lo que te da tiempo para actuar antes de que salgan los fondos. |
| OR-006 | Mantén el acceso a tus sistemas de autenticación | Las llaves de respaldo y los códigos de recuperación evitan que te quedes sin acceso. |
| SDR-009 | Verifica todos los enlaces antes de iniciar sesión | Las páginas de inicio de sesión copiadas son la forma más común de robar contraseñas y códigos. |
| GR-007 | Nunca guardes tu frase semilla en la nube, en el correo ni en capturas de pantalla | Si te roban la cuenta de correo electrónico o de almacenamiento en la nube, tu frase semilla no debe estar en ella. |
| TSR-006 | Separa dispositivos y cuentas para el uso de cripto | Un correo electrónico aparte para cripto limita lo que deja expuesto una sola filtración o un robo de cuenta. |

*Tabla 4.2: Reglas CSF para el robo de cuentas*

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

## 4.10 Si esto te acaba de pasar

Para ver la lista completa de la primera hora, consulta el **capítulo 9**. Los pasos específicos para el robo de cuentas:

| Si… | Haz esto ahora |
|---|---|
| de repente no tienes servicio móvil | Llama a tu operador móvil desde otro teléfono y pregunta si se cambió tu tarjeta SIM. Desde otro dispositivo, protege primero tu correo electrónico y después tus exchanges. |
| perdiste el acceso a tu correo electrónico | Usa de inmediato el proceso oficial de recuperación de la cuenta del proveedor. Al mismo tiempo, ponte en contacto con tus exchanges a través de sus sitios web oficiales para congelar los retiros. |
| ves inicios de sesión, retiros o claves API nuevas que no hiciste tú | Desde un dispositivo limpio: cierra todas las sesiones, cambia la contraseña, elimina las claves API desconocidas, revisa la lista blanca de retiros y ponte en contacto con el soporte oficial del exchange. |
| te robaron una cuenta de mensajería | Recupérala a través de la app, cierra las demás sesiones, activa la verificación en dos pasos y avisa a tus contactos por otro canal. |

*Tabla 4.3: Primeros pasos después de un robo de cuenta*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para rastrear o recuperar las cripto robadas. Nadie puede revertir una transferencia confirmada a cambio de una comisión. Consulta **Estafas de recuperación** y denuncia el robo: **Cómo denunciar una estafa cripto**.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

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

**cryptosafetyfirst.com/sim-swap-scams-crypto-web3/**

CAPÍTULO 5

# Ataques de red y wifi público

*“El wifi del hotel me pidió primero los datos de acceso de mi correo.”*

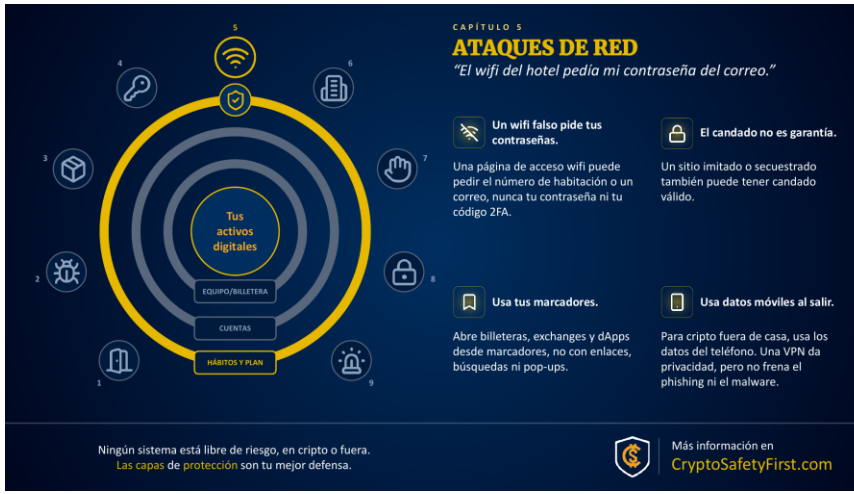


*Figura 5.1: Ataques de red y wifi público de un vistazo*

Los ataques de red reciben mucha atención, pero causan muchas menos pérdidas que el malware o el robo de cuentas. La mayoría de los sitios web y las apps de billetera ya cifran su tráfico, así que limitarse a espiar una red revela poco. Los riesgos reales hoy son las redes y las páginas que te engañan para que escribas algo —una contraseña, un código o una frase semilla (frase de recuperación)— o que te envían a un sitio falso.

Este capítulo es breve a propósito. Explica lo que sigue importando en las redes que no controlas y los pocos hábitos que hacen que lo demás deje de importar.

EN ESTE CAPÍTULO


- 5.1 Los riesgos reales hoy
- 5.2 Lo que sigue importando
- 5.3 Escenario ilustrativo: el inicio de sesión en el aeropuerto
- 5.4 Reglas CSF de este capítulo
- 5.5 Si esto te acaba de pasar


## 5.1 Los riesgos reales hoy

- **Puntos de acceso wifi falsos:** una red con un nombre conocido, creada por un atacante, cuya “página de inicio de sesión” te pide la contraseña de tu correo electrónico o los datos de acceso de otra cuenta.
- **Avisos falsos de actualización o de inicio de sesión** que aparecen mientras estás conectado y te piden instalar algo o volver a iniciar sesión.
- **Sitios web redirigidos:** un atacante que controla la red te envía a una dirección que imita a la real o, si se ha tomado el control del dominio de un proyecto, a un sitio falso en la dirección real. En ambos casos puede aparecer un candado válido.
- **Shoulder surfing (mirar tu pantalla por encima del hombro):** alguien observa tu pantalla o tu teclado en una cafetería, un tren o un espacio de coworking.

**El candado de la barra de direcciones significa que la conexión está cifrada, no que el sitio sea auténtico.** Un sitio falso también puede tenerlo.

## 5.2 Lo que sigue importando

- **Abre billeteras, exchanges (plataformas de intercambio) y DApps desde tus propios marcadores,** no desde enlaces, resultados de búsqueda ni ventanas emergentes.
- **Nunca introduzcas una contraseña, un código 2FA ni tu frase semilla en una página de inicio de sesión de una red wifi.** Un punto de acceso auténtico puede pedirte una dirección de correo electrónico, un número de habitación o un código de acceso, pero nunca la contraseña de tu correo, un código 2FA ni tu frase semilla.

- **Usa preferiblemente los datos móviles o el punto de acceso de tu teléfono** para operar con cripto cuando estés fuera de casa.
- **Mantén actualizados el navegador y el sistema,** y activa el DNS seguro en los ajustes del navegador si aún no está activado.
- **Comprueba las transacciones en la pantalla de tu billetera de hardware (hardware wallet),** para que una página manipulada no pueda cambiar lo que apruebas.
- **Haz las transferencias grandes en casa,** no en lugares públicos, donde pueden observar tu pantalla y manipular tu conexión.

Una **VPN** añade privacidad en redes en las que no confías: oculta tu tráfico al dueño de la red y traslada esa confianza al proveedor de VPN. No te protege de páginas de phishing, malware ni aplicaciones falsas, y no es motivo para relajar los hábitos anteriores.

## 5.3 Escenario ilustrativo: el inicio de sesión en el aeropuerto

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

Mientras espera un vuelo retrasado, Omar se conecta a una red abierta que lleva el nombre del aeropuerto. La página de inicio de sesión le pide “iniciar sesión con tu cuenta de correo electrónico” para tener acceso gratuito. Lo hace y luego consulta su saldo en el exchange. Esa misma noche, le cambian la contraseña del correo.

### Qué pasó

La red era un punto de acceso wifi falso. Su página de inicio de sesión recopiló la contraseña de su correo, y su correo no tenía 2FA basada en hardware. No se interceptó nada; la escribió él mismo.

### Conclusiones clave

- Una página de inicio de sesión de wifi nunca necesita la contraseña de tu correo ni la de tu exchange.
- Usa datos móviles para todo lo relacionado con cripto cuando viajes.
- La 2FA basada en hardware habría dejado inútil la contraseña robada.

## 5.4 Reglas CSF de este capítulo

**REGLA PRINCIPAL · TSR-003**

### Evita el wifi público para operar con cripto.

Usa datos móviles o una red que controles para iniciar sesión y hacer transferencias.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| TSR-002 | Da por hecho que tu dispositivo puede estar comprometido | Verifica en la pantalla de la billetera de hardware lo que una página puede haber cambiado. |
| SDR-009 | Verifica todos los enlaces antes de iniciar sesión | Los marcadores te protegen de redirecciones y de páginas de inicio de sesión falsas. |
| TSR-004 | Usa autenticación de dos factores basada en hardware | Una contraseña robada en una red no sirve de nada sin la llave de seguridad física. |

*Tabla 5.1: Reglas CSF para los riesgos de red*

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

## 5.5 Si esto te acaba de pasar

Para ver la lista completa de la primera hora, consulta el **capítulo 9**.

| Si… | Haz esto ahora |
|---|---|
| introdujiste una contraseña o un código en una página de inicio de sesión de wifi o en una página a la que llegaste a través de una red pública | Desde una conexión de confianza: cambia esa contraseña, cierra las sesiones activas y revisa los ajustes de 2FA. Empieza por tu correo electrónico. |
| instalaste algo que te pidió una página de la red | Trata el dispositivo como infectado: consulta el **capítulo 2**. |
| escribiste tu frase semilla en cualquier sitio en línea | Considera la frase semilla comprometida: crea una billetera nueva en un dispositivo limpio y mueve todos los fondos ahora. |

*Tabla 5.2: Primeros pasos tras una exposición relacionada con la red*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para rastrear o recuperar las cripto robadas. Nadie puede revertir una transferencia confirmada a cambio de una comisión. Consulta **Estafas de recuperación** y denuncia el robo: **Cómo denunciar una estafa cripto**.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

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

**cryptosafetyfirst.com/network-based-attacks/**

CAPÍTULO 6

# Brechas en plataformas y ataques internos

*“Hackearon el exchange. ¿Por qué me están llamando?”*

*Figura 6.1: Brechas en plataformas y ataques internos de un vistazo*

A veces el punto débil no eres tú, sino una empresa en la que confías: un exchange (plataforma de intercambio), un proveedor de billeteras, una tienda que te vendió un dispositivo o un servicio que guarda tus datos. Cuando una plataforma sufre una brecha, se pueden perder dos cosas: los fondos que guarda por ti y los datos personales que tiene sobre ti. Lo segundo suele usarse en tu contra durante meses.

No puedes evitar una brecha en una empresa ajena. Puedes limitar lo que guarda cada plataforma y reconocer los ataques que llegan después.

EN ESTE CAPÍTULO


- 6.1 Dos tipos de brecha en plataformas
- 6.2 Ataques internos
- 6.3 Cómo limitar tu exposición
- 6.4 Escenario ilustrativo: el aviso de brecha
- 6.5 Reglas CSF de este capítulo
- 6.6 Si esto te acaba de pasar


## 6.1 Dos tipos de brecha en plataformas

| Qué se vulnera | Qué puedes perder | Qué viene después |
|---|---|---|
| Fondos que guarda la plataforma (exchange, billetera custodiada, servicio de préstamos) | Tu saldo en esa plataforma, total o parcialmente | Congelación de retiros, procesos de recuperación largos, ofertas falsas de "compensación" |
| Datos de clientes (nombres, direcciones postales, números de teléfono, saldos, historial de pedidos) | Tu privacidad (tus fondos siguen donde están) | Phishing dirigido, llamadas de soporte falsas, envíos falsos de dispositivos, amenazas y ataques físicos dirigidos |

*Tabla 6.1: Brechas de fondos y brechas de datos*

Los casos reales muestran ambos tipos. En febrero de 2025, un ataque a un gran exchange se llevó una de las mayores cantidades jamás robadas a un exchange, después de que los atacantes comprometieran la interfaz del servicio de billeteras que usaba; el exchange cubrió los saldos de los clientes. En mayo de 2025, otro gran exchange reveló que contratistas de soporte sobornados se habían llevado datos de clientes, que luego se usaron para suplantar al exchange y convencer a los clientes de que enviaran fondos.

## 6.2 Ataques internos

Las personas con acceso interno son las que tienen un acceso legítimo: el personal y los contratistas de la plataforma, pero también personas de tu entorno, como un técnico, un familiar o alguien con quien compartes vivienda que sabe dónde está tu copia de seguridad. Los casos internos son raros, y la mayoría de las personas de tu entorno son de confianza.

No se trata de sospechar, sino de diseñar: organízalo todo para que ninguna persona por sí sola pueda llevárselo todo.

- En las plataformas: da por hecho que el personal de soporte puede ver tus datos. El soporte real nunca te pide tu frase semilla (frase de recuperación), tu contraseña ni una transferencia “para proteger tus fondos”.
- En casa: guarda las copias de seguridad de tu frase semilla donde solo puedan acceder las personas de tu plan de recuperación, y no dejes una billetera de hardware (hardware wallet) con su copia de seguridad al lado.
- Para cantidades mayores: usa multisig (multifirma), para que una sola persona con una sola clave no pueda mover los fondos (**capítulo 8**).

## 6.3 Cómo limitar tu exposición

- **Guarda en cualquier plataforma solo lo que uses para operar.** Tus ahorros deben estar en tu propia billetera Bóveda (**The Three-Wallet Model** [Modelo de Tres Billeteras]).
- **Reparte el riesgo:** no lo guardes todo en un solo exchange ni en un solo servicio.
- **Da a las plataformas los menos datos posibles,** y usa tu dirección de correo electrónico separada para cripto (**capítulo 4**).
- **Es probable que recibas ataques posteriores tras cualquier aviso de brecha:** llamadas, correos, cartas y paquetes “de” la plataforma. Ponte en contacto con ella solo a través de su app o su sitio web oficial.
- **Tras una filtración de datos que incluya tu dirección postal,** revisa la seguridad y la privacidad de tu hogar (**capítulo 7**).

## 6.4 Escenario ilustrativo: el aviso de brecha

**Este es un escenario ilustrativo, no un caso concreto denunciado.**
Una semana después de que un exchange informe de una filtración de datos, Priya recibe una llamada de su “equipo antifraude”. Quien llama conoce su nombre, su dirección postal y su saldo, y le dice que su cuenta está en riesgo y que, para proteger sus fondos, debe moverlos a una “billetera segura” que el equipo le configurará.

### Qué pasó

Quien llamaba era un estafador que usaba los datos filtrados. La brecha no había afectado a los fondos de Priya; la llamada era el ataque.

### Conclusiones clave

- Los datos filtrados hacen que las llamadas falsas resulten convincentes. Que conozcan tus datos no demuestra nada.
- Ningún exchange real te pide mover fondos a una billetera que te proporciona él.
- Cuelga y ponte en contacto con la plataforma a través de su app oficial.

## 6.5 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.**

Lo que no está en una plataforma no se puede perder en una brecha de esa plataforma.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| GR-005 | Nunca sigas instrucciones urgentes de soporte o seguridad. Sal del canal y vuelve a entrar por la app o la URL oficial | Las llamadas de soporte falsas llegan después de casi todas las filtraciones de datos. |
| TSR-005 | Activa las listas blancas de retiros en los exchanges | Limita lo que un atacante puede hacer con una cuenta robada. |
| SDR-010 | Nunca pagues a nadie para recuperar criptomonedas perdidas | Las víctimas de brechas son objetivo de servicios falsos de recuperación y compensación. |

*Tabla 6.2: Reglas CSF para brechas en plataformas*

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

## 6.6 Si esto te acaba de pasar

Para ver la lista completa de la primera hora, consulta el **capítulo 9**.

| Si… | Haz esto ahora |
|---|---|
| una plataforma que usas informa de un hackeo de fondos | Sigue solo sus anuncios oficiales. No envíes fondos a ninguna dirección de “recuperación” o “compensación”. Guarda registros de tu saldo y de la correspondencia. |
| una plataforma informa de una filtración de tus datos | Cambia la contraseña de esa plataforma, revisa la 2FA y ten en cuenta que es probable que intenten contactarte con mensajes dirigidos a ti. Si se filtró tu dirección postal, consulta el **capítulo 7**. |
| alguien llama, escribe o envía un paquete “de” la plataforma tras una brecha | No hagas lo que te pide. Ponte tú mismo en contacto con la plataforma a través de su app o su sitio web oficial. |

*Tabla 6.3: Primeros pasos tras una brecha en una plataforma*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para rastrear, recuperar o “compensar” las cripto perdidas. Nadie puede revertir una transferencia confirmada a cambio de una comisión. Consulta **Estafas de recuperación** y denuncia: **Cómo denunciar una estafa cripto**.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

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

**cryptosafetyfirst.com/crypto-exchange-hacked-what-to-do/**

CAPÍTULO 7

# Coacción física (ataques de llave inglesa)

*“Encontraron mi dirección postal en una captura de pantalla antigua.”*

*Figura 7.1: Coacción física (ataques de llave inglesa) de un vistazo*

Un “ataque de llave inglesa” (wrench attack) es el ataque más antiguo que existe: en lugar de entrar en un dispositivo, los delincuentes obligan a una persona a desbloquearlo. Se han denunciado robos, asaltos a viviendas y secuestros dirigidos a poseedores de cripto y a sus familias en varios países, incluida una serie de casos en Francia en 2025. Siguen siendo raros, pero como las cripto se pueden mover en minutos y no se pueden revertir, quienes las poseen son objetivos atractivos.

Este capítulo no trata de enfrentarte a los atacantes. Tu seguridad y la de tu familia son lo primero, siempre. Trata de no convertirte en objetivo y de organizar tus cripto para que, incluso bajo presión, haya poco que llevarse en el momento.

EN ESTE CAPÍTULO


- 7.1 Cómo se convierte alguien en objetivo
- 7.2 Privacidad: la mejor protección
- 7.3 Organiza tus cripto para que haya poco que llevarse
- 7.4 Si ocurre
- 7.5 Reglas CSF de este capítulo
- 7.6 Si esto te acaba de pasar


## 7.1 Cómo se convierte alguien en objetivo

- **Hablar de tus fondos en público:** publicaciones, capturas de pantalla de saldos o ganancias, charlas en encuentros cripto o un cargo conocido en una empresa cripto.
- **Datos de clientes filtrados:** las brechas en exchanges (plataformas de intercambio), tiendas de billeteras de hardware (hardware wallets) y otros servicios han expuesto nombres, números de teléfono y direcciones de domicilio (**capítulo 6**).
- **Señales visibles en casa:** cajas de billeteras de hardware en el contenedor de reciclaje, etiquetas de envío o una billetera visible en una videollamada.
- **Reunirse en persona con desconocidos** para intercambiar cripto o hardware.
- **Personas que lo saben:** amigos, familiares o contactos que saben que tienes cripto y pueden contárselo a otros, a menudo sin mala intención.

## 7.2 Privacidad: la mejor protección

- **No compartas saldos, ganancias ni capturas de pantalla,** ni en internet ni fuera de internet. “Tengo un poco, como todo el mundo” es suficiente.
- **Mantén tu dirección de domicilio fuera de las cuentas y los envíos relacionados con cripto siempre que puedas:** por ejemplo, un apartado postal o la dirección del trabajo para los pedidos de billeteras de hardware.

- **Separa tu identidad pública de tus fondos:** un seudónimo para las redes sociales de cripto y ninguna dirección de billetera vinculada a tu nombre real.
- **Elimina publicaciones y perfiles antiguos** que te vinculen con cripto, y pide a los sitios de venta de datos personales (data brokers) que borren tu ficha cuando la ley de tu país lo permita.
- **Habla con tu familia** para que no mencionen las cripto a otras personas y sepan qué hacer si alguien pregunta.

## 7.3 Organiza tus cripto para que haya poco que llevarse

El objetivo es que nada de lo que puedan obligarte a hacer en el momento mueva tus ahorros.

- **Guarda solo cantidades pequeñas en billeteras que puedas abrir con un teléfono o con un solo dispositivo,** y nada grande en una app de exchange que puedas desbloquear con la cara o la huella dactilar.
- **Protege tus ahorros con más de una clave:** con multisig (multifirma), las claves se guardan en lugares distintos, así que los fondos no se pueden mover desde un solo lugar ni por una sola persona (**capítulo 8** y **The Three-Wallet Model [Modelo de Tres Billeteras]**).
- **Añade retraso:** algunas configuraciones y servicios permiten bloqueos temporales (time-locks) o retrasos en los retiros, para que una transferencia grande no pueda hacerse de inmediato.
- **Una billetera señuelo:** la passphrase (frase de contraseña adicional) de una billetera de hardware puede abrir una segunda billetera independiente. Tener un saldo pequeño en la billetera principal y los ahorros detrás de una passphrase es una opción que usan algunos poseedores para tener menos en riesgo. Un señuelo es una forma de tener menos en riesgo, nunca algo que defender.

## 7.4 Si ocurre

**Obedece.** Tu vida y tu familia valen más que cualquier cantidad de cripto. No te resistas, no negocies, no intentes engañar a los atacantes. Si te preguntan por una billetera oculta o una passphrase, entrégala. Si

tu configuración hace que no puedas mover fondos en el momento, dilo con calma y con sinceridad.

- Cuando estés a salvo, llama a la policía y diles que había cripto de por medio.
- Anota la hora, lo que se llevaron y cualquier dato de las transacciones que puedas ver después en un explorador de bloques.
- Mueve los fondos que te queden a billeteras nuevas con frases semilla (frases de recuperación) nuevas, porque los atacantes pueden haber visto tus copias de seguridad o tus dispositivos.
- Es probable que vuelvan a contactarte, incluso con ofertas de recuperación falsas. Sigue los pasos para denunciar del **capítulo 9**.

## 7.5 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.

Los ahorros en una billetera Bóveda lejos de tu teléfono, idealmente protegidos con más de una clave o con un retraso, son mucho más difíciles de llevarse en el momento.

| 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 | Mantiene los ahorros fuera del teléfono que llevas en el bolsillo. |
| OR-007 | Planifica la recuperación de tu billetera para emergencias y herencia | Tu familia necesita un plan que no dependa de que tú tengas libertad para actuar. |
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | A menudo se investiga a los objetivos mediante contactos que parecen inofensivos. |

*Tabla 7.1: Reglas CSF para la seguridad física*

Todavía no hay una regla CSF específica para la coacción física; es una candidata para la próxima versión de las reglas. Las 32 reglas: **Reglas de seguridad cripto de CSF**.

## 7.6 Si esto te acaba de pasar

Ponte a salvo y llama primero a la policía. Después sigue los pasos de "Si ocurre" más arriba y la lista de la primera hora del **capítulo 9**, desde un dispositivo que los atacantes no hayan tenido.

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para rastrear o recuperar las cripto robadas. Nadie puede revertir una transferencia confirmada a cambio de una comisión. Consulta **Estafas de recuperación** y denuncia: **Cómo denunciar una estafa cripto**.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

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

**cryptosafetyfirst.com/crypto-wrench-attacks/**

CAPÍTULO 8

# Protección avanzada

*“Que falle un solo dispositivo nunca debería ser suficiente.”*

*Figura 8.1: Protección avanzada de un vistazo*

Los hábitos de los capítulos 2 a 7 protegen bien a la mayoría de las personas. Este capítulo es para fondos más grandes, o para quien quiera que sus ahorros sobrevivan incluso a un dispositivo comprometido, una billetera manipulada o una copia de seguridad robada. Cada opción de este capítulo añade pasos, y cada paso extra es algo que tú, y cualquiera que herede tus cripto, deben entender. Elige lo que de verdad vayas a mantener.

EN ESTE CAPÍTULO


- 8.1 Un dispositivo dedicado a cripto
- 8.2 Multisig: más de una clave
- 8.3 Otras opciones comparadas
- 8.4 Hábitos de firma que importan en cualquier nivel
- 8.5 Reglas CSF de este capítulo

## 8.1 Un dispositivo dedicado a cripto

El paso avanzado más sencillo es un equipo o un teléfono que se use solo para cripto: sin correo electrónico, sin juegos, sin navegar, sin código de prueba, solo las apps oficiales de tus billeteras y exchanges (plataformas de intercambio). El malware suele llegar a través del uso diario, así que un dispositivo sin uso diario está mucho menos expuesto.

Un sistema Linux en modo live iniciado desde una memoria USB (descargado del sitio oficial y comprobado con su firma publicada) es una alternativa más barata para un uso ocasional. Ayuda contra el malware de tu sistema habitual. No ayuda contra hardware o firmware comprometidos, y no hace que sea seguro escribir una frase semilla (frase de recuperación): **nunca escribas una frase semilla en ningún equipo, ni siquiera en uno limpio.**

## 8.2 Multisig: más de una clave

Una billetera **multisig (multifirma)** necesita varias claves para mover fondos, por ejemplo 2 de 3. Cada clave está en su propia billetera de hardware (hardware wallet), idealmente de fabricantes distintos, y se guarda en un lugar distinto.

- **De qué te protege:** de un dispositivo comprometido o manipulado, de una copia de seguridad robada o de una persona obligada o tentada a actuar sola.
- **Por qué 2 de 3 y no 2 de 2:** con 2 de 2, si pierdes una clave, los fondos quedan bloqueados para siempre. Con 2 de 3, puedes perder una clave y aun así recuperarlos.
- **Lo que cuesta:** cada clave necesita su propia copia de seguridad, y también debes hacer una copia de seguridad de la configuración de la billetera (a menudo llamada descriptor), que registra cómo funcionan las claves en conjunto. Sin ella, dos frases semilla por sí solas no suelen bastar para recuperar los fondos. Guarda una copia de la configuración con cada copia de seguridad de clave: no permite mover fondos, pero revela tus saldos, así que guárdala en privado. El riesgo pasa de los hackers a tu propia forma de llevar los registros.

Para ver cómo encaja el multisig en tu billetera Bóveda, consulta **The Three-Wallet Model (Modelo de Tres Billeteras)**. Para las copias

de seguridad, consulta el **capítulo 2 de la Guía de prevención de errores de usuario**.

## 8.3 Otras opciones comparadas

| Opción | Lo que aporta | Inconveniente |
|---|---|---|
| **Passphrase (frase de contraseña adicional)** en una billetera de hardware | Un segundo secreto: la frase semilla por sí sola no abre la billetera de la passphrase | Si la olvidas, pierdes los fondos; hay que hacer una copia de seguridad aparte |
| Dispositivo de firma aislado (air-gapped) | Nunca se conecta a un equipo; las transacciones se transfieren mediante código QR o tarjeta de memoria | Más lento de usar; sigue necesitando una fuente de confianza y una configuración cuidadosa |
| Multisig con varios fabricantes | Ningún dispositivo, lugar o persona puede mover fondos por sí solo | Más copias de seguridad, más pasos, herencia más difícil |
| **Billetera MPC** | Los fragmentos de clave se guardan en varios lugares, a menudo también en un proveedor; no existe una clave completa | Dependes de la seguridad del proveedor y de que siga prestando el servicio cuando guarda un fragmento |
| Billetera de contrato inteligente | Límites de gasto, retrasos y contactos de recuperación | Depende del código del contrato; la configuración y la recuperación varían según la red |

*Tabla 8.1: Opciones avanzadas y sus inconvenientes*

## 8.4 Hábitos de firma que importan en cualquier nivel

- **Verifica en la pantalla del dispositivo:** la dirección completa y el importe, no solo los primeros y últimos caracteres.
- **Evita la firma a ciegas (blind signing)** en todo lo que afecte a tus ahorros: si el dispositivo no puede mostrar lo que apruebas, no lo apruebes.

- **Revoca las aprobaciones que ya no necesites** en las billeteras que todavía tienen fondos.
- **Prueba la recuperación** de cualquier configuración avanzada antes de confiar en ella, y otra vez después de cualquier cambio.

## 8.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · TSR-006

### Separa dispositivos y cuentas para el uso de cripto.

Un solo dispositivo infectado o una sola cuenta vulnerada nunca deberían exponer todas tus cripto a la vez.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| TSR-004 | Usa autenticación de dos factores basada en hardware | Protege las cuentas que rodean tu configuración avanzada. |
| TSR-005 | Activa las listas blancas de retiros en los exchanges | Las nuevas direcciones de retiro quedan en espera, lo que te da tiempo para actuar. |
| GR-003 | Usa siempre una billetera de hardware para guardar cripto a largo plazo o de alto valor | La base de toda configuración avanzada. |
| GR-004 | Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos | Las aprobaciones antiguas eluden cualquier refuerzo de la billetera. |
| OR-001 | Prueba la recuperación de tu billetera antes de confiar en ella | Una configuración compleja que no puedes restaurar no protege a nadie. |
| OR-003 | Documenta cómo se creó tu billetera | El multisig y las passphrases no sirven de nada sin un registro claro. |

*Tabla 8.2: Reglas CSF de protección avanzada*

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

CONTINÚA EN CRYPTOSAFETYFIRST.COM

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

cryptosafetyfirst.com/advanced-security-practices-cryptocurrency/

CAPÍTULO 9

# Si te han hackeado

*“Me quedé mirando el explorador en vez de actuar.”*

*Figura 9.1: Si te han hackeado de un vistazo*

Encontrar una billetera o una cuenta vaciada es un golpe, y la primera reacción es averiguar cómo ocurrió. Eso puede esperar. En la primera hora, lo que importa es detener más pérdidas: todo lo que un atacante pudo alcanzar una vez, normalmente puede volver a alcanzarlo.

Este capítulo ofrece la lista de la primera hora, una forma de encontrar la causa probable y qué hacer en los días siguientes, incluido cómo evitar las estafas de recuperación que siguen a casi toda pérdida.

EN ESTE CAPÍTULO


- 9.1 La primera hora
- 9.2 Encuentra la causa probable
- 9.3 Denúncialo
- 9.4 Reconstruye de forma segura
- 9.5 Reglas CSF de este capítulo

## 9.1 La primera hora

Sigue los pasos que correspondan, en este orden, desde un dispositivo de confianza; idealmente, uno que nunca se haya usado con la billetera o las cuentas afectadas. Si una cuenta de un exchange (plataforma de intercambio) se está vaciando en este momento, ponte en contacto con su soporte oficial para congelarla al mismo tiempo que haces el paso 1.

**1. Mueve lo que queda.** Crea una billetera nueva con una frase semilla (frase de recuperación) nueva, en una billetera de hardware (hardware wallet) nueva o, de forma temporal, en un dispositivo limpio, y mueve los fondos restantes de todas las billeteras que compartan la frase semilla o el dispositivo afectados. Incluye los tokens y NFT que todavía se puedan mover. Si la frase semilla o la clave privada están comprometidas, no envíes más monedas a la billetera para pagar comisiones: los bots barredores automáticos (sweeper bots) suelen llevárselas en segundos. Mueve solo lo que permita el saldo que ya hay, y da el resto por perdido, salvo que el soporte oficial de la billetera o del token describa un método seguro.

**2. Protege tu correo electrónico.** Cambia su contraseña, cierra todas las sesiones, elimina las reglas de reenvío y las opciones de recuperación que no reconozcas, y activa una llave de seguridad física (hardware security key) o una llave de acceso (passkey).

**3. Bloquea tus exchanges.** Cierra las sesiones, cambia las contraseñas, elimina las claves API (API keys) que no reconozcas, revisa las listas blancas de retiros y ponte en contacto con el soporte oficial para congelar los retiros si es necesario.

**4. Llama a tu operador móvil** si perdiste el servicio móvil o recibiste mensajes inesperados sobre tu tarjeta SIM o tu número.

**5. Revoca las aprobaciones de tokens** en las billeteras cuyas claves no estén comprometidas y que todavía tengan fondos, con una herramienta de confianza para revisar aprobaciones (consulta **Herramientas de seguridad**) abierta desde tus marcadores.

**6. Deja de usar el dispositivo afectado para cripto** hasta que lo hayas borrado por completo y reinstalado. Hazlo solo después de poner los fondos a salvo.

No envíes fondos a la dirección del atacante, no le respondas y no pagues a nadie que se ofrezca a recuperar los fondos.

## 9.2 Encuentra la causa probable

Saber cómo ocurrió te dice qué más está expuesto. Revisa las transacciones en un explorador de bloques y la actividad de tus cuentas.

| Lo que ves | Causa probable | Qué más está expuesto |
|---|---|---|
| Los fondos salieron de tu billetera sin ninguna firma tuya | Frase semilla o **clave privada** expuesta: malware, una copia digital, un dispositivo manipulado o alguien que la vio | Todas las billeteras creadas con la misma frase semilla; cualquier otro secreto en el mismo dispositivo |
| Los tokens salieron a través de un contrato después de conectarte a un sitio | Una aprobación de tokens o una firma que diste (una estafa; consulta la **guía de estafas**) | Otras aprobaciones en la misma billetera |
| Un retiro del exchange que no hiciste | Robo de cuenta: contraseña, correo electrónico, SIM swap (duplicado fraudulento de la tarjeta SIM) o sesión robada | Tu correo electrónico y todas las cuentas que se restablecen a través de él |
| Una transferencia fue a una dirección que no elegiste | Clipboard swapper (malware que reemplaza lo que copias en el portapapeles) o una aplicación o página manipuladas | El dispositivo que usaste |
| Todo ocurrió justo después de configurar un dispositivo nuevo | Dispositivo manipulado o preconfigurado | Todo lo configurado en ese dispositivo |

*Tabla 9.1: Señales y causas probables*

A veces no se puede encontrar la causa. Considera expuesto todo lo que haya tenido contacto con la billetera (dispositivos, copias de seguridad y cuentas) y reconstruye desde cero.

## 9.3 Denúncialo

- Denuncia el robo ante tu policía local o el servicio nacional de denuncia de ciberdelitos. Enlaces por país: **Cómo denunciar una estafa cripto**.

- Avisa a los exchanges implicados, incluido el exchange que pueda recibir los fondos robados, con los hashes de las transacciones y las horas.
- Si te robaron stablecoins, comunica rápidamente los hashes de las transacciones al emisor de la stablecoin a través de su sitio web oficial; a veces los emisores pueden congelarlas.
- Guarda un registro: hashes de las transacciones, direcciones, capturas de pantalla de los mensajes y de la actividad de las cuentas, fechas y horas.
- Si había implicada una aplicación de billetera, una extensión o un dispositivo, comunícaselo al desarrollador o al fabricante a través de su sitio web oficial.

Las denuncias rara vez devuelven los fondos rápidamente, pero ayudan a los investigadores a relacionar casos, y algunos fondos se congelan cuando llegan a exchanges regulados.

## 9.4 Reconstruye de forma segura

- Borra por completo y reinstala los dispositivos afectados, o reemplázalos.
- Billeteras nuevas con frases semilla nuevas, escritas en papel o metal, con copia en dos lugares.
- Un correo electrónico aparte para cripto, con una llave de seguridad física; sin recuperación por SMS.
- Revisa The Three-Wallet Model (Modelo de Tres Billeteras), para que el próximo problema no pueda llegar a tus ahorros.

## 9.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · TSR-002

### Da por hecho que tu dispositivo puede estar comprometido.

Después de un hackeo, actúa desde un dispositivo limpio y considera expuesto todo secreto del anterior.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-010 | Nunca pagues a nadie para recuperar criptomonedas perdidas | Las ofertas de recuperación no solicitadas son estafas; nadie puede revertir una transferencia confirmada a cambio de una comisión. |
| GR-004 | Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos | Las aprobaciones antiguas pueden seguir vaciando una billetera después de la primera pérdida. |
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | Los falsos ayudantes contactan a las víctimas a las pocas horas de una pérdida. |

*Tabla 9.2: Reglas CSF después de un hackeo*

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

DESPUÉS DE UNA PÉRDIDA

Es probable que recibas ofertas para rastrear o recuperar las cripto robadas, en comentarios, mensajes e incluso cartas falsas de “bufetes de abogados”. Nadie puede revertir una transferencia confirmada 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-wallet-drained-what-to-do/

# 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-003 | Usa siempre una billetera de hardware para guardar cripto a largo plazo o de alto valor | 2, 3, 7, 8 |
| GR-004 | Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos | 8, 9 |
| GR-005 | Nunca sigas instrucciones urgentes de soporte o seguridad. Sal del canal y vuelve a entrar por la app o la URL oficial | 1, 6 |
| GR-007 | Nunca guardes tu frase semilla en la nube, en el correo ni en capturas de pantalla | 2, 4 |
| GR-008 | Guarda tus fondos a largo plazo en una billetera bóveda. Usa otra billetera para DApps, trading y Web3 | 1, 3, 6, 7 |
| OR-001 | Prueba la recuperación de tu billetera antes de confiar en ella | 8 |
| OR-003 | Documenta cómo se creó tu billetera | 8 |
| OR-006 | Mantén el acceso a tus sistemas de autenticación | 4 |
| OR-007 | Planifica la recuperación de tu billetera para emergencias y herencia | 7 |
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | 1, 7, 9 |
| SDR-009 | Verifica todos los enlaces antes de iniciar sesión | 1, 4, 5 |
| SDR-010 | Nunca pagues a nadie para recuperar criptomonedas perdidas | 6, 9 |
| TSR-001 | Nunca instales software cripto de fuentes no oficiales | 2, 3 |

| Regla | Enunciado | Capítulos |
|---|---|---|
| TSR-002 | Da por hecho que tu dispositivo puede estar comprometido | 2, 3, 5, 9 |
| TSR-003 | Evita el wifi público para operar con cripto | 5 |
| TSR-004 | Usa autenticación de dos factores basada en hardware | 4, 5, 8 |
| TSR-005 | Activa las listas blancas de retiros en los exchanges | 4, 6, 8 |
| TSR-006 | Separa dispositivos y cuentas para el uso de cripto | 2, 4, 8 |
| TSR-007 | Tómate tu tiempo antes de hacer clic o instalar | 1, 2 |

*Reglas CSF usadas en este libro*

# Sigue aprendiendo

Los métodos de ataque cambian más rápido que cualquier libro. CryptoSafetyFirst.com mantiene viva esta guía entre ediciones:

- **Una página para cada capítulo**, siempre actualizada.
- Las guías de **estafas** y de **errores de usuario**, para las pérdidas que empiezan con una estafa o un error.
- **The Three-Wallet Model** (Modelo de Tres Billeteras): una guía y un kit de herramientas gratuitos que evitan que una billetera o un dispositivo comprometidos lleguen a tus ahorros.
- **Herramientas de seguridad prácticas**: lo que previene cada una y lo que no puede hacer.

**cryptosafetyfirst.com**