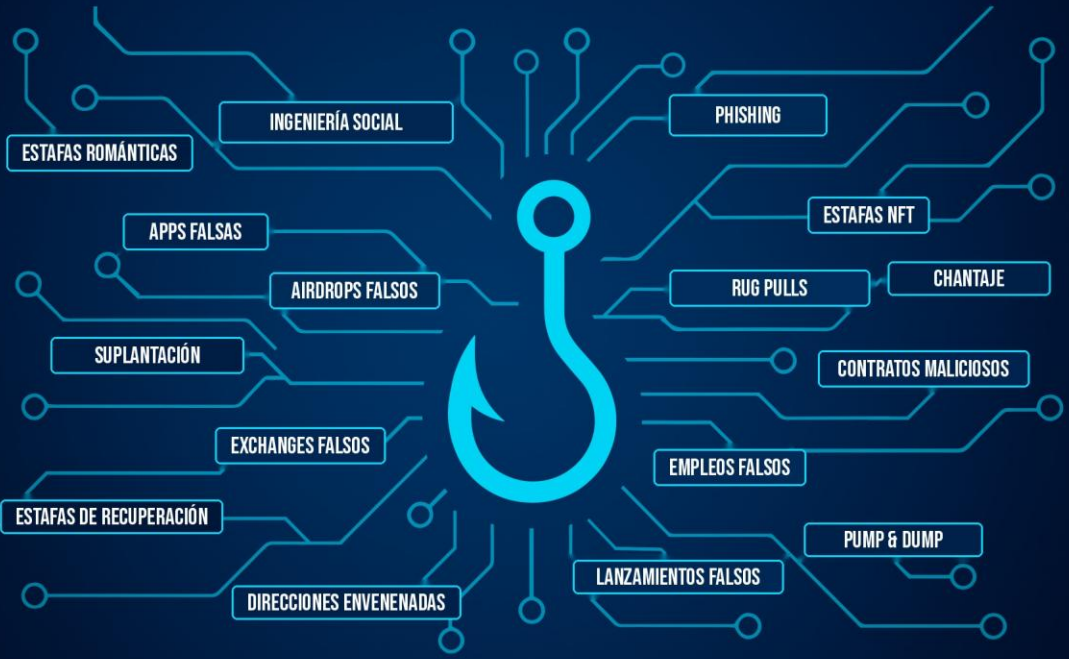
EDICIÓN 2026

# GUÍA DE PREVENCIÓN DE ESTAFAS EN CRIPTO Y WEB3




Detecta y frena las estafas cripto: tu guía para proteger tus activos digitales en ecosistemas descentralizados

JUAN PABLO RENEDO

# Guía de prevención de estafas en cripto y Web3

Detecta y detén las estafas cripto: tu guía para proteger tus activos digitales en ecosistemas descentralizados

**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 ..... 8
Cómo usar este libro ..... 9
Si crees que te han estafado ..... 11
Estafas de ingeniería social ..... 18
1.1 Cómo funcionan las estafas: siete detonantes ..... 19
1.2 El patrón detrás de casi toda estafa ..... 20
1.3 Estafas de ingeniería social que debes conocer ..... 21
1.4 Escenario ilustrativo: la trampa de la “billetera gratis” ..... 24
1.5 Cómo protegerte ..... 25
1.6 Reglas CSF de este capítulo ..... 26
1.7 Si esto te acaba de pasar ..... 26
Estafas de suplantación de identidad ..... 28
2.1 Estafas de suplantación de identidad que debes conocer ..... 29
2.2 Cómo actúan los suplantadores ..... 33
2.3 Escenario ilustrativo: la llamada del “equipo de seguridad” ..... 34
2.4 Cómo protegerte ..... 34
2.5 Reglas CSF de este capítulo ..... 35
2.6 Si esto te acaba de pasar ..... 36
Estafas de phishing ..... 38
3.1 Estafas de phishing que debes conocer ..... 39
3.2 Phishing con billetera conectada: aprobaciones, firmas y drainers ..... 42
3.3 Ejercicio práctico: detecta el correo de phishing ..... 43
3.4 Cómo protegerte ..... 44
3.5 Reglas CSF de este capítulo ..... 44
3.6 Si esto te acaba de pasar ..... 45

Aplicaciones y billeteras falsas ..... 47
4.1 Aplicaciones y billeteras falsas que debes conocer ..... 48
4.2 Por qué una billetera de hardware no arregla una configuración falsa ..... 51
4.3 Escenario ilustrativo: la extensión de asistente de trading ..... 52
4.4 Cómo protegerte ..... 53
4.5 Reglas CSF de este capítulo ..... 53
4.6 Si esto te acaba de pasar ..... 54
Contratos y aprobaciones maliciosos ..... 56
5.1 Aprobaciones y firmas en lenguaje sencillo ..... 57
5.2 Estafas con contratos maliciosos que debes conocer ..... 58
5.3 Escenario ilustrativo: el tutorial del bot MEV ..... 60
5.4 Cómo protegerte ..... 61
5.5 Reglas CSF de este capítulo ..... 61
5.6 Si esto te acaba de pasar ..... 62
Estafas de envenenamiento de direcciones ..... 64
6.1 Cómo funciona el envenenamiento de direcciones ..... 65
6.2 Variantes que debes conocer ..... 65
6.3 Escenario ilustrativo: el depósito en el exchange ..... 66
6.4 Cómo protegerte ..... 67
6.5 Reglas CSF de este capítulo ..... 67
6.6 Si esto te acaba de pasar ..... 68
Estafas de regalos y airdrops ..... 69
7.1 Estafas de regalos y airdrops que debes conocer ..... 70
7.2 Tokens inesperados en tu billetera ..... 73
7.3 Escenario ilustrativo: el token con un sitio web en su nombre ..... 73
7.4 Cómo protegerte ..... 74
7.5 Reglas CSF de este capítulo ..... 74
7.6 Si esto te acaba de pasar ..... 75
Plataformas de inversión falsas ..... 77

8.1 Plataformas de inversión falsas que debes conocer ..... 78
8.2 La trampa del retiro ..... 80
8.3 Señales que no son prueba ..... 81
8.4 Escenario ilustrativo: la cuenta rentable ..... 81
8.5 Cómo protegerte ..... 82
8.6 Reglas CSF de este capítulo ..... 83
8.7 Si esto te acaba de pasar ..... 83
Estafas con tokens ..... 85
9.1 Estafas con tokens que debes conocer ..... 86
9.2 Señales que no son prueba ..... 89
9.3 Escenario ilustrativo: la memecoin de la comunidad ..... 90
9.4 Cómo protegerte ..... 91
9.5 Reglas CSF de este capítulo ..... 91
9.6 Si esto te acaba de pasar ..... 92
Estafas románticas ..... 94
10.1 Estafas románticas que debes conocer ..... 95
10.2 Las etapas de una estafa romántica de inversión ..... 98
10.3 Escenario ilustrativo: el número equivocado ..... 98
10.4 Cómo protegerte ..... 99
10.5 Reglas CSF de este capítulo ..... 100
10.6 Si esto te acaba de pasar ..... 100
Estafas de empleo y tareas ..... 102
11.1 Estafas de empleo y tareas que debes conocer ..... 103
11.2 Cómo te atrapan las estafas de tareas ..... 105
11.3 Escenario ilustrativo: el trabajo de optimización ..... 106
11.4 Cómo protegerte ..... 106
11.5 Reglas CSF de este capítulo ..... 107
11.6 Si esto te acaba de pasar ..... 107
Estafas de chantaje y extorsión ..... 109
12.1 Estafas de chantaje y extorsión que debes conocer ..... 110

12.2 ¿Farol o real? Qué comprobar ..... 112
12.3 Escenario ilustrativo: la contraseña antigua ..... 112
12.4 Cómo protegerte ..... 113
12.5 Reglas CSF de este capítulo ..... 114
12.6 Si esto te acaba de pasar ..... 114
Estafas de recuperación ..... 116
13.1 Estafas de recuperación que debes conocer ..... 117
13.2 Cómo es la ayuda legítima ..... 120
13.3 Escenario ilustrativo: el panel de recuperación ..... 121
13.4 Cómo protegerte ..... 122
13.5 Reglas CSF de este capítulo ..... 122
13.6 Si esto te acaba de pasar ..... 123
Índice de reglas CSF ..... 125
Sigue aprendiendo ..... 127

# Sobre esta edición

La primera edición de esta guía describía dieciséis categorías de estafas. Desde entonces, las estafas han cambiado, y también lo que CryptoSafetyFirst sabe sobre ellas. Cada semana, CSF recopila y clasifica incidentes reales comunicados por usuarios de cripto. La Edición 2026 se ha reconstruido en torno a lo que muestra ese trabajo.

### Qué hay de nuevo

- **Trece capítulos que reflejan cómo ocurren realmente las estafas.** Los capítulos siguen la taxonomía de incidentes de CSF, de modo que el libro, el sitio web y las herramientas de evaluación de CSF usan las mismas categorías.
- **Una sección "Empieza aquí"** para quien crea que puede haber sido estafado. Te dice qué hacer según lo que hiciste realmente: ver, conectar, aprobar, firmar, enviar, exponer tu frase semilla (frase de recuperación) o instalar algo.
- **Nuevos capítulos** sobre suplantación de identidad, envenenamiento de direcciones y estafas de recuperación.
- **Reglas CSF en cada capítulo**, con una regla principal por tipo de estafa y las reglas de apoyo que la respaldan.
- **Consejos corregidos y actualizados**, incluida la diferencia entre desconectar y revocar, lo que las billeteras de hardware (hardware wallets) pueden y no pueden hacer, y por qué algunas señales tranquilizadoras no son prueba.

### Cómo se tratan los ejemplos y los datos

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

# Cómo usar este libro

| Si… | Ve a |
|---|---|
| crees que te acaban de estafar | **Empieza aquí: Si crees que te han estafado**, y luego el capítulo de tu estafa. |
| quieres entender cómo funcionan las estafas | **Capítulo 1**: los siete detonantes y el patrón de cinco pasos detrás de casi todas las estafas. |
| quieres protegerte de una estafa concreta | El capítulo de esa estafa (consulta el mapa de capítulos más abajo). |
| quieres configurar tus billeteras de forma segura | La guía **Three-Wallet Model** (Modelo de Tres Billeteras) (gratis en CryptoSafetyFirst.com). Este libro usa sus términos: billetera Bóveda (Vault), billetera de Uso Frecuente (Frequent Use wallet) y billetera Desechable (Disposable wallet). |

*Por dónde empezar*

### Cómo funciona cada capítulo

Todos los capítulos siguen la misma estructura, para que encuentres rápido lo que necesitas: una infografía de un vistazo, las estafas que debes conocer con sus señales de alerta y cómo evitarlas, un escenario ilustrativo, cómo protegerte, las reglas CSF para esa estafa y **Si esto te acaba de pasar**, con las primeras acciones de ese capítulo. Cada capítulo termina con un enlace a su página en CryptoSafetyFirst.com.

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

| Cap. | Capítulo | Suele combinarse con | Regla CSF principal |
|---|---|---|---|
| 1 | Estafas de ingeniería social | Todos los capítulos (cómo funcionan las estafas) | SDR-001 |

| Cap. | Capítulo | Suele combinarse con | Regla CSF principal |
|---|---|---|---|
| 2 | Estafas de suplantación de identidad | 3, 4, 12, 13 | SDR-004 |
| 3 | Estafas de phishing | 2, 5, 7 | SDR-009 |
| 4 | Aplicaciones y billeteras falsas | 3, 11; guía Hackers (malware) | TSR-001 |
| 5 | Contratos y aprobaciones maliciosos | 3, 7, 9 | GR-004 |
| 6 | Estafas de envenenamiento de direcciones | guía User Mistakes (dirección equivocada) | OR-005 |
| 7 | Estafas de regalos y airdrops | 2, 3, 5 | SDR-005 |
| 8 | Plataformas de inversión falsas | 9, 10, 11, 13 | SDR-003 |
| 9 | Estafas con tokens | 5, 7, 8 | SDR-007 |
| 10 | Estafas románticas | 8, 12, 13 | SDR-006 |
| 11 | Estafas de empleo y tareas | 4, 8, 13 | SDR-002 |
| 12 | Estafas de chantaje y extorsión | 2, 10; guía Hackers (amenazas físicas) | GR-005 |
| 13 | Estafas de recuperación | 2, 8, 10, 11 | SDR-010 |

*Mapa de capítulos: cómo se conectan las estafas*

Las estafas rara vez vienen solas. Un contacto romántico lleva a una plataforma de inversión falsa; una pérdida lleva a una estafa de recuperación; un empleo falso lleva a malware. El mapa de capítulos muestra las combinaciones más comunes, para que puedas leer los capítulos que van juntos.

EMPIEZA AQUÍ

# Si crees que te han estafado

Lo que debes hacer a continuación depende de **lo que realmente pasó**. Visitar un sitio web sospechoso no es lo mismo que conectar una billetera. Conectar una billetera no es lo mismo que aprobar un token, firmar una autorización, enviar una transacción, exponer tu frase semilla (frase de recuperación) o instalar malware.

Busca la fila que corresponde a lo que hiciste. Cada fila indica qué hacer ahora y qué no puede solucionar esa acción.

| Qué pasó | Qué hacer ahora | Qué no soluciona esto |
|---|---|---|
| Solo viste un sitio web, un mensaje o un anuncio sospechosos, o un token inesperado | Ciérralo. No hagas clic en enlaces, no descargues archivos, no conectes una billetera, no firmes ni respondas. Denuncia el mensaje o la cuenta ante la plataforma. Puedes ocultar un token inesperado, pero no intentes venderlo, hacer un swap (intercambio de tokens) con él ni reclamarlo. | Solo verlo no compromete tu billetera. Si hiciste alguna de las cosas de abajo, sigue también esa fila. |
| Conectaste tu billetera, pero no aprobaste, firmaste ni enviaste nada | Desconecta el sitio en la configuración de sitios conectados de tu billetera. Revisa con cuidado si también aprobaste, firmaste o enviaste algo; si es así, sigue esas filas. | Desconectar termina la sesión del sitio. No elimina las aprobaciones de tokens o NFT ya registradas en la blockchain. |

| Qué pasó | Qué hacer ahora | Qué no soluciona esto |
|---|---|---|
| Aprobaste un permiso de token o NFT | Desde un dispositivo de confianza, abre la lista de aprobaciones de tu billetera o un verificador de aprobaciones reconocido (escribe tú mismo su dirección web) y revoca la aprobación sospechosa. Revocar cuesta una pequeña comisión de red. Revisa si hay transferencias no autorizadas. Si los activos ya están saliendo de la billetera, mover los activos restantes a otra billetera que controles puede ser más rápido que revocar las aprobaciones una por una. | Revocar impide el uso futuro de ese permiso. No devuelve nada de lo que ya se llevaron. |
| Firmaste un mensaje o una autorización | Averigua qué firmaste: revisa la solicitud en el sitio y la actividad de tu billetera. Algunas firmas (por ejemplo, las autorizaciones de tokens de tipo Permit) permiten que alguien mueva tokens más adelante sin una transacción de aprobación aparte. Si no puedes saber qué autorizaste, deja de usar esa billetera para operaciones nuevas y mueve los activos restantes a otra billetera que controles. | Una firma no se puede deshacer. Revocar solo ayuda si la firma creó un permiso que se puede revocar. |
| Enviaste una transacción o transferencia (a un estafador, a una dirección equivocada o a una dirección envenenada) | Busca la transacción en el explorador de bloques correcto y guarda el hash de la transacción. Si los fondos fueron a una dirección de depósito de un exchange (plataforma de intercambio), contacta de inmediato a ese exchange a través de su app o sitio web oficial; es posible que pueda congelar los fondos que controla. Denuncia el incidente (consulta Denuncia más abajo). | Una transferencia confirmada en blockchain desde autocustodia por lo general no se puede revertir. Nadie puede recuperarla a cambio de una comisión. |

| Qué pasó | Qué hacer ahora | Qué no soluciona esto |
|---|---|---|
| Expusiste tu frase semilla o tu clave privada | Considera la billetera comprometida de forma permanente. En un dispositivo de confianza y limpio, y con software de billetera de la fuente oficial, crea una billetera nueva con una frase semilla nueva y luego mueve a ella los activos restantes. Mueve los activos de todas las redes y cuentas creadas a partir de esa frase semilla. Si alguna moneda que envías para comisiones desaparece al instante, un bot está vaciando la billetera: deja de enviar más. Si puede haber malware de por medio, hazlo desde otro dispositivo. Nunca reutilices la frase semilla expuesta. | Cambiar una contraseña o un PIN, revocar aprobaciones o borrar una copia digital de la frase semilla no hace que vuelva a ser secreta. Una billetera de hardware (hardware wallet) configurada con la frase semilla expuesta también está comprometida. |
| Instalaste software sospechoso, o tu dispositivo puede tener malware | Deja de usar ese dispositivo para cripto, correo electrónico y banca. Desde otro dispositivo de confianza, cambia las contraseñas importantes (primero la del correo, luego las de los exchanges) y cierra las demás sesiones. Si alguna vez escribiste o guardaste una frase semilla en el dispositivo infectado, sigue la fila de la frase semilla desde el dispositivo limpio. Haz que limpien o restablezcan el dispositivo infectado antes de volver a usarlo. | Un análisis antimalware puede pasar por alto amenazas, y no vuelve seguras las contraseñas ni las frases semilla que ya quedaron expuestas. |
| Tu cuenta de exchange o tu cuenta en línea puede estar comprometida | Contacta al servicio solo a través de su app o sitio web oficial y pídele que bloquee la cuenta. Protege primero tu cuenta de correo. Cambia la contraseña, restablece la autenticación de dos factores (mejor con una app de autenticación o una llave de seguridad), cierra las demás sesiones y revisa las direcciones de retiro, las listas blancas y las claves API. Guarda las pruebas. | Proteger la cuenta impide más accesos. Los retiros ya confirmados en la blockchain por lo general no se pueden revertir. |

| Qué pasó | Qué hacer ahora | Qué no soluciona esto |
|---|---|---|
| Tu teléfono se quedó sin servicio de repente, o recibiste un mensaje inesperado de cambio de SIM | Llama de inmediato a tu operador de telefonía desde otro teléfono, avisa de un posible SIM swap y pídele que restablezca y bloquee tu número. Luego protege las cuentas de correo y de exchange que usan ese número y cámbialas de códigos SMS a una app de autenticación o una llave de seguridad. | Recuperar el número no deshace los restablecimientos de contraseña ni los retiros realizados mientras el atacante lo tenía. |
| Una plataforma dice que debes pagar antes de poder retirar | Detente. No pagues ninguna comisión, impuesto, depósito ni importe de verificación o desbloqueo. Deja de depositar. Guarda la dirección web de la plataforma, tus chats y los hashes de las transacciones, y denúncialo. | Pagar más casi nunca libera los fondos; normalmente lleva a la siguiente exigencia. Es posible que el saldo que muestra la plataforma no exista. |
| Enviaste dinero o cripto a un estafador (inversión, romance, empleo, compra) | Deja de enviar. Corta el contacto. Conserva las pruebas. Si pagaste a través de un exchange o un banco, contáctalos de inmediato por los canales oficiales. Denuncia ante la policía. | Denunciar es importante, pero rara vez recupera cripto con rapidez. Es probable que después recibas ofertas de recuperación (siguiente fila). |
| Te están amenazando o extorsionando | No pagues y no negocies. Guarda los mensajes. Si el mensaje muestra una contraseña antigua, cámbiala en todos los lugares donde todavía la uses y activa la autenticación de dos factores. Si crees que tu seguridad física está en riesgo, contacta de inmediato a la policía. | Pagar no garantiza que las amenazas se detengan; te marca como alguien que paga. |

| Qué pasó | Qué hacer ahora | Qué no soluciona esto |
|---|---|---|
| Alguien se ofrece a recuperar tus pérdidas | Trátalo como una estafa, a menos que tú mismo hayas contactado a un organismo oficial a través de su sitio web oficial. No pagues comisiones por adelantado, no compartas tu frase semilla ni tu clave privada y no instales software de acceso remoto. Denuncia el contacto. | Nadie puede revertir una transferencia confirmada en blockchain. La policía no cobra a las víctimas por investigar un caso. |

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

## Si se aplica más de una situación

Sigue las indicaciones para la **exposición más grave**, además de las acciones de menor nivel. Por ejemplo, si conectaste una billetera, aprobaste un token y luego expusiste tu frase semilla, desconectar el sitio y revocar la aprobación no es suficiente: la frase semilla expuesta significa que la propia billetera está comprometida. Si instalaste software malicioso y luego introdujiste tu frase semilla, no crees la billetera de reemplazo en el mismo dispositivo.

DÓNDE OBTENER AYUDA

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

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

## Conserva las pruebas

Antes de borrar mensajes, cuentas o apps, guarda lo que puedas guardar de forma segura:

- hashes de transacciones y direcciones de billetera

- direcciones de sitios web, nombres de usuario y nombres de cuenta
- correos electrónicos, chats y capturas de pantalla, con fechas y horas aproximadas
- registros de pagos y comunicaciones con el exchange o la plataforma
- qué dispositivo y qué billetera usaste

Nunca compartas frases semilla, claves privadas, contraseñas ni PIN como prueba.

**DENUNCIA**

Los enlaces específicos de cada país se mantienen actualizados en cryptosafetyfirst.com/how-to-report-a-crypto-scam/ (en inglés)

- **Conserva las pruebas** (lista de arriba).
- **Contacta al exchange o servicio involucrado** a través de su app o sitio web oficial. Es posible que pueda congelar los fondos que controla.
- **Denuncia ante tu policía local** o el servicio nacional de denuncia de ciberdelitos.
- **Denuncia la dirección o el sitio web de la estafa** ante la plataforma donde los encontraste y ante un servicio de denuncia de direcciones como Chainabuse.

**MANTENTE ALERTA ANTE LAS ESTAFAS DE RECUPERACIÓN**

Después de una pérdida, es posible que te contacten personas que afirman que pueden rastrear, congelar o recuperar tu cripto. Trata toda oferta de recuperación no solicitada como una estafa. No compartas tu frase semilla ni tu clave privada, y no envíes más dinero porque alguien diga que se necesita una comisión, un impuesto o un depósito para liberar tus fondos. Consulta el Capítulo 13.

## Lo que estas acciones no pueden deshacer

- Revocar una aprobación no revierte una transferencia ya completada.
- Desconectar un sitio no revoca una aprobación on-chain.

- Cambiar la contraseña de la app de la billetera no vuelve segura una frase semilla expuesta.
- Una billetera de hardware no puede protegerte de una transacción dañina que tú mismo apruebas.

CAPÍTULO 1

# Estafas de ingeniería social

*“La estafa te ataca a ti, no a tu dispositivo.”*

*Figura 1.1: Estafas de ingeniería social de un vistazo*

La mayoría de las pérdidas de cripto no empiezan con un hackeo. Empiezan con un mensaje, una llamada, una oferta o una solicitud que te lleva a hacer algo tú mismo: pagar, instalar, firmar o compartir. Eso es ingeniería social. Ataca a las personas, no a la tecnología, y está detrás de casi todas las estafas de este libro.

Este capítulo cumple dos funciones. Primero, explica **cómo funcionan las estafas**: los detonantes que usan los estafadores y el patrón que sigue casi toda estafa. Ese conocimiento se aplica a todos los capítulos siguientes. Segundo, cubre las estafas que no encajan en ningún otro capítulo: ofertas de pago por adelantado, fraudes en operaciones P2P y OTC, vendedores y servicios falsos, trampas de “billetera gratis” y falsas campañas benéficas.

EN ESTE CAPÍTULO


- 1.1 Cómo funcionan las estafas: siete detonantes
- 1.2 El patrón detrás de casi toda estafa
- 1.3 Estafas de ingeniería social que debes conocer
- 1.4 Escenario ilustrativo: la trampa de la “billetera gratis”
- 1.5 Cómo protegerte
- 1.6 Reglas CSF de este capítulo
- 1.7 Si esto te acaba de pasar


## 1.1 Cómo funcionan las estafas: siete detonantes

Las estafas cambian de historia constantemente. La psicología de fondo no. Casi toda estafa activa uno o más de estos siete detonantes. Aprende a reconocer el detonante y podrás detectar estafas que nunca has visto.

| Detonante | Cómo suena | Tu respuesta |
|---|---|---|
| Confianza | “Soy de soporte.” “Me conoces del grupo.” | La confianza se gana fuera del chat. Verifica a través de un canal que hayas encontrado tú mismo. |
| Urgencia | “Solo quedan 10 minutos.” “Actúa ahora o lo pierdes todo.” | Los plazos reales siguen en pie después de una pausa de 24 horas. Los falsos no. |
| Miedo | “Tu cuenta está comprometida.” “Publicaremos tus datos.” | Cierra el mensaje. Revisa tu cuenta a través de la app oficial. |
| Codicia | “Duplica tus cripto.” “3 % diario garantizado.” | Los rendimientos garantizados son señal de estafa, no de oportunidad. |
| Curiosidad | “Recibiste un token.” “Mira quién vio tu billetera.” | No hagas clic, no conectes ni reclames nada para averiguarlo. |
| Autoridad | “Le habla la policía / el exchange (plataforma de intercambio) / la autoridad tributaria.” | Las autoridades no piden cripto, frases semilla (frases de recuperación) ni acceso remoto. |

| Detonante | Cómo suena | Tu respuesta |
|---|---|---|
| Oportunidad | “Preventa exclusiva.” “Acceso anticipado, solo para miembros.” | Un acceso exclusivo que se ofrece a desconocidos no es exclusivo. |

*Tabla 1.1: Los siete detonantes y cómo contrarrestarlos*

Los estafadores rara vez usan un solo detonante. Un mensaje típico combina autoridad (“seguridad del exchange”), miedo (“inicio de sesión inusual”) y urgencia (“en un plazo de 30 minutos”). Cuantos más detonantes notes, más seguro puedes estar de que algo anda mal.

## 1.2 El patrón detrás de casi toda estafa

Sea cual sea la historia, la mayoría de las estafas avanzan por los mismos cinco pasos. Puedes romper la cadena en cualquier paso, pero cuanto antes, mejor.

| Paso | Qué ocurre | Dónde puedes detenerlo |
|---|---|---|
| 1. Contacto | Alguien te contacta primero: un mensaje directo, una llamada, una respuesta a un comentario, un correo electrónico, un anuncio o una invitación a un grupo. | El contacto no solicitado sobre cripto es la primera señal de alerta (Regla SDR-001). |
| 2. Confianza | Construyen credibilidad: un nombre conocido, un logotipo, capturas de pantalla, pequeñas ganancias iniciales. | Verifica la identidad fuera de la conversación (Regla SDR-004). |
| 3. Presión | Aparece un detonante: un plazo, una amenaza, un bono que vence. | La presión es tu señal para detenerte, no para apresurarte (Regla SDR-006). |
| 4. Acción | Te piden que hagas algo: pagar, instalar, conectar, firmar, compartir. | Nunca actúes dentro del canal que controla el estafador. |
| 5. Extracción | El dinero o el acceso sale de tus manos, a menudo seguido de “un pago más”. | Deja de pagar. Ve a la tabla de triaje (Empieza aquí). |

*Tabla 1.2: El patrón de estafa en cinco pasos*

## 1.3 Estafas de ingeniería social que debes conocer

Las estafas siguientes son ingeniería social pura: sin app falsa, sin contrato malicioso, solo engaño. Las estafas que usan un canal o método específico tienen sus propios capítulos: suplantación de identidad de soporte y autoridades (Capítulo 2), plataformas de inversión falsas (Capítulo 8), estafas románticas (Capítulo 10), regalos falsos y airdrops (Capítulo 7), empleos y tareas (Capítulo 11).

### 1. Estafas de pago por adelantado

Te dicen que hay cripto esperándote (una herencia, una subvención, fondos no reclamados, un premio), pero primero debes pagar una comisión, un impuesto o un importe de “activación” para liberarlas.

**Ejemplo:** Un desconocido te contacta por “tus” fondos y el siguiente paso siempre es pagar algo primero.

#### Señales de alerta

- Dinero que no esperabas, de alguien que no conoces.
- Comisiones que deben pagarse en cripto, antes de la liberación.
- Nuevas comisiones después de cada pago.

#### Cómo evitarlo

- Nunca pagues para recibir dinero (Regla SDR-002).
- Pregúntate: ¿por qué alguien te cobraría una comisión en lugar de descontarla del importe que te debe?

### 2. Fraude en operaciones P2P y OTC

En las operaciones entre particulares (P2P) o extrabursátiles (OTC), el estafador manipula el paso del pago: una captura de pantalla de un pago falso, un pago bancario que se revierte después de que liberes las cripto, un pago de un tercero o una solicitud para cerrar el trato fuera de la plataforma.

**Ejemplo:** Un comprador envía una captura de pantalla convincente de una transferencia bancaria y te pide que liberes las cripto ya porque “el banco es lento”.

#### Señales de alerta

- Presión para liberar antes de que el dinero esté en tu cuenta.
- Pagos de un nombre que no coincide con el del comprador.

- Solicitudes para llevar el trato a un chat privado o fuera del depósito en garantía (escrow).

### Cómo evitarlo

- Libera las cripto solo cuando el pago haya llegado y no pueda revertirse.
- Mantén cada operación y cada mensaje dentro de la plataforma y su escrow.
- Considera una solicitud de salir de la plataforma como el fin del trato.

## 3. Vendedores y servicios falsos

Pagas en cripto por algo que nunca llega: hosting, servidores, equipos de minería, cuentas, tarjetas de regalo, artículos de una tienda o un servicio de “escrow” gestionado por el propio vendedor.

**Ejemplo:** Un vendedor en un grupo ofrece hardware de minería con descuento, solo a cambio de cripto, con “escrow” a través de un sitio que él recomienda.

### Señales de alerta

- Pago solo en cripto por artículos comunes.
- Precios muy por debajo del mercado.
- Un escrow o intermediario elegido por el vendedor.

### Cómo evitarlo

- Compra en tiendas establecidas con protección al comprador.
- Nunca uses un servicio de escrow que sugiera el vendedor.
- Si la única forma de pagar es con cripto, aléjate.

## 4. Trampas de “billetera gratis”

Alguien publica “por accidente” una frase semilla, o la comparte como regalo, de una billetera que parece tener un saldo alto. Para mover los fondos necesitas una pequeña cantidad de cripto para las comisiones de red. La billetera está amañada: los fondos no pueden salir y todo lo que envías se lo llevan.

**Ejemplo:** Un comentario bajo un video dice: “Mi frase semilla, no puedo acceder, por favor ayuda”. La billetera muestra miles en stablecoins, pero nada de gas.

### Señales de alerta

- Una frase semilla compartida públicamente, con un saldo visible.
- Una billetera que necesita “solo un poco” de gas de tu parte.
- Cualquier historia que termine contigo llevándote fondos que no son tuyos.

### Cómo evitarlo

- Nunca importes una frase semilla que hayas encontrado o que te hayan dado.
- Nunca envíes cripto para desbloquear fondos en la billetera de otra persona.
- Recuerda: una frase semilla compartida en internet es un cebo, no un golpe de suerte.

## 5. Falsas campañas benéficas y de emergencia

Después de un desastre, una guerra o una tragedia pública, los estafadores publican direcciones de billetera para donaciones, o un contacto te pide ayuda urgente en cripto.

**Ejemplo:** Una publicación con una foto de noticias pide donaciones en cripto para un fondo de ayuda que no existe.

### Señales de alerta

- Direcciones de donación en comentarios, mensajes directos o cuentas nuevas.
- Ninguna organización registrada detrás de la campaña.
- Presión emocional para donar ya.

### Cómo evitarlo

- Dona solo a través del sitio web de la propia organización, que debes buscar tú mismo.
- Comprueba la dirección en ese sitio web antes de enviar.
- Si un contacto te pide ayuda urgente, llámalo a un número que ya tengas.

| Estafa | Cómo funciona | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Pago por adelantado | Pagar una comisión para liberar fondos que “te deben” | Pagar primero, recibir después | Nunca pagues para recibir |
| Fraude P2P / OTC | Pago falso o reversible antes de que liberes | Presión para liberar antes de tiempo | Libera solo tras el pago definitivo |
| Vendedores y servicios falsos | Pago en cripto por artículos que nunca se entregan | Solo cripto, escrow del vendedor | Compra donde tengas protección |
| Trampas de “billetera gratis” | Una billetera amañada se queda con tu dinero para el gas | Frase semilla pública con saldo | Nunca importes frases semilla encontradas |
| Falsas campañas benéficas | Donaciones a la dirección de un estafador | Dirección en comentarios o mensajes directos | Dona a través del sitio web oficial |

*Tabla 1.3: Estafas de ingeniería social que debes conocer*

## 1.4 Escenario ilustrativo: la trampa de la “billetera gratis”

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

Alex está leyendo los comentarios bajo un video popular sobre cripto. Un comentario destaca: un usuario dice que no puede acceder a su billetera y publica la frase de recuperación de 12 palabras, pidiendo consejo. Por curiosidad, Alex importa la frase en una app de billetera. La billetera muestra un saldo de varios miles de dólares en stablecoins.

Cuando Alex intenta mover las stablecoins, la billetera indica que no hay suficiente moneda nativa de la red para pagar la comisión. Alex envía una pequeña cantidad desde su propia billetera para cubrirla. Momentos después, desaparece. Envía un poco más. Ocurre lo mismo. Las stablecoins nunca se mueven.

### Qué ocurrió

La billetera estaba preparada como trampa. Sus permisos se habían modificado para que la frase publicada no pudiera autorizar

transferencias de las stablecoins, o un bot barría cada pago entrante. El saldo era el cebo; los pagos de comisiones de Alex eran la ganancia.

### Puntos clave

- Una frase semilla publicada a la vista de todos nunca es un hallazgo afortunado.
- La trampa funciona porque parece dinero fácil y activa los detonantes de la codicia y la curiosidad.
- Importar una frase semilla desconocida también te enseña malos hábitos: nunca escribas una frase semilla en una app a menos que sea tuya y la hayas creado tú.

## 1.5 Cómo protegerte

1. **Trata el contacto no solicitado como una advertencia.** Quien inicia la conversación sobre cripto es lo primero que debes cuestionar.
2. **Verifica fuera del canal.** Usa un sitio web, una app o un número de teléfono que hayas encontrado tú mismo, no uno que te haya dado la otra persona.
3. **Nunca pagues para recibir.** Las comisiones, impuestos y depósitos que desbloquean dinero son la firma de una estafa.
4. **Mantén los tratos dentro de la plataforma.** El depósito en garantía y el soporte solo existen dentro de la plataforma; fuera de ella no tienes protección.
5. **Usa la regla de las 24 horas.** Cualquier solicitud que no pueda esperar un día es una solicitud para que dejes de pensar. Espera ese día.
6. **Nunca importes ni escribas frases semilla que no hayas creado tú.** Ni para probar, ni para ayudar, ni por curiosidad.

## 1.6 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-001

**Nunca confíes en un contacto cripto que no solicitaste.**

Antes de pagar, instalar o firmar cualquier cosa, verifica a través de un canal que hayas encontrado tú mismo.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-004 | Verifica las identidades fuera del canal del mensaje | El estafador controla el chat. La verificación real ocurre en otro lugar. |
| SDR-006 | Desconfía de la urgencia, la euforia y las ganancias garantizadas | La urgencia y los rendimientos garantizados son detonantes, no información. |
| SDR-002 | Nunca envíes cripto para recibir cripto | Las ofertas de pago por adelantado y las trampas de la “billetera gratis” dependen de ello. |
| TSR-007 | Tómate tu tiempo antes de hacer clic o instalar | La mayor parte de la ingeniería social solo funciona si actúas rápido. |

*Tabla 1.4: Reglas CSF complementarias*

## 1.7 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Luego añade los pasos para tu estafa:

| Si… | Haz esto ahora |
|---|---|
| pagaste una comisión por adelantado | Deja de pagar. Cada nueva comisión forma parte de la misma estafa. Guarda los mensajes y los datos del pago y denúncialo. |
| liberaste cripto en una operación P2P u OTC sin recibir el pago | Abre una disputa con la plataforma de inmediato, usando el ID de la orden, y mantén toda la comunicación dentro de la plataforma. |

| Si… | Haz esto ahora |
|---|---|
| recibiste un pago que podría revertirse | No liberes nada. Contacta con la plataforma y con tu banco antes de actuar. |
| pagaste a un vendedor o servicio falso | Denuncia al vendedor ante la plataforma o el grupo donde lo encontraste y ante la policía. Si pagaste desde un exchange, contacta con él indicando el hash de la transacción. |
| enviaste gas a una “billetera gratis” | Detente. La cantidad que enviaste está perdida; enviar más no desbloqueará nada. Tu propia billetera no queda comprometida por haber enviado, pero no reutilices la frase semilla de la trampa en ningún sitio. |
| donaste a una campaña de ayuda falsa | Denuncia la dirección y la publicación ante la plataforma. Avisa a las personas que la compartieron. |

*Tabla 1.5: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

Lee el artículo completo del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/social-engineering-scams-crypto-web3/

CAPÍTULO 2

# Estafas de suplantación de identidad

*“Nombres reales. Personas falsas.”*

*Figura 2.1: Estafas de suplantación de identidad de un vistazo*

En una estafa de suplantación de identidad, una persona real habla contigo mientras finge ser alguien en quien confías: el soporte de un exchange (plataforma de intercambio), una empresa de billeteras, la policía, la autoridad tributaria, un fundador conocido o un amigo al que le robaron la cuenta. La conversación es en vivo, por mensaje, llamada, video o respuesta a un comentario, y eso es lo que hace que funcione. El estafador puede responder a tus dudas, ajustar la historia y mantener la presión hasta que actúes.

La suplantación de identidad es distinta del phishing (Capítulo 3). Una página o un correo electrónico de phishing copian una marca y te esperan. Un suplantador habla contigo, te guía y normalmente te aleja de los canales oficiales que, de otro modo, comprobarías.

EN ESTE CAPÍTULO


- 2.1 Estafas de suplantación de identidad que debes conocer
- 2.2 Cómo trabajan los suplantadores
- 2.3 Escenario ilustrativo: la llamada del “equipo de seguridad”
- 2.4 Cómo protegerte
- 2.5 Reglas CSF de este capítulo
- 2.6 Si esto te acaba de pasar


# 2.1 Estafas de suplantación de identidad que debes conocer

## 1. Falso servicio de atención al cliente

Publicas en público una pregunta o una queja sobre una billetera o un exchange y, en cuestión de minutos, “soporte” te responde o te envía un mensaje directo. La cuenta parece oficial. Se ofrece a ayudarte y luego te envía un enlace, te pide tu frase semilla (frase de recuperación) o te pide que compartas tu pantalla.

**Ejemplo:** Tras una publicación sobre un retiro atascado, una cuenta con un nombre parecido al del servicio de ayuda del exchange envía un DM con un “formulario de ticket” que pide la frase semilla de 24 palabras para “verificar la propiedad”.

### Señales de alerta

- El soporte te contacta primero, por DM o respondiendo a un comentario.
- Te llevan a un chat privado, a un formulario o a una llamada.
- Solicitudes de tu frase semilla, de tu clave privada, de compartir pantalla o de acceso remoto.

### Cómo evitarlo

- Abre el soporte solo desde la app oficial o desde el sitio web oficial cuya dirección escribas tú mismo.
- Recuerda que el soporte real nunca pide tu frase semilla.
- No respondas a una “ayuda” que no solicitaste; en su lugar, denuncia la cuenta.

## 2. Llamadas de seguridad falsas y transferencias a una “billetera segura”

Alguien te llama o te escribe diciendo ser del equipo de seguridad o de fraude de tu exchange o de tu proveedor de billetera. Te advierte de actividad sospechosa y te dice que muevas tus fondos a una “billetera segura”, que apruebes una transacción de “protección” o que leas en voz alta un código. Muchas de estas llamadas usan datos personales procedentes de filtraciones de datos, lo que las hace convincentes.

**Ejemplo:** Alguien que llama y conoce tu nombre, tu dirección y la billetera de hardware (hardware wallet) que compraste dice que tu dispositivo fue comprometido y te guía paso a paso para enviar tus fondos a una nueva dirección “segura”.

### Señales de alerta

- Una llamada o un mensaje que no esperabas sobre un problema de seguridad.
- Quien llama ya conoce datos personales tuyos.
- Instrucciones para mover fondos, aprobar una transacción o compartir un código.

### Cómo evitarlo

- Cuelga. Abre tu cuenta a través de la app oficial y compruébalo tú mismo.
- Ninguna empresa legítima te dice que muevas fondos a una dirección que ella te da.
- Que una llamada incluya datos personales demuestra una filtración de datos, no que quien llama sea auténtico.

## 3. Suplantación de autoridades

El suplantador dice ser la policía, un regulador, la autoridad tributaria, un tribunal o un abogado. Te dice que tu cuenta está vinculada a un delito, que debes impuestos o que tus fondos serán congelados a menos que pagues o cooperes. Algunos envían cartas o credenciales de aspecto oficial.

**Ejemplo:** Un mensaje de una “unidad de ciberdelincuencia” dice que tu billetera se usó para lavado de dinero y que debes transferir tus fondos a una “billetera de custodia del gobierno” mientras se investiga el caso.

### Señales de alerta

- Amenazas de arresto, multas o congelación de fondos.
- Exigen el pago en cripto o en tarjetas de regalo.
- Un documento de aspecto oficial enviado por chat o por correo.

### Cómo evitarlo

- Las autoridades no piden pagos en cripto, frases semilla ni acceso remoto.
- Contacta tú mismo con el organismo usando los datos de contacto de su sitio web oficial.
- No respondas, no pagues ni discutas; guarda los mensajes y denúncialos.

## 4. Suplantación de celebridades y fundadores

Los estafadores se hacen pasar por fundadores, influencers o directivos conocidos, en mensajes, transmisiones en vivo o respuestas bajo publicaciones reales. El objetivo es promocionar un regalo falso, una inversión o una “oportunidad privada”.

**Ejemplo:** Una transmisión en vivo que parece el canal de un fundador conocido promociona una oferta por tiempo limitado para duplicar cualquier cripto enviada a una dirección que aparece en pantalla.

### Señales de alerta

- Una persona famosa te contacta directamente.
- Respuestas bajo publicaciones reales que promueven un enlace o una oferta.
- Insignias de verificación de pago y un gran número de seguidores.

### Cómo evitarlo

- Las personas famosas no envían DM con ofertas a desconocidos.
- Consulta el sitio web oficial y la cuenta principal de la persona, no la cuenta que te contactó.
- Trata cualquier oferta de “envía cripto para recibir más” como una estafa (Capítulo 7).

## 5. Contactos conocidos y cuentas hackeadas

Alguien toma el control de la cuenta de un amigo, un colega o un miembro de la comunidad, o la copia, y la usa para pedirte dinero, una

transferencia rápida de cripto o que pruebes una app o un enlace nuevos.

**Ejemplo:** La cuenta de mensajería de un colega escribe que está atrapado en el extranjero y pide cripto porque le bloquearon la tarjeta bancaria.

### Señales de alerta

- Una solicitud inusual y urgente de alguien que conoces.
- Un número o una cuenta nuevos “porque se me rompió el teléfono”.
- Reticencia a hablar por voz o por video.

### Cómo evitarlo

- Llama a la persona a un número que ya tengas.
- Haz una pregunta que solo la persona real pueda responder.
- Avisa a la persona y a los demás del grupo si la cuenta está comprometida.

## 6. Llamadas y videos deepfake

Una voz o un video generados por IA imitan a una persona real: un gerente que aprueba un pago, un familiar en apuros o un fundador que anuncia un airdrop. La calidad mejora rápidamente, así que no puedes confiar en detectar fallos.

**Ejemplo:** En una videollamada, alguien que parece y suena como un director de la empresa te pide que envíes un pago con urgencia y que lo mantengas en secreto.

### Señales de alerta

- Solicitudes urgentes de dinero en una videollamada o llamada de voz.
- Solicitudes de mantener la llamada en secreto.
- Un canal o una cuenta nuevos de una persona conocida.

### Cómo evitarlo

- Verifica a través de un segundo canal que controles antes de actuar.
- Acuerda una palabra clave familiar o de equipo para las solicitudes urgentes.
- No tomes una cara o una voz convincentes como prueba.

| Estafa | A quién fingen ser | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Soporte falso | Servicio de asistencia de un exchange o una billetera | El soporte te contacta primero | Usa el soporte solo desde la app oficial |
| Llamada de seguridad falsa | Equipo de fraude o seguridad | “Mueve tus fondos a una billetera segura” | Cuelga y revisa en la app |
| Autoridad | Policía, regulador, autoridad tributaria | Amenazas más pago en cripto | Contacta tú mismo a la agencia |
| Celebridad o fundador | Persona famosa o líder de un proyecto | Ofertas directas a desconocidos | Revisa los canales oficiales |
| Contacto conocido | Amigo o colega | Solicitud urgente desde una cuenta nueva | Llama a un número que ya tengas |
| Deepfake | Cualquier persona con video o voz públicos | Urgencia y secretismo en una llamada | Verifica por un segundo canal |

*Tabla 2.1: Estafas de suplantación de identidad que debes conocer*

## 2.2 Cómo actúan los suplantadores

La suplantación de identidad usa los detonantes del Capítulo 1, sobre todo la **autoridad**, la **confianza** y el **miedo**. Lo que la diferencia es el control de la conversación. Los suplantadores actúan en cuatro movimientos:

1. **Toman prestada credibilidad.** Un nombre de marca real, un logotipo, un cargo o datos personales filtrados.
2. **Crean un problema.** Una cuenta hackeada, un retiro bloqueado, un caso legal, una emergencia.
3. **Te aíslan.** Llevan la conversación a un chat privado, una llamada o a compartir pantalla, lejos de los canales oficiales y de las personas que podrían advertirte.

4. **Ofrecen la solución.** La “solución” es siempre una acción que entrega tus activos: compartir una frase semilla, mover fondos, aprobar una transacción, instalar software de acceso remoto.

La defensa es siempre la misma: **sal del canal**. Cierra el chat o cuelga, y luego ve a la empresa o a la agencia a través de un sitio web o una app que abras tú mismo. Si el problema es real, seguirá ahí.

## 2.3 Escenario ilustrativo: la llamada del “equipo de seguridad”

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

María recibe una llamada de alguien que dice trabajar en el equipo de seguridad del exchange que ella usa. Sabe su nombre, su dirección de correo electrónico y que ella inició sesión ayer. Le dice que se agregó un dispositivo desconocido a su cuenta y que sus fondos están en riesgo.

Le pide que instale una app de soporte para poder “proteger la cuenta” y luego la guía para mover su saldo a una “billetera protegida” mientras dura la investigación. Sigue al teléfono todo el tiempo, tranquilizándola y diciéndole que cada minuto cuenta.

### Qué pasó

Quien llamaba usó datos personales de una filtración para parecer auténtico. La app de soporte le dio acceso remoto al equipo de María, y la “billetera protegida” era suya. Su cuenta no tenía ningún problema antes de la llamada.

### Conclusiones clave

- Que quien llama conozca tus datos no lo hace auténtico.
- Ningún exchange te pide que muevas fondos a una dirección que él te da, ni que instales software de acceso remoto.
- Colgar y revisar en la app oficial habría terminado con la estafa en un minuto.

## 2.4 Cómo protegerte

1. **Nunca actúes dentro de una conversación que inició otra persona.** Cuelga o cierra el chat, y luego revisa a través de la app o el sitio web oficial.

2. **El soporte real nunca te pide tu frase semilla**, tu clave privada, acceso remoto ni una transferencia a una “billetera segura”.
3. **Mantén privados tus datos de contacto.** No publiques en abierto problemas con tu exchange o tu billetera usando tu nombre de usuario; usa el formulario de soporte oficial.
4. **Acuerda una palabra clave** con tu familia o tu equipo para las solicitudes urgentes de dinero.
5. **Da por hecho que usarán datos filtrados en tu contra.** Si compraste una billetera de hardware o usaste un exchange que sufrió una filtración de datos, trata con más desconfianza las llamadas y cartas relacionadas.
6. **Denuncia las cuentas que suplantan identidades** ante la plataforma y advierte a tu comunidad.

## 2.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-004

**Verifica las identidades fuera del canal del mensaje.**

Termina el chat o la llamada. Contacta tú mismo a la empresa o agencia a través de su sitio web o app oficial.

| 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 | El guion del “equipo de seguridad” depende de que sigas las instrucciones durante la llamada. |
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | Los suplantadores casi siempre te contactan primero. |
| GR-001 | Nunca compartas tu frase semilla | La solicitud más común en los chats de soporte falso. |

*Tabla 2.2: Reglas CSF de apoyo*

## 2.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: cuenta comprometida, frase semilla expuesta, instalaste software, enviaste una transacción. Luego añade los pasos para tu situación:

| Si… | Haz esto ahora |
|---|---|
| compartiste tu frase semilla o tu clave privada | Considera la billetera comprometida y sigue ahora la fila de la frase semilla, desde un dispositivo limpio. |
| instalaste software de acceso remoto o de “soporte” | Desconecta el dispositivo de internet, desinstala el software y sigue la fila de malware. Cambia las contraseñas desde otro dispositivo. |
| moviste fondos a una “billetera segura” | Guarda la dirección y el hash de la transacción. Si los fondos fueron a una dirección de un exchange, contacta a ese exchange de inmediato. Denúncialo a la policía. |
| diste un código de inicio de sesión o una contraseña | Cambia la contraseña y la configuración de la autenticación de dos factores desde la app oficial, cierra las demás sesiones y revisa las direcciones de retiro. |
| pagaste a una “autoridad” | Deja de pagar. Contacta a la agencia real a través de su sitio web oficial y denuncia la suplantación de identidad a la policía. |
| sigues en la llamada o en el chat | Termínala ahora. Nada legítimo tiene que ocurrir dentro de esa conversación. |

*Tabla 2.3: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/impersonation-scams-crypto-web3/

CAPÍTULO 3

# Estafas de phishing

*“El ataque empieza cuando confías en la página equivocada.”*

*Figura 3.1: Estafas de phishing de un vistazo*

El phishing copia algo en lo que confías: la página de inicio de sesión de un exchange (plataforma de intercambio), el sitio de descarga de una billetera, un aviso de entrega, un correo electrónico de soporte. A diferencia de la suplantación de identidad (Capítulo 2), normalmente no hay una conversación en vivo. La página, el correo, el mensaje de texto, el anuncio o el código QR falsos simplemente esperan a que escribas una contraseña, introduzcas tu frase semilla (frase de recuperación) o conectes tu billetera y firmes.

El phishing sigue siendo una de las vías de entrada más comunes de las pérdidas en cripto porque funciona a gran escala: una sola página falsa puede llegar a miles de personas. La buena noticia es que un solo hábito frena la mayoría de estos ataques: **nunca accedas a una cuenta importante a través de un enlace que te dio otra persona.**

EN ESTE CAPÍTULO


- 3.1 Estafas de phishing que debes conocer
- 3.2 Phishing con billetera conectada: aprobaciones, firmas y drainers (vaciadores de billeteras)
- 3.3 Ejercicio práctico: detecta el correo de phishing
- 3.4 Cómo protegerte
- 3.5 Reglas CSF de este capítulo
- 3.6 Si esto te acaba de pasar


# 3.1 Estafas de phishing que debes conocer

## 1. Phishing por correo electrónico

Correos electrónicos que imitan a un exchange, una billetera, un proveedor de correo o un servicio de entregas y te presionan para que inicies sesión, “verifiques” o “actualices” a través de un enlace. El spear phishing es la versión dirigida: usa tu nombre, tus activos o datos de una filtración.

**Ejemplo:** Un correo que parece venir de tu proveedor de billetera dice que tu billetera será suspendida si no la “verificas” hoy, con un botón que lleva a un sitio que imita al real.

### Señales de alerta

- Plazos urgentes y amenazas de suspensión.
- Direcciones del remitente o dominios de enlaces parecidos al real, pero no iguales.
- Solicitudes para introducir una frase semilla “para verificar”.

### Cómo evitarlo

- No hagas clic en enlaces de correos inesperados; en su lugar, abre la app o un marcador.
- Revisa el dominio del remitente y pasa el cursor sobre los enlaces antes que nada.
- Recuerda: ningún servicio te pide nunca tu frase semilla.

## 2. Sitios web clonados y phishing con anuncios patrocinados

Copias exactas de exchanges, páginas de descarga de billeteras, apps DeFi o sitios de NFT en dominios parecidos. Muchos se promocionan con anuncios patrocinados que aparecen por encima del resultado real.

**Ejemplo:** Una búsqueda de una app de billetera muestra un anuncio en primer lugar. El sitio parece idéntico al real, pero la descarga instala una billetera falsa, o la página de “restaurar” te pide tu frase semilla.

### Señales de alerta

- Un dominio con una letra de más, un guion o una terminación inusual.
- Llegar a través de un anuncio patrocinado o de un enlace en un chat.
- Un sitio que te pide tu frase semilla.

### Cómo evitarlo

- Guarda en marcadores los sitios oficiales que usas y usa solo esos marcadores.
- No hagas clic en anuncios patrocinados para nada relacionado con tu dinero.
- Descarga billeteras solo desde el sitio oficial del fabricante o desde la ficha oficial de la tienda de apps enlazada desde él.

## 3. Smishing y phishing por apps de mensajería

Mensajes de texto y mensajes por apps de mensajería que dicen venir de un exchange, un banco, una empresa de entregas o la autoridad tributaria, con un enlace corto.

**Ejemplo:** Un mensaje de texto dice que se solicitó un retiro de una cantidad grande desde tu cuenta y te da un enlace o un número de teléfono para cancelarlo.

### Señales de alerta

- Mensajes alarmantes sobre retiros o inicios de sesión que no hiciste.
- Enlaces cortos o números inusuales.
- Un número para devolver la llamada dentro del mensaje.

### Cómo evitarlo

- Revisa la actividad en la app oficial, nunca a través del mensaje.
- No llames a los números que aparecen en el mensaje.

- Denúncialo y bórralo.

## 4. Phishing con códigos QR

Códigos QR en correos electrónicos, cartas, carteles o chats de soporte falsos que llevan a páginas de phishing o a solicitudes de conexión de billetera. Algunos llegan por correo postal como cartas de apariencia oficial.

**Ejemplo:** Una carta impresa que parece venir de una empresa de billeteras de hardware te pide escanear un código QR para “validar” tu dispositivo e introducir tu frase semilla.

### Señales de alerta

- Un código QR que no esperabas, sobre todo en una carta o un correo.
- Un escaneo que lleva a un inicio de sesión, a una conexión de billetera o a un formulario para la frase semilla.

### Cómo evitarlo

- No escanees códigos QR para hacer gestiones en tu cuenta o billetera; abre la app oficial.
- Ningún fabricante de billeteras de hardware te pide introducir tu frase semilla en un sitio web.

## 5. Páginas falsas de NFT y para hacer mint o reclamar tokens

Páginas que copian proyectos NFT reales, lanzamientos de tokens o programas de recompensas y te piden conectar tu billetera para hacer mint, reclamar o “verificar”. Suelen difundirse a través de cuentas de proyectos hackeadas y anuncios falsos.

**Ejemplo:** El canal de la comunidad de un proyecto publica un enlace de “mint sorpresa” después de que su cuenta fue comprometida. La página copia el diseño del proyecto y pide una firma.

### Señales de alerta

- Mints o airdrops sorpresa con plazo corto.
- Enlaces publicados en chats o respuestas en lugar de en el sitio web del proyecto.
- Solicitudes de firma que no entiendes.

### Cómo evitarlo

- Revisa los anuncios en el sitio web y los canales principales del proyecto antes de actuar.
- Usa una billetera Desechable para hacer mint y reclamar tokens.
- Rechaza cualquier firma que no puedas explicar.

| Tipo | Dónde te llega | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Phishing por correo electrónico | Bandeja de entrada | Enlaces urgentes de “verificación” | Usa la app o un marcador |
| Sitios clonados y anuncios | Resultados de búsqueda, enlaces | Dominio parecido | Solo marcadores; no hagas clic en anuncios |
| Smishing | SMS y apps de mensajería | Avisos alarmantes de retiros | Compruébalo en la app oficial |
| Phishing con QR | Cartas, correos, carteles | Código QR para gestiones de la cuenta | Nunca escanees un QR para operar con tu billetera |
| Páginas falsas para hacer mint o reclamar tokens | Canales de la comunidad, respuestas | Mint sorpresa con plazo | Billetera Desechable, verifica primero |

*Tabla 3.1: Estafas de phishing que debes conocer*

## 3.2 Phishing con billetera conectada: aprobaciones, firmas y drainers

No todos los ataques de phishing piden una contraseña o una frase semilla. Muchos sitios de phishing te piden **conectar tu billetera y luego aprobar o firmar** algo. Los kits de drainers convierten esa aprobación o firma en un robo: la víctima cree que está reclamando un airdrop, haciendo mint de un NFT o “verificando” una billetera.

| Acción en el sitio | Qué puede darle al atacante |
|---|---|
| Conectar la billetera | Tu dirección y tus saldos. Por sí sola, la conexión no mueve fondos. |
| Aprobar un token o NFT | Permiso para mover esos tokens o NFT más adelante, hasta la cantidad aprobada, que a menudo es ilimitada. |
| Firmar un mensaje o una autorización | Según lo que firmes, permiso para mover tokens sin una transacción de aprobación separada (por ejemplo, firmas de tipo Permit). |
| Enviar una transacción | Lo que haga la transacción: una transferencia, un swap (intercambio de tokens), una nueva aprobación. |
| Escribir la frase semilla | Control total de la billetera. |

*Tabla 3.2: Conectar, aprobar, firmar, enviar: lo que cada paso puede entregar*

Los sitios que no imitan ninguna marca y cuyo único truco es la aprobación o la propia transacción se tratan en el Capítulo 5 (Contratos y aprobaciones maliciosos). Las billeteras de hardware protegen tus claves privadas, pero no pueden protegerte de una aprobación o firma dañina que confirmes en el dispositivo.

## 3.3 Ejercicio práctico: detecta el correo de phishing

Antes de hacer algo a raíz de un correo sobre tus cuentas, haz estas cinco comprobaciones. Si falla alguna, detente.

1. **Remitente:** ¿el dominio es exactamente el dominio propio de la empresa?
2. **Enlace:** ¿el enlace (pasa el cursor por encima para verlo) va al dominio real de la empresa?
3. **Solicitud:** ¿pide una contraseña, un código o una frase semilla? Una solicitud de frase semilla siempre es phishing.
4. **Presión:** ¿hay un plazo, una amenaza o una oferta inusualmente buena?
5. **Expectativa:** ¿hiciste algo que explique este correo?

## 3.4 Cómo protegerte

1. **Guarda en marcadores cada sitio financiero que uses** y accede a ellos solo a través de los marcadores o de la app oficial.
2. **Nunca introduzcas tu frase semilla en un sitio web, formulario o app**, salvo cuando restaures una billetera que sea tuya, en software de la fuente oficial.
3. **Lee cada solicitud de la billetera** antes de confirmarla. Rechaza todo lo que no entiendas.
4. **Separa tus billeteras.** Usa una billetera Desechable para sitios nuevos, mints y para reclamar tokens, y nunca conectes tu billetera Bóveda a ningún sitio web.
5. **Usa un inicio de sesión resistente al phishing** para exchanges y correo: una llave de seguridad de hardware o una llave de acceso (passkey) cuando esté disponible.
6. **Usa las advertencias de tu billetera y una extensión de seguridad de confianza** como capa adicional, nunca como tu única comprobación.

## 3.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-009

**Verifica todos los enlaces antes de iniciar sesión.**

Usa marcadores o direcciones que escribas tú mismo, y lee cada solicitud de la billetera antes de firmar.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| GR-002 | Verifica siempre la URL y el dominio completos antes de conectar tu billetera a cualquier sitio web | Los sitios clonados se basan en dominios que a simple vista parecen correctos. |
| GR-001 | Nunca compartas tu frase semilla | Una solicitud de frase semilla es la señal de phishing más clara. |

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| TSR-004 | Usa autenticación de dos factores basada en hardware | Las llaves de seguridad no caen ante las páginas de phishing que roban códigos. |
| SDR-005 | Nunca conectes tu billetera a sitios web desconocidos | Las páginas de drainers necesitan primero una conexión de billetera. |

*Tabla 3.3: Reglas CSF de apoyo*

## 3.6 Si esto te acaba de pasar

Primero encuentra tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: solo lo viste, conectaste, aprobaste, firmaste, frase semilla expuesta, instalaste software, cuenta comprometida. Después añade los pasos para tu situación:

| Si… | Haz esto ahora |
|---|---|
| solo abriste el correo o la página | Ciérralo. Si no escribiste, conectaste ni descargaste nada, tus cuentas no quedan comprometidas por haberlo visto. |
| introdujiste una contraseña o un código de inicio de sesión | Cambia esa contraseña desde la app o el sitio oficial, también en todos los lugares donde la reutilizaste, cierra las demás sesiones y revisa si tu cuenta de correo tiene reglas de reenvío. |
| introdujiste tu frase semilla | Considera la billetera comprometida. Sigue ahora la fila de la frase semilla, desde un dispositivo limpio. |
| conectaste, aprobaste o firmaste en un sitio de phishing | Sigue las filas de conectar, aprobar y firmar en ese orden. Revoca lo que puedas y mueve los activos restantes si ya empezaron las transferencias. |
| descargaste una “billetera” o un archivo | Sigue la fila de malware y considera expuesta cualquier frase semilla que hayas escrito en esa app. |

*Tabla 3.4: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee el artículo completo del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/phishing-scams-crypto-web3/

CAPÍTULO 4

# Aplicaciones y billeteras falsas

*“Una sola app falsa puede anular una buena seguridad.”*

*Figura 4.1: Aplicaciones y billeteras falsas de un vistazo*

Todo usuario de cripto depende de software: una app de billetera, una extensión del navegador, la app de un exchange (plataforma de intercambio) y, a veces, una billetera de hardware (hardware wallet). Si esa herramienta es falsa o ha sido manipulada, todo lo que haces con ella es visible para el estafador, empezando por la frase semilla (frase de recuperación) que escribes en ella. Los buenos hábitos no pueden protegerte de una herramienta que fue creada para robar.

Este capítulo trata las billeteras, apps, extensiones, herramientas de recuperación y dispositivos de hardware falsos o manipulados que tú mismo instalas, configuras y usas. El software malicioso que infecta tu dispositivo de otras formas (infostealers, secuestradores del portapapeles, herramientas de acceso remoto) se trata en la guía Hackers.

EN ESTE CAPÍTULO


- 4.1 Aplicaciones y billeteras falsas que debes conocer
- 4.2 Por qué una billetera de hardware no arregla una configuración falsa
- 4.3 Escenario ilustrativo: la extensión de ayuda para trading
- 4.4 Cómo protegerte
- 4.5 Reglas CSF de este capítulo
- 4.6 Si esto te acaba de pasar


# 4.1 Aplicaciones y billeteras falsas que debes conocer

## 1. Apps de billetera y extensiones del navegador falsas

Copias de billeteras populares en tiendas de apps, tiendas de extensiones del navegador o en sitios de descarga que imitan al real. Parecen idénticas a la billetera real. Cuando creas o restauras una billetera, la frase semilla se envía al estafador.

**Ejemplo:** Un anuncio patrocinado en un buscador lleva a una página de descarga de una conocida extensión de billetera. La extensión funciona con normalidad, pero cada frase semilla que se introduce durante la configuración se copia al estafador.

### Señales de alerta

- Un enlace de descarga que viene de un anuncio, un chat o la descripción de un video.
- Un nombre de editor, número de reseñas o número de instalaciones que no coincide con la billetera real.
- Que te pida restaurar una billetera existente justo después de instalar la app.

### Cómo evitarlo

- Empieza en el sitio web oficial del fabricante de la billetera y sigue su propio enlace a la ficha de la tienda.
- Comprueba el nombre del editor antes de instalar.
- Crea billeteras nuevas en lugar de restaurar frases semilla antiguas en apps recién instaladas que no has verificado.

## 2. Billeteras de hardware manipuladas y preconfiguradas

Las billeteras de hardware compradas en marketplaces, a revendedores o a vendedores de segunda mano pueden estar modificadas, o venir con una frase semilla ya impresa en una tarjeta “para tu comodidad”. Quien preparó esa frase semilla controla la billetera.

**Ejemplo:** Una billetera de hardware con descuento comprada en un marketplace en línea llega con una tarjeta para raspar que muestra una frase semilla e instrucciones para usarla.

### Señales de alerta

- Una frase semilla incluida en la caja.
- Sellos dañados o ausentes, o un dispositivo que ya está configurado.
- Precios muy por debajo de los de la tienda oficial.

### Cómo evitarlo

- Compra solo al fabricante o a los revendedores oficiales que figuran en su lista.
- Genera siempre tú mismo una nueva frase semilla en el dispositivo.
- Nunca uses una frase semilla que no hayas creado tú.

## 3. Herramientas falsas de recuperación, validación y “sincronización”

Sitios web y apps que dicen arreglar una billetera bloqueada, “validarla” o “sincronizarla”, recuperar fondos perdidos o comprobar su seguridad, y para ello te piden introducir tu frase semilla.

**Ejemplo:** Después de una transacción fallida, una respuesta en un foro enlaza a una herramienta de “rectificación de billetera” que pide la frase semilla para reparar la billetera.

### Señales de alerta

- Cualquier herramienta que te pida tu frase semilla para arreglar, comprobar o sincronizar una billetera.
- Enlaces compartidos en respuestas a preguntas de soporte.

### Cómo evitarlo

- Ninguna herramienta legítima necesita tu frase semilla, excepto tu propia billetera durante una restauración.

- Pide ayuda solo a través del soporte oficial del fabricante de la billetera.

## 4. Aplicaciones falsificadas de exchanges y de trading

Versiones falsas de exchanges o plataformas de trading reales, distribuidas como archivos de aplicación, versiones de prueba (test-flight) o enlaces fuera de las tiendas oficiales. Capturan tu inicio de sesión y tus códigos de dos factores, o muestran saldos falsos.

**Ejemplo:** Un mensaje ofrece una versión “pro” de la aplicación de un exchange conocido con comisiones más bajas, que se instala desde un enlace en lugar de la tienda de aplicaciones.

### Señales de alerta

- Aplicaciones instaladas desde un enlace o un archivo en lugar de la tienda oficial.
- Versiones especiales con funciones o comisiones que la aplicación real no ofrece.

### Cómo evitarlo

- Instala las aplicaciones de exchanges solo desde la tienda oficial, a través del propio sitio web del exchange.
- Si la aplicación de un exchange te pide que vuelvas a iniciar sesión de forma inesperada, ciérrala y revisa la aplicación oficial.

## 5. Falsos asistentes de trading, herramientas de seguridad y verificadores de billeteras

Extensiones del navegador y aplicaciones que prometen señales de trading, seguimiento de portafolio, verificación de airdrops o seguridad para la billetera. Algunas leen todo lo que haces en el navegador, incluidas las sesiones abiertas en exchanges, o reemplazan las direcciones que copias.

**Ejemplo:** Una extensión gratuita que añade herramientas de trading al sitio web de un exchange lee en silencio los datos de sesión del usuario conectado.

### Señales de alerta

- Extensiones que piden permiso para leer y cambiar datos en todos los sitios web.

- Herramientas recomendadas en grupos de trading o por influencers que no puedes verificar.
- Herramientas publicadas recientemente con pocas reseñas pero mucha promoción.

### Cómo evitarlo

- Instala la menor cantidad posible de extensiones, y ninguna en el navegador que usas para cripto.
- Revisa los permisos solicitados antes de instalar.
- Elimina las extensiones que ya no uses.

| Tipo | Qué roba | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Aplicación o extensión de billetera falsa | Frase semilla durante la configuración | Descarga desde un anuncio o un chat | Empieza desde el sitio web oficial |
| Billetera de hardware manipulada | Control de la billetera | Frase incluida en la caja | Compra directamente; crea tu propia frase |
| Herramienta falsa de recuperación o sincronización | Frase semilla | Pide tu frase para arreglar la billetera | Usa solo el soporte oficial |
| Aplicación de exchange falsificada | Inicio de sesión y códigos | Instalada desde un enlace | Solo la tienda oficial |
| Falso asistente o herramienta de seguridad | Sesiones, direcciones copiadas | Permisos amplios | Extensiones mínimas, navegador separado |

*Tabla 4.1: Aplicaciones y billeteras falsas que debes conocer*

## 4.2 Por qué una billetera de hardware no arregla una configuración falsa

Las billeteras de hardware mantienen tus claves privadas fuera de tu equipo, y eso te protege de muchos ataques. No pueden ayudarte en tres situaciones que se tratan en este capítulo:

- **La frase no la creaste tú.** Un dispositivo preconfigurado o una frase preimpresa le da las claves a otra persona desde el primer día.
- **Escribiste la frase en un software.** Introducir la frase de tu billetera de hardware en una aplicación o herramienta de recuperación falsa la expone igual que la de una billetera de software.
- **Apruebas lo que se te muestra.** Una aplicación falsa puede mostrarte una transacción dañina; si la confirmas en el dispositivo, queda firmada.

El robo de la sesión del navegador es un caso aparte. Si una extensión roba tu sesión abierta en un exchange, el atacante puede actuar como tú sin necesitar tu contraseña ni tu código de dos factores, porque la sesión ya está iniciada. Una autenticación de dos factores sólida protege el inicio de sesión, no una sesión que ya fue robada.

## 4.3 Escenario ilustrativo: la extensión de asistente de trading

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

Leo opera activamente en un exchange. En un grupo de trading ve una extensión gratuita para el navegador que añade gráficos y alertas avanzados al sitio web del exchange. La instala en su navegador habitual y concede los permisos que pide.

Unos días después, aparecen en su cuenta operaciones que él no hizo, y su saldo se mueve a través de pares con poco volumen. Cuando inicia sesión, todo parece normal: su contraseña y su configuración de dos factores no han cambiado.

### Qué pasó

La extensión leyó la sesión del exchange en el navegador de Leo y se la pasó al atacante, que usó directamente la sesión ya iniciada. Nunca necesitó la contraseña ni el código de dos factores de Leo.

### Conclusiones clave

- Las extensiones con acceso a todos los sitios web pueden leer lo que haces en tu exchange.
- Usa un navegador separado, o un perfil de navegador, sin extensiones para tus cuentas cripto.

- Si sospechas un robo de sesión, cierra todas las sesiones desde la aplicación oficial y elimina la extensión.

## 4.4 Cómo protegerte

1. **Empieza desde el sitio web oficial** de la billetera o del exchange y sigue sus enlaces a las descargas y a las fichas de las tiendas.
2. **Compra las billeteras de hardware directamente** al fabricante o a sus revendedores oficiales indicados.
3. **Crea tu propia frase semilla** en cada billetera y dispositivo nuevos. Nunca aceptes una frase que haya preparado otra persona.
4. **Nunca escribas tu frase semilla en ninguna aplicación, sitio web o herramienta**, excepto en tu propia billetera cuando la restaures.
5. **Opera con cripto en un perfil de navegador limpio** sin extensiones, o en un dispositivo que uses solo para cripto.
6. **Revisa y elimina extensiones** con regularidad, y comprueba los permisos de todo lo que conserves.

## 4.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · TSR-001

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

Obtén billeteras y aplicaciones solo del sitio oficial del fabricante o de la tienda de aplicaciones. Nunca escribas tu frase semilla en una aplicación o sitio web: restáurala solo en tu propia billetera oficial y, en una billetera de hardware, solo en la pantalla del propio dispositivo.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| GR-001 | Nunca compartas tu frase semilla | Las herramientas falsas existen para capturar la frase. |
| GR-003 | Usa siempre una billetera de hardware para guardar cripto a largo plazo o de alto valor | Solo si la compraste al fabricante y la configuraste con tu propia frase. |

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| TSR-002 | Da por hecho que tu dispositivo puede estar comprometido | Planifica como si una extensión o aplicación pudiera estar leyendo tu actividad. |
| TSR-006 | Separa dispositivos y cuentas para el uso de cripto | Un navegador o dispositivo limpio limita lo que una herramienta falsa puede ver. |

*Tabla 4.2: Reglas CSF complementarias*

## 4.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: frase semilla expuesta, instalaste software, cuenta comprometida. Luego añade los pasos para tu situación:

| Si tú… | Haz esto ahora |
|---|---|
| introdujiste tu frase semilla en una aplicación, extensión o herramienta | Considera la billetera comprometida. Sigue la fila de la frase semilla desde un dispositivo limpio, y no crees la billetera nueva en la misma aplicación. |
| configuraste una billetera de hardware con una frase que venía en la caja | Considérala comprometida. Mueve los fondos a una billetera nueva cuya frase hayas generado tú mismo en un dispositivo comprado al fabricante. |
| instalaste una extensión o aplicación sospechosa | Elimínala. Cierra todas las sesiones del exchange desde la aplicación oficial, cambia las contraseñas desde un dispositivo limpio y sigue la fila de malware. |
| iniciaste sesión en una aplicación de exchange falsificada | Cambia la contraseña y la configuración de dos factores en la aplicación oficial, cierra las demás sesiones y revisa las direcciones de retiro. |

*Tabla 4.3: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/scam-apps-browser-extension-crypto-web3/

CAPÍTULO 5

# Contratos y aprobaciones maliciosos

*“Toda firma merece sospecha.”*

*Figura 5.1: Contratos y aprobaciones maliciosos de un vistazo*

En estas estafas, la trampa es el propio contrato inteligente. No hay una marca falsa ni una conversación, solo una dApp, un bot o una página de mint que te pide aprobar, firmar o enviar. Una vez que confirmas, el contrato hace aquello para lo que fue escrito: mover tus tokens al estafador.

Este capítulo explica qué entregas realmente con cada acción de la billetera, las principales estafas basadas en contratos y cómo limitar el daño con la gestión de aprobaciones y la separación de billeteras. Las páginas de phishing que copian una marca real se tratan en el Capítulo 3; los exploits de protocolos legítimos, en los que los usuarios no hicieron nada mal, se tratan en la guía de Hackers.

EN ESTE CAPÍTULO


- 5.1 Aprobaciones y firmas en lenguaje sencillo
- 5.2 Estafas con contratos maliciosos que debes conocer
- 5.3 Escenario ilustrativo: el tutorial del bot MEV
- 5.4 Cómo protegerte
- 5.5 Reglas CSF de este capítulo
- 5.6 Si esto te acaba de pasar


## 5.1 Aprobaciones y firmas en lenguaje sencillo

| Término | Qué significa | Por qué importa |
|---|---|---|
| Aprobación (allowance) | Permiso para que un contrato mueva un token específico desde tu billetera, hasta una cantidad determinada. | Las aprobaciones ilimitadas siguen activas hasta que las revocas, incluso después de salir del sitio. |
| Aprobación de NFT para todo (approval for all) | Permiso para que un contrato mueva todos los NFT de una colección. | Un solo clic puede exponer una colección entera. |
| Firma | Un mensaje que firmas con tu billetera. Algunos son inicios de sesión inofensivos; otros autorizan transferencias. | Las firmas de tipo permit pueden conceder acceso a los tokens sin una transacción de aprobación aparte. |
| Firma a ciegas (blind signing) | Confirmar una solicitud que tu billetera no puede decodificar por completo, de modo que solo ves datos sin procesar. | No puedes saber qué estás aceptando. |
| Revocar | Una transacción que devuelve una aprobación a cero. | Detiene el uso futuro del permiso; no devuelve lo que ya se llevaron. |

*Tabla 5.1: Aprobaciones y firmas en lenguaje sencillo*

## 5.2 Estafas con contratos maliciosos que debes conocer

### 1. Solicitudes de aprobación maliciosas

DApps desconocidas, juegos, herramientas de rendimiento o páginas para “reclamar” tokens piden una aprobación como parte de una acción que parece normal. La aprobación es por una cantidad ilimitada o para un token que no esperabas.

**Ejemplo:** Un nuevo sitio de rendimiento te pide aprobar USDC ilimitados “para habilitar los depósitos” y, días después, vacía la billetera.

#### Señales de alerta

- Aprobaciones ilimitadas para una acción sencilla.
- Aprobación para un token que no tiene relación con lo que estás haciendo.
- Una dirección de contrato que no puedes verificar en ningún otro lugar.

#### Cómo evitarlo

- Aprueba solo la cantidad que necesitas, cuando tu billetera lo permita.
- Usa una billetera Desechable para DApps que no conoces.
- Revoca las aprobaciones cuando termines.

### 2. Bots falsos de trading, arbitraje y MEV

Videos y publicaciones ofrecen un “bot rentable”: despliega un contrato a partir de un fragmento de código, depósitale fondos y ponlo en marcha. El código oculta una función que envía los fondos al estafador.

**Ejemplo:** Un video tutorial muestra cómo desplegar un contrato de “bot de arbitraje” con código copiado y depositarle ETH para empezar a operar.

#### Señales de alerta

- Ganancias garantizadas de un bot que despliegas tú mismo.
- Código que no puedes leer, copiado de un video o de un chat.
- Secciones de comentarios llenas de elogios.

### Cómo evitarlo

- Nunca despliegues ni deposites fondos en código que no puedas leer por completo.
- Trata los tutoriales de “ganancias pasivas con bots” como estafas.

## 3. Vaciados mediante firmas

En lugar de una transacción de aprobación, el sitio te pide firmar un mensaje. La firma autoriza transferencias de tokens, así que los fondos pueden moverse más tarde sin ninguna otra solicitud.

**Ejemplo:** Un “mint gratuito” pide una firma que parece un inicio de sesión, pero es una autorización de tipo Permit sobre tus tokens.

### Señales de alerta

- Solicitudes de firma en sitios que acabas de encontrar.
- Firma a ciegas o datos ilegibles.
- Un “inicio de sesión” que no hace falta para lo que estás haciendo.

### Cómo evitarlo

- Rechaza las firmas que no puedas leer y explicar.
- Mantén desactivada la firma a ciegas, salvo que la necesites para una app específica de confianza.

## 4. Mints falsos que no imitan ninguna marca y contratos para reclamar tokens

Páginas para hacer mint o reclamar tokens de proyectos que no existen, promocionadas mediante anuncios, respuestas y tokens enviados por airdrop. La transacción de mint incluye una aprobación sobre todos tus NFT o tokens.

**Ejemplo:** Una página que ofrece un mint gratuito limitado te pide aprobar toda tu colección de NFT “para verificación”.

### Señales de alerta

- Aprobación sobre todos tus NFT para mintear uno.
- Plazos y contadores que muestran que casi está agotado.

### Cómo evitarlo

- Mintea solo de proyectos que hayas comprobado de forma independiente.
- Mintea desde una billetera Desechable que no guarde nada más.

| Tipo | Lo que confirmas | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Aprobación maliciosa | Aprobación ilimitada de tokens | Más acceso del que la acción necesita | Limita, separa, revoca |
| Bot falso de trading o MEV | Desplegar un contrato y depositarle fondos | Código que no puedes leer | Nunca despliegues código desconocido |
| Vaciado mediante firma | Un mensaje firmado | Firma ilegible o inesperada | Rechaza lo que no puedas explicar |
| Mint falso o reclamación falsa de tokens | Mint con aprobación total | Aprobación total para mintear uno | Solo billetera Desechable |

*Tabla 5.2: Estafas con contratos maliciosos que debes conocer*

## 5.3 Escenario ilustrativo: el tutorial del bot MEV

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

Nina ve un video muy cuidado que explica cómo los “bots MEV” generan ganancias pasivas. El creador comparte el código del contrato y una guía paso a paso: pegar el código en un editor en línea, desplegarlo, enviar ETH al contrato y pulsar “start”.

Nina sigue los pasos con 1 ETH. Cuando pulsa “start”, el saldo del contrato baja a cero. El historial de transacciones muestra que el ETH fue a una dirección que ella no reconoce.

### Qué pasó

El código contenía una dirección oculta que recibía los fondos cuando se llamaba a la función de inicio. Nunca hubo un bot.

### Conclusiones clave

- Las ganancias de un código que copias y no entiendes no son reales.
- La sección de comentarios era parte de la estafa.
- Desplegar un contrato no te convierte en su único controlador si el código dice lo contrario.

## 5.4 Cómo protegerte

1. **Separa tus billeteras.** Guarda tus fondos a largo plazo en una billetera Bóveda que nunca se conecte a DApps. Usa una billetera de Uso Frecuente para apps de confianza y una billetera Desechable para cualquier cosa nueva.
2. **Lee antes de confirmar.** Revisa la acción, el token, la cantidad y el contrato. Si tu billetera no puede decodificarlo, recházalo.
3. **Aprueba lo mínimo.** Prefiere aprobaciones limitadas en lugar de ilimitadas.
4. **Revoca con regularidad.** Revisa tus aprobaciones en tu billetera o en un verificador de aprobaciones de buena reputación y revoca todo lo que ya no uses.
5. **Nunca despliegues ni deposites fondos en código que no puedas leer.**
6. **Recuerda lo que hace una billetera de hardware (hardware wallet).** Protege tus claves privadas. No convierte en segura una aprobación o una firma dañina si la confirmas en el dispositivo.

## 5.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · GR-004

**Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos.**

Rechaza las aprobaciones ilimitadas que no necesites y usa una billetera Desechable para contratos que no conoces.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-005 | Nunca conectes tu billetera a sitios web desconocidos | Toda estafa con contratos empieza con una conexión. |
| GR-008 | Guarda tus fondos a largo plazo en una billetera bóveda. Usa otra billetera para DApps, trading y Web3 | La separación limita lo que puede alcanzar una sola aprobación maliciosa. |

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| GR-002 | Verifica siempre la URL y el dominio completos antes de conectar tu billetera a cualquier sitio web | Debes saber exactamente a qué sitio te estás conectando. |

*Tabla 5.3: Reglas CSF complementarias*

## 5.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: conectaste, aprobaste, firmaste, enviaste una transacción. Luego añade los pasos para tu situación:

| Si… | Haz esto ahora |
|---|---|
| aprobaste un contrato sospechoso | Revoca la aprobación desde un dispositivo de confianza. Si las transferencias ya empezaron, primero mueve los activos restantes a otra billetera que controles. |
| firmaste un mensaje que no puedes explicar | Deja de usar la billetera para nueva actividad y mueve los activos restantes a otra billetera que controles. |
| desplegaste un bot o le depositaste fondos | No envíes más fondos para “desbloquearlo”. Guarda la dirección del contrato y las transacciones, y denúncialos. |
| minteaste con una aprobación total | Revoca la aprobación de la colección y mueve los NFT valiosos a otra billetera. |

*Tabla 5.4: Primeras acciones específicas de este capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/smart-contract-scams-crypto-web3/

CAPÍTULO 6

# Estafas de envenenamiento de direcciones

*“La dirección parecía correcta. Solo el centro estaba mal.”*

*Figura 6.1: Estafas de envenenamiento de direcciones de un vistazo*

Las direcciones cripto son largas y difíciles de leer, así que la mayoría de la gente solo revisa los primeros y los últimos caracteres. El envenenamiento de direcciones aprovecha exactamente eso. Los estafadores crean direcciones que empiezan y terminan como una que tú usas y luego las colocan en tu historial de transacciones. La próxima vez que copies una dirección de tu historial, puede que copies la suya.

Es un capítulo corto porque la estafa es sencilla. También es una de las pérdidas más fáciles de prevenir y de las más difíciles de revertir.

EN ESTE CAPÍTULO


- 6.1 Cómo funciona el envenenamiento de direcciones
- 6.2 Variantes que debes conocer
- 6.3 Escenario ilustrativo: el depósito en el exchange
- 6.4 Cómo protegerte
- 6.5 Reglas CSF de este capítulo
- 6.6 Si esto te acaba de pasar


## 6.1 Cómo funciona el envenenamiento de direcciones

1. **Observan.** Los estafadores vigilan la blockchain en busca de billeteras que mueven cantidades importantes.
2. **Copian la apariencia.** Generan una dirección cuyos primeros y últimos caracteres coinciden con los de una a la que envías a menudo.
3. **Envenenan.** Envían desde esa dirección parecida una transferencia diminuta, de valor cero o de un token falso, para que aparezca en tu historial junto a tus transacciones reales.
4. **Esperan.** La próxima vez que copies una dirección de tu historial para enviar fondos, puede que elijas la dirección parecida.

La transferencia de envenenamiento no le da a nadie acceso a tu billetera. Verla es inofensivo. La pérdida solo ocurre si envías fondos a la dirección parecida.

## 6.2 Variantes que debes conocer

| Variante | Lo que ves | Señal de alerta clave |
|---|---|---|
| Transferencias de valor cero | Una transferencia de 0 tokens “desde” ti o hacia ti | Transferencias que no hiciste en tu historial |
| Transferencias de polvo (dust) | Una cantidad entrante diminuta desde una dirección parecida | Depósitos pequeños inesperados |
| Transferencias de tokens falsos | Una transferencia de un token con el mismo nombre y símbolo que uno real | Un token conocido desde un contrato desconocido |

| Variante | Lo que ves | Señal de alerta clave |
|---|---|---|
| Cambios en el portapapeles | La dirección cambia entre copiar y pegar | Malware en tu dispositivo; consulta la guía de Hackers |

*Tabla 6.1: Variantes del envenenamiento de direcciones*

## 6.3 Escenario ilustrativo: el depósito en el exchange

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

Ben mueve sus ahorros de su billetera de hardware (hardware wallet) a un exchange (plataforma de intercambio) cada pocos meses. Normalmente copia la dirección de depósito del exchange de su última transacción. Esta vez, el historial muestra una transferencia entrante que no recuerda, desde una dirección que empieza y termina exactamente igual que su dirección de depósito.

Ben copia la primera dirección de la lista, revisa los primeros y los últimos cuatro caracteres en la pantalla del dispositivo y confirma. Los fondos nunca llegan al exchange.

### Qué pasó

La primera entrada era una transferencia de envenenamiento. La revisión de Ben de los primeros y los últimos caracteres salió bien porque el estafador había generado una dirección que coincidía con ellos. El dispositivo mostraba la dirección completa, pero él no comparó el centro.

### Puntos clave

- Nunca copies direcciones de tu historial de transacciones.
- Revisar solo el inicio y el final es exactamente lo que la estafa está diseñada para burlar.
- Una billetera de hardware muestra la dirección completa; compárala entera.

## 6.4 Cómo protegerte

1. **Nunca copies una dirección de tu historial de transacciones.** Cópiala de la fuente: la página de depósito del exchange, un contacto guardado o directamente del destinatario.
2. **Usa la libreta de direcciones de tu billetera** y la lista blanca de retiros del exchange para las direcciones que usas con frecuencia.
3. **Compara la dirección completa**, no solo el principio y el final, en la pantalla de tu billetera de hardware.
4. **Envía una pequeña transacción de prueba** antes de transferencias grandes y luego vuelve a revisar la dirección completa para la transferencia principal: los estafadores a veces reaccionan a tu prueba con una nueva dirección parecida.
5. **Ignora las transferencias inesperadas** en tu historial. No interactúes con ellas.

## 6.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · OR-005

**Verifica siempre el destino antes de enviar cripto.**

Nunca copies direcciones de tu historial. Usa tu libreta de direcciones y revisa cada carácter.

| Regla | Enunciado | Por qué aplica aquí |
|---|---|---|
| GR-006 | Envía siempre una pequeña transacción de prueba antes de transferir grandes cantidades de cripto | Una prueba confirma la ruta, siempre que vuelvas a revisar la dirección para la transferencia principal. |
| TSR-005 | Activa las listas blancas de retiros en los exchanges | Las listas blancas impiden enviar a direcciones que no has guardado. |

*Tabla 6.2: Reglas CSF complementarias*

## 6.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: enviaste una transacción, solo viste, instalaste software. Luego añade los pasos para tu situación:

| Si tú… | Haz esto ahora |
|---|---|
| enviaste fondos a una dirección envenenada | Guarda el hash de la transacción y ambas direcciones. Denuncia la dirección. Actúa rápido: si los fondos llegan a un exchange, ese exchange podría congelarlos tras una denuncia. |
| ves transferencias de envenenamiento en tu historial | No hay nada comprometido. No interactúes con ellas y, de ahora en adelante, copia las direcciones solo desde su fuente. |
| crees que la dirección cambió al pegarla | Eso apunta a malware, no a envenenamiento. Sigue la fila de malware. |

*Tabla 6.3: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/address-poisoning-scams-crypto-web3/

CAPÍTULO 7

# Estafas de regalos y airdrops

*“Los tokens gratis pueden convertirse en errores caros.”*

*Figura 7.1: Estafas de regalos y airdrops de un vistazo*

Los airdrops y los regalos son una parte real de cripto: los proyectos recompensan a los primeros usuarios y promocionan tokens nuevos. Los estafadores los copian para que conectes, firmes, pagues o compartas datos. El cebo siempre es algo gratis; el precio es tu billetera.

Existen airdrops legítimos, y algunos requieren que conectes una billetera y envíes una transacción para reclamarlos, con una comisión de red. Así que la pregunta nunca es solo “¿me pide que me conecte?”, sino **¿dónde lo encontré y qué exactamente me están pidiendo que apruebe o pague?**

EN ESTE CAPÍTULO


- 7.1 Estafas de regalos y airdrops que debes conocer
- 7.2 Tokens inesperados en tu billetera
- 7.3 Escenario ilustrativo: el token con un sitio web en su nombre
- 7.4 Cómo protegerte
- 7.5 Reglas CSF de este capítulo
- 7.6 Si esto te acaba de pasar

# 7.1 Estafas de regalos y airdrops que debes conocer

## 1. Regalos falsos de “envía para recibir”

Una persona famosa, un proyecto o un exchange (plataforma de intercambio) parece prometer que te devolverá el doble de lo que envíes. Las transmisiones en vivo, los videos deepfake y las respuestas bajo publicaciones reales son canales habituales.

**Ejemplo:** Una transmisión en vivo con la cara de un fundador conocido muestra una dirección y una cuenta regresiva: envía cualquier cantidad y recibe el doble de vuelta.

### Señales de alerta

- Cualquier promesa de devolver más de lo que envías.
- Cuentas regresivas y listas de “ganadores” en vivo.
- Nombres famosos en cuentas que no son sus canales principales.

### Cómo evitarlo

- Nunca envíes cripto para recibir cripto. No hay excepciones.
- Denuncia la transmisión o la publicación ante la plataforma.

## 2. Sitios falsos para reclamar airdrops

Sitios que copian un airdrop real o inventado y te piden que te conectes y apruebes o firmes para reclamarlo. La aprobación o la firma entrega tus tokens a un drainer (vaciador de billeteras).

**Ejemplo:** Una publicación anuncia un airdrop para los poseedores de un token popular, con un enlace para reclamarlo. La página pide una aprobación sobre tu mayor saldo de tokens.

### Señales de alerta

- Enlaces para reclamar en respuestas, anuncios o mensajes directos.
- Solicitudes de aprobación de tokens que no tienen relación con el airdrop.
- Plazos cortos.

### Cómo evitarlo

- Busca airdrops solo en el sitio web oficial del proyecto y en sus canales principales.

- Reclama desde una billetera Desechable.
- Revisa exactamente qué te piden aprobar o firmar.

## 3. Pagar para reclamar y tarifas de elegibilidad

Te dicen que eres elegible para una recompensa, pero que primero debes pagar una tarifa, un “depósito de gas” o un impuesto a una dirección específica antes de que se pueda liberar.

**Ejemplo:** Un mensaje dice que tu billetera cumple los requisitos para un gran airdrop y te pide que envíes una pequeña cantidad de ETH para activar la reclamación.

### Señales de alerta

- Una tarifa pagada a una dirección en lugar de una comisión de red normal por una transacción que envías tú mismo.
- Una elegibilidad que nunca solicitaste.

### Cómo evitarlo

- Reclamar un airdrop real solo cuesta la comisión de red de tu propia transacción para reclamarlo.
- Nunca envíes fondos a una dirección para desbloquear una recompensa.

## 4. Airdrops que recopilan datos

Formularios que piden datos personales, documentos de identidad, datos de la billetera o la frase semilla (frase de recuperación) para “registrarte” en un airdrop.

**Ejemplo:** Un formulario de registro para un próximo airdrop te pide tu correo electrónico, tu número de teléfono, una foto de tu documento de identidad y la frase semilla de tu billetera “para verificar la propiedad”.

### Señales de alerta

- Cualquier solicitud de tu frase semilla.
- Documentos de identidad a cambio de una recompensa gratuita.

### Cómo evitarlo

- Nunca le des tu frase semilla a nadie.
- Comparte datos personales solo con servicios que hayas verificado.

## 5. Regalos falsos de NFT y tokens

Entregas gratuitas de NFT o tokens que llevan a páginas para hacer mint o reclamar con aprobaciones ocultas, a menudo promocionadas después de que hackean la cuenta de redes sociales de un proyecto.

**Ejemplo:** La cuenta hackeada de un proyecto anuncia un mint gratuito sorpresa para los poseedores leales.

### Señales de alerta

- Entregas sorpresa con urgencia.
- Anuncios que aparecen en un solo canal.

### Cómo evitarlo

- Comprueba los anuncios en el sitio web del proyecto y en varios canales oficiales.
- Haz mint y reclama solo desde una billetera Desechable.

| Tipo | Lo que te piden hacer | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Envía para recibir | Enviar cripto primero | Promesa de devolver más | Nunca envíes para recibir |
| Sitio falso para reclamar | Conectar y aprobar o firmar | Aprobación sin relación con el airdrop | Canales oficiales, billetera Desechable |
| Pagar para reclamar | Pagar una tarifa a una dirección | Tarifa en lugar del gas normal | Nunca pagues para desbloquear recompensas |
| Recopilación de datos | Completar un formulario | Se pide la frase semilla o un documento de identidad | Nunca compartas la frase semilla |
| Entrega falsa de NFT o tokens | Hacer mint o reclamar | Entrega sorpresa desde un solo canal | Verifica en varios canales |

*Tabla 7.1: Estafas de regalos y airdrops que debes conocer*

## 7.2 Tokens inesperados en tu billetera

Los estafadores envían tokens a muchas billeteras a la vez. El nombre del token a menudo contiene la dirección de un sitio web o dice algo como “reclama tu recompensa”. El objetivo es que visites el sitio o que intentes hacer un swap (intercambio de tokens) o vender el token, lo que puede activar una aprobación maliciosa.

| Lo que haces | Riesgo |
|---|---|
| Ver el token en tu billetera | Ninguno. Recibir un token no le da a nadie acceso a tu billetera. |
| Ocultarlo en la app de tu billetera | Ninguno. Ocultarlo es un ajuste de visualización. |
| Visitar el sitio web que aparece en su nombre | Alto. Suele ser una página para reclamar o de un drainer. |
| Intentar venderlo, hacer un swap o transferirlo | Posible aprobación o firma para un contrato malicioso. No interactúes con él. |

*Tabla 7.2: Tokens inesperados: qué es seguro y qué no*

## 7.3 Escenario ilustrativo: el token con un sitio web en su nombre

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

Chris ve un token nuevo en su billetera que, según la billetera, vale varios miles de dólares. Su nombre incluye una dirección web y las palabras “claim reward”. Visita el sitio, que le explica que es uno de los pocos poseedores seleccionados para un bono.

El sitio le pide que conecte su billetera y apruebe el token para “activar” la recompensa. Él aprueba. En cuestión de minutos, sus stablecoins salen de su billetera.

### Qué pasó

El token era un cebo con un valor falso. La aprobación que dio no era para el token cebo, sino para sus stablecoins, que el drainer movió de inmediato.

**Puntos clave**

- Los tokens inesperados con sitios web en su nombre son anuncios de drainers.
- Un valor mostrado no significa nada para un token que no compraste.
- Ocultar el token habría sido completamente seguro.

## 7.4 Cómo protegerte

1. **Nunca envíes cripto para recibir cripto.**
2. **Busca los airdrops tú mismo**, en el sitio web del proyecto y en sus canales principales, nunca a través de enlaces en respuestas, anuncios o mensajes.
3. **Reclama desde una billetera Desechable** que no contenga nada más y luego mueve lo que recibas.
4. **Revisa cada aprobación y cada firma**: qué token, cuánto y para qué contrato.
5. **Cuenta con que reclamar un airdrop real solo cuesta comisiones de red** por la transacción que envías tú mismo.
6. **Oculta los tokens inesperados** y no interactúes con ellos.

## 7.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-005

### Nunca conectes tu billetera a sitios web desconocidos.

Busca los airdrops en los canales oficiales del proyecto y reclámalos desde una billetera Desechable.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-002 | Nunca envíes cripto para recibir cripto | La base de toda estafa de regalos falsos. |

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| GR-008 | Guarda tus fondos a largo plazo en una billetera bóveda. Usa otra billetera para DApps, trading y Web3 | Una billetera Desechable limita lo que puede llevarse una página falsa para reclamar tokens. |
| GR-004 | Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos | Cuando termines, revoca las aprobaciones que diste para reclamar. |

*Tabla 7.3: Reglas CSF complementarias*

## 7.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: solo visto, aprobado, firmado, frase semilla expuesta, dinero enviado a un estafador. Luego añade los pasos para tu situación:

| Si tú… | Haz esto ahora |
|---|---|
| enviaste cripto por un regalo falso | Detente. No volverá, y enviar más no servirá de nada. Denuncia la publicación o la transmisión. |
| aprobaste o firmaste en un sitio para reclamar tokens | Sigue las filas de aprobar o firmar: revoca y mueve los activos restantes si ya empezaron las transferencias. |
| pagaste una comisión para reclamar o por elegibilidad | Deja de pagar. Guarda la dirección y denúnciala. |
| compartiste tu frase semilla en un formulario | Considera la billetera comprometida. Sigue ahora la fila de la frase semilla. |
| solo recibiste o viste un token inesperado | No hay nada comprometido. Ocúltalo y no interactúes con él. |

*Tabla 7.4: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/airdrop-scams-crypto-web3/

CAPÍTULO 8

# Plataformas de inversión falsas

*“Los depósitos generan confianza. Los retiros revelan la verdad.”*

*Figura 8.1: Plataformas de inversión falsas de un vistazo*

Una plataforma de inversión falsa parece un exchange (plataforma de intercambio) real, una app de trading, un servicio de minería o un programa de staking. Depositas, tu saldo crece en la pantalla e incluso los primeros retiros pequeños pueden funcionar. Cuando intentas sacar una cantidad mayor, la plataforma inventa un motivo por el que primero debes pagar: un impuesto, una comisión, un “depósito de verificación”, un saldo mínimo. Cada pago lleva a la siguiente exigencia.

En la colección de incidentes de CSF, esta es una de las categorías de estafa más grandes. Las víctimas suelen llegar a través de otra persona: un contacto romántico (Capítulo 10), una oferta de empleo o de tareas (Capítulo 11), un grupo de inversión o un anuncio. Este capítulo trata de la plataforma en sí y de la regla que la deja en evidencia: **una plataforma legítima nunca te pide que pagues para poder retirar.**

EN ESTE CAPÍTULO


- 8.1 Plataformas de inversión falsas que debes conocer
- 8.2 La trampa del retiro
- 8.3 Señales que no son prueba
- 8.4 Escenario ilustrativo: la cuenta rentable
- 8.5 Cómo protegerte
- 8.6 Reglas CSF de este capítulo
- 8.7 Si esto te acaba de pasar


# 8.1 Plataformas de inversión falsas que debes conocer

## 1. Exchanges y apps de trading falsos

Un sitio web o una app que parece un exchange o una plataforma de trading profesional, a menudo con gráficos que parecen en vivo, una app para descargar y un chat de soporte. Los precios y los saldos son simulados.

**Ejemplo:** Una app de “trading con IA” recomendada en un grupo de inversión muestra ganancias diarias de operaciones automatizadas. La app no figura en el registro de ningún regulador.

### Señales de alerta

- Una plataforma de la que supiste por un contacto, un grupo o un anuncio, no por tu propia investigación.
- Rendimientos inusualmente altos o constantes.
- Una app instalada desde un enlace en lugar de desde una tienda oficial.

### Cómo evitarlo

- Consulta la plataforma en el registro y en las listas de advertencias de tu regulador financiero antes de depositar.
- Desconfía de las plataformas que solo aceptan depósitos en cripto.
- Busca el nombre de la plataforma junto con “scam” (estafa) y “withdrawal” (retiro).

## 2. Esquemas de minería, staking y “rendimiento”

Servicios que prometen rendimientos diarios fijos por minería en la nube, staking, liquidez o “arbitraje”. Muchos son esquemas Ponzi que pagan a los primeros usuarios con los depósitos de los usuarios posteriores hasta que colapsan.

**Ejemplo:** Un sitio de minería en la nube ofrece un 2% diario garantizado sobre cualquier depósito, con niveles “VIP” más altos para cantidades mayores.

### Señales de alerta

- Rendimientos fijos o garantizados.
- Niveles de bonificación por depositar más o traer amigos.
- Explicaciones vagas sobre de dónde sale la ganancia.

### Cómo evitarlo

- Considera los rendimientos garantizados una señal de estafa.
- Pregunta cómo se genera la ganancia; si nadie puede explicarlo, aléjate.
- Nunca persigas niveles “VIP” con depósitos más grandes.

## 3. Grupos de copy trading y de señales con una plataforma

Grupos en apps de mensajería dirigidos por un “mentor” o “profesor” que comparte operaciones ganadoras y recomienda una plataforma concreta para seguirlas. Los miembros del grupo que elogian sus ganancias a menudo forman parte de la estafa.

**Ejemplo:** Un grupo en una app de mensajería comparte señales diarias. El asistente les dice a los nuevos miembros que abran una cuenta en una plataforma asociada para copiar las operaciones.

### Señales de alerta

- Un mentor que te envía a una plataforma en particular.
- Muchos miembros entusiastas publicando capturas de pantalla.
- Presión para depositar antes de una “gran señal”.

### Cómo evitarlo

- Usa solo plataformas que hayas elegido y verificado tú mismo.
- Trata las capturas de pantalla como marketing, no como prueba.
- Sal de los grupos que promueven una plataforma concreta.

| Tipo | Lo que ves | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Exchange o app de trading falsos | Sitio profesional, saldo creciente | No figura en el registro de ningún regulador | Consulta primero los registros y las advertencias |
| Minería, staking, rendimiento | Rendimientos diarios fijos | Ganancia garantizada | Pregunta cómo se genera la ganancia |
| Grupo de señales con una plataforma | Mentor y miembros contentos | Te dirigen a una sola plataforma | Elige las plataformas tú mismo |

*Tabla 8.1: Plataformas de inversión falsas que debes conocer*

## 8.2 La trampa del retiro

Casi todas las plataformas falsas terminan igual. Cuando pides retirar, aparece un nuevo obstáculo:

- un “impuesto” o una “tasa sobre ganancias de capital” que hay que pagar primero;
- un depósito de “verificación” o “contra el lavado de dinero”;
- un saldo mínimo, una “puntuación de crédito” o un nivel de cuenta que no has alcanzado;
- una cuenta congelada que un “departamento de riesgos” desbloqueará a cambio de una comisión;
- penalizaciones por “operaciones irregulares”.

LA REGLA DEL RETIRO

**Si una plataforma te pide que pagues antes de poder retirar, considérala una estafa y detente.** Las plataformas legítimas descuentan sus comisiones de tu saldo; no necesitan dinero nuevo para liberar el tuyo. Pagar casi nunca libera los fondos. Lleva a la siguiente exigencia, y el saldo en la pantalla puede que ni siquiera exista.

## 8.3 Señales que no son prueba

Las plataformas falsas invierten en parecer de confianza. Nada de lo siguiente prueba que una plataforma sea legítima:

| Señal | Por qué no es prueba |
|---|---|
| Funcionó un pequeño retiro de prueba | Muchas plataformas falsas permiten pequeños retiros al principio precisamente para generar confianza antes de depósitos más grandes. |
| Un sitio web y una app profesionales | Las plantillas y los creadores de apps hacen que producir plataformas convincentes sea barato. |
| Documentos de registro de la empresa | El registro de una empresa no es una licencia, y los documentos se pueden falsificar. |
| Reseñas, testimonios y redes sociales | Las reseñas se pueden comprar; los miembros del grupo pueden ser cómplices. |
| Soporte por chat en vivo | El soporte existe para que sigas depositando y para justificar los retrasos. |
| Un número de registro de una autoridad financiera | Un registro contra el lavado de dinero (por ejemplo, un número “MSB” de FinCEN en EE. UU. o de FINTRAC en Canadá) no es una licencia ni un aval: las plataformas falsas a menudo muestran uno. Comprueba si existe una licencia real y revisa la lista de advertencias del regulador. |

*Tabla 8.2: Señales que no son prueba*

Lo que sí ayuda: consultar la plataforma en el registro de proveedores de servicios cripto autorizados de tu regulador financiero nacional (en la UE, el registro de proveedores de servicios de criptoactivos que se lleva conforme al reglamento MiCA) y revisar las listas de advertencias de los reguladores. Incluso un nombre registrado puede ser copiado por un sitio clonado, así que confirma que la dirección web coincide con la que figura en el registro.

## 8.4 Escenario ilustrativo: la cuenta rentable

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

Tom conoce a una persona amable en un grupo de trading en línea. Ella comparte sus resultados en una plataforma que parece un exchange

moderno. Tom deposita una pequeña cantidad, ve ganancias constantes y retira con éxito un poco de beneficio. Animado, deposita sus ahorros.

Un mes después, su saldo muestra más del doble de lo que depositó. Cuando pide retirar, el soporte le dice que primero debe pagar un impuesto del 20%. Después de pagar, su cuenta queda congelada por "actividad inusual", y descongelarla cuesta otra comisión.

### Qué pasó

La plataforma nunca estuvo conectada a ningún mercado. El saldo era un número en una base de datos, y el pequeño retiro inicial se pagó para generar confianza. El "impuesto" y la "comisión de descongelación" fueron las siguientes etapas de la misma estafa.

### Conclusiones clave

- Un pequeño retiro exitoso no prueba que la plataforma sea real.
- La primera exigencia de pagar antes de retirar es el momento de detenerte.
- El contacto que te presentó la plataforma suele formar parte del esquema.

## 8.5 Cómo protegerte

1. **Elige las plataformas tú mismo.** Nunca uses un exchange ni una app de inversión que te haya recomendado alguien que conociste en línea.
2. **Consulta el registro del regulador** y las listas de advertencias antes de depositar, y confirma que la dirección web coincide.
3. **Aplica la regla del retiro.** Cualquier exigencia de pagar antes de poder retirar pone fin a la relación.
4. **Desconfía de los rendimientos garantizados.** Las inversiones reales suben y bajan.
5. **No persigas las pérdidas.** Pagar más para recuperar dinero ya depositado es lo que multiplica las pérdidas.
6. **Habla con alguien de confianza** antes de hacer depósitos grandes. Los estafadores aíslan; una segunda opinión rompe el hechizo.

## 8.6 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-003

**Nunca pagues para desbloquear o retirar fondos.**

Si una plataforma te pide una comisión, un impuesto o un depósito antes de poder retirar, detente y denúncialo.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-007 | Verifica los proyectos antes de invertir | Las comprobaciones en el registro del regulador y en las listas de advertencias van antes de cualquier depósito. |
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | A la mayoría de las víctimas las lleva a la plataforma alguien que las contactó. |
| SDR-006 | Desconfía de la urgencia, la euforia y las ganancias garantizadas | Los rendimientos garantizados y las “grandes señales” son el anzuelo. |

*Tabla 8.3: Reglas CSF de apoyo*

## 8.7 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: una plataforma dice que debes pagar antes de poder retirar, enviaste dinero o cripto a un estafador. Luego añade los pasos para tu situación:

| Si tú… | Haz esto ahora |
|---|---|
| te piden pagar antes de retirar | Deja de pagar y deja de depositar. No le digas a la plataforma que sospechas una estafa; primero guarda todo. |
| depositaste a través de un exchange | Contacta con ese exchange y dale los hashes de las transacciones y la dirección de la plataforma. Es posible que pueda marcar o congelar los fondos que aún estén bajo su control. |

| Si tú… | Haz esto ahora |
|---|---|
| pagaste por transferencia bancaria o con tarjeta | Contacta con tu banco de inmediato y pregunta si es posible recuperar el pago. |
| instalaste la app de la plataforma | Desinstálala. Si se instaló fuera de una tienda de apps oficial, sigue la fila de malware. |
| compartiste documentos de identidad para el "KYC" | Vigila el uso indebido de tu identidad. Denuncia la pérdida de los documentos si tu país ofrece esa opción y plantéate activar una alerta de crédito o de identidad. |

*Tabla 8.4: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/crypto-exchange-scams/

CAPÍTULO 9

# Estafas con tokens

*“La euforia no es diligencia debida.”*

*Figura 9.1: Estafas con tokens de un vistazo*

En una estafa con tokens, lo que compras es la trampa. El token puede ser un lanzamiento o una preventa que nunca cumple, una moneda inflada por personas internas que venden mientras otros compran, un proyecto cuyos creadores retiran la liquidez o un contrato que te deja comprar pero nunca vender. En todos los casos, las personas detrás del token controlan algo que los compradores no controlan: la oferta, la liquidez, el contrato o la promoción.

Este capítulo reúne tres capítulos anteriores (lanzamientos de tokens, pump and dump, rug pulls) porque las víctimas los viven de la misma manera: compran por la euforia y se quedan con un token que vale poco o que no se puede vender. Las plataformas falsas que solo te muestran un saldo se tratan en el Capítulo 8.

EN ESTE CAPÍTULO


- 9.1 Estafas con tokens que debes conocer
- 9.2 Señales que no son prueba
- 9.3 Escenario ilustrativo: la memecoin de la comunidad
- 9.4 Cómo protegerte
- 9.5 Reglas CSF de este capítulo
- 9.6 Si esto te acaba de pasar


# 9.1 Estafas con tokens que debes conocer

## 1. Lanzamientos y preventas falsos

Un token nuevo se vende antes del lanzamiento mediante una preventa, una lista blanca o una ronda de “acceso anticipado”. El equipo recauda el dinero y el token nunca se lanza, o se lanza con la mayor parte de la oferta en manos de personas internas.

**Ejemplo:** Una preventa promocionada en un grupo de chat promete un precio de lanzamiento fijo y una cotización en pocas semanas. Cuando se agota, el sitio web y las cuentas del equipo dejan de dar señales de vida.

### Señales de alerta

- Equipos anónimos y planes vagos.
- Presión para comprar antes de una fecha límite o de una subida de precio.
- Preventas pagadas a una dirección de billetera personal.

### Cómo evitarlo

- Trata las preventas como especulación de alto riesgo, no como inversiones.
- Nunca envíes fondos a una dirección publicada en un chat.
- Da por hecho que puedes perder todo lo que pongas en una preventa.

## 2. Pump and dump

Los organizadores compran un token de precio bajo y luego lo promocionan a través de grupos, influencers o bots. Cuando la gente de

fuera entra en masa y el precio sube, los organizadores venden y el precio se desploma.

**Ejemplo:** Un grupo de chat grande anuncia la “próxima moneda 100x” a una hora fijada. En cuestión de minutos el precio se triplica y luego cae por debajo de donde empezó.

#### Señales de alerta

- Convocatorias coordinadas para comprar a una hora fijada.
- Influencers que promocionan tokens que tienen sin decirlo.
- Subidas repentinas de precio sin ninguna noticia detrás.

#### Cómo evitarlo

- No compres porque un grupo o un influencer diga que es el momento.
- Pregúntate quién te está vendiendo cuando todos están comprando.
- Revisa la actividad de trading en un explorador de bloques o en un sitio de datos de mercado antes de comprar.

### 3. Rug pulls

Los creadores retiran la liquidez que permite negociar el token, emiten tokens nuevos para venderlos o simplemente abandonan el proyecto después de recaudar fondos. Los tenedores se quedan con tokens que no pueden vender a ningún precio significativo.

**Ejemplo:** Un proyecto DeFi con altos rendimientos anunciados atrae depósitos. De la noche a la mañana, los creadores retiran la liquidez y eliminan sus cuentas en redes sociales.

#### Señales de alerta

- Liquidez que no está bloqueada, o que solo está bloqueada por poco tiempo.
- Unas pocas billeteras que tienen la mayor parte de la oferta.
- Contratos que permiten al propietario emitir tokens o cambiar las comisiones.

#### Cómo evitarlo

- Revisa la distribución de tenedores y la liquidez antes de comprar.
- Evita los tokens cuyo propietario puede emitir tokens o cambiar las reglas a voluntad.
- Pon en cualquier posición solo dinero que puedas permitirte perder.

## 4. Tokens honeypot

El contrato del token permite comprar, pero bloquea la venta o la grava con impuestos muy altos para todos excepto los creadores. El gráfico de precios parece sano porque nadie más puede vender.

**Ejemplo:** Un token sube de forma constante con muchos compradores y casi ninguna venta. Cuando intentas vender, la transacción falla o casi todo el importe se pierde en una comisión oculta.

### Señales de alerta

- Muchas compras y casi ninguna venta.
- Impuestos de venta inusuales o transacciones de venta fallidas de las que informan otras personas.
- Código del contrato no verificado o modificado recientemente.

### Cómo evitarlo

- Comprueba si otros tenedores han podido vender.
- Usa una herramienta de verificación de tokens como una señal, no como prueba.
- Evita los tokens que no puedas verificar.

## 5. Migraciones y swaps (intercambio de tokens) falsos

A los tenedores de un token real se les dice que está migrando a un nuevo contrato, o que deben hacer el swap a través de un sitio especial. El sitio de “migración” obtiene aprobaciones o se lleva los propios tokens.

**Ejemplo:** Un mensaje en la comunidad de un proyecto dice que el token se está actualizando y que los tenedores deben hacer el swap a través de un enlace en un plazo de 48 horas.

### Señales de alerta

- Plazos para migraciones anunciados solo en chats o en respuestas.
- Sitios de swap que no están enlazados desde el sitio web del proyecto.

### Cómo evitarlo

- Confirma las migraciones en el sitio web del proyecto y en varios canales oficiales.
- Nunca hagas una migración con prisas; las reales dan tiempo.

| Tipo | Cómo pierdes | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Lanzamiento o preventa falsos | El token nunca se entrega | Preventa a una dirección personal | Trátalo como especulación; cantidades pequeñas |
| Pump and dump | Compras caro mientras las personas internas venden | Convocatorias coordinadas para comprar | Nunca compres por una señal |
| Rug pull | Liquidez retirada o diluida por emisión | Liquidez no bloqueada, pocos tenedores | Revisa los tenedores y los poderes del contrato |
| Honeypot | No puedes vender | Hay compras, pero no ventas | Comprueba que otros puedan vender |
| Migración falsa | Se llevan aprobaciones o tokens | Plazo en un chat | Confirma en los canales oficiales |

*Tabla 9.1: Estafas con tokens que debes conocer*

## 9.2 Señales que no son prueba

Los tokens fraudulentos invierten mucho en parecer dignos de confianza. Nada de lo siguiente prueba que un token sea seguro:

| Señal | Por qué no es prueba |
|---|---|
| Una auditoría | Las auditorías pueden ser falsas, estar desactualizadas, tener un alcance limitado o ignorar las partes que importan. Una auditoría no impide que un equipo venda o retire la liquidez. |
| Liquidez bloqueada | Los bloqueos pueden ser cortos, parciales o estar en otro pool. Comprueba qué está bloqueado, cuánto y hasta cuándo. |

| Señal | Por qué no es prueba |
|---|---|
| Una cotización en un rastreador o en un exchange (plataforma de intercambio) | Muchos rastreadores listan tokens automáticamente. Una cotización no dice nada sobre las intenciones del equipo. |
| Un equipo con identidad pública (doxxed) o con “KYC” | Las verificaciones de identidad de terceros varían mucho en calidad, y las personas identificadas pueden desaparecer igualmente. |
| Seguidores, tenedores y tamaño de la comunidad | Los seguidores, los tenedores y la interacción se pueden comprar o generar artificialmente. |
| Apoyo de influencers | Los promotores a menudo cobran por ello o tienen el token ellos mismos. |

*Tabla 9.2: Señales que no son prueba*

## 9.3 Escenario ilustrativo: la memecoin de la comunidad

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

Una memecoin nueva se lanza con una mascota graciosa y una gran comunidad en línea. A los pocos minutos del lanzamiento, el valor de mercado sube rápido y las publicaciones sobre “la próxima gran moneda” se difunden por las redes sociales. Jamie compra después del primer gran salto.

Durante la hora siguiente el precio oscila y luego cae más del 80% cuando varias billeteras grandes venden. Las cuentas del proyecto dicen que todo está bien. Días después, los datos on-chain muestran que un puñado de billeteras compró la mayor parte de la oferta en los primeros segundos tras el lanzamiento.

### Qué pasó

Personas internas o snipers compraron temprano y vendieron aprovechando la ola de compradores que atrajo la euforia. Jamie, como la mayoría de los compradores, llegó después de quienes planearon la salida.

### Conclusiones clave

- Cuando un token está en todas partes, los primeros compradores normalmente ya están vendiendo.
- Revisa la distribución de tenedores antes de comprar, no después.
- Las memecoins son un riesgo que debes tratar como un gasto en entretenimiento. Nunca uses dinero que necesites.

## 9.4 Cómo protegerte

1. **Averigua quién tiene la oferta.** Si unas pocas billeteras tienen la mayor parte, ellas deciden el precio.
2. **Revisa lo que permite el contrato.** ¿Puede el propietario emitir tokens, cambiar las comisiones o bloquear las ventas? Si no puedes saberlo, no compres.
3. **Revisa la liquidez.** ¿Cuánta hay, está bloqueada y hasta cuándo?
4. **No compres por una señal de compra.** Las llamadas coordinadas a comprar existen para que quienes están dentro del proyecto tengan a quién vender.
5. **Trata las auditorías, los listados y los seguidores como señales, no como pruebas.**
6. **Usa una billetera Desechable o de Uso Frecuente** para tokens nuevos, nunca tu billetera Bóveda, y revoca las aprobaciones después. La separación de billeteras limita los riesgos de las aprobaciones, pero no puede proteger el dinero que tú decides invertir.

## 9.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-007

**Verifica los proyectos antes de invertir.**

Comprueba quién tiene el suministro y si la liquidez está bloqueada. Las auditorías, los listados y los seguidores son señales, no pruebas.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-006 | Desconfía de la urgencia, la euforia y las ganancias garantizadas | Las estafas con tokens encuentran compradores gracias a la euforia y los plazos. |
| SDR-008 | Nunca confíes en la popularidad en redes sociales | Los seguidores, los holders y las publicaciones de influencers se pueden fabricar. |

*Tabla 9.3: Reglas CSF complementarias*

## 9.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: aprobaste, enviaste dinero a un estafador, la plataforma dice que pagues antes de retirar. Luego añade los pasos para tu situación:

| Si tú… | Haz esto ahora |
|---|---|
| tienes un token que se desplomó o que no se puede vender | No compres más para “promediar a la baja” y no pagues a nadie para “desbloquear” la venta. Revoca las aprobaciones que diste al token o a sus sitios. |
| te pidieron pagar una comisión para vender o retirar | Detente. Es la trampa del retiro del Capítulo 8. Guarda los detalles y denúncialo. |
| usaste un sitio de migración o de swap | Sigue las filas de aprobaciones: revoca y mueve los activos restantes si ya empezaron las transferencias. |
| crees que el proyecto era fraudulento | Guarda la dirección del contrato, las publicaciones del proyecto y tus transacciones, y denúncialo a la policía y a las plataformas que lo promocionaron. |

*Tabla 9.4: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/token-launch-scams-crypto-web3/

CAPÍTULO 10

# Estafas románticas

*“La relación es el arma.”*

*Figura 10.1: Estafas románticas de un vistazo*

Las estafas románticas usan una relación personal para manipular a la víctima. Pueden empezar en una app de citas, a través de una amistad en redes sociales o con un mensaje de “número equivocado” que se convierte en una charla amistosa. Durante semanas o meses, el estafador construye confianza y cercanía emocional, y luego introduce el dinero: una emergencia, un regalo o, con mayor frecuencia, una oportunidad de inversión.

La versión de inversión suele llamarse **pig butchering ("matanza del cerdo")**: a la víctima se la “engorda” con atención y pequeñas ganancias iniciales en una plataforma falsa, y luego se la anima a invertirlo todo antes de que la plataforma bloquee los retiros (Capítulo 8). Las estafas románticas causan algunas de las mayores pérdidas individuales, y las víctimas a menudo vuelven a ser blanco de estafas de recuperación (Capítulo 13).

EN ESTE CAPÍTULO


- 10.1 Estafas románticas que debes conocer
- 10.2 Las etapas de una estafa romántica de inversión
- 10.3 Escenario ilustrativo: el número equivocado
- 10.4 Cómo protegerte
- 10.5 Reglas CSF de este capítulo
- 10.6 Si esto te acaba de pasar


# 10.1 Estafas románticas que debes conocer

## 1. Estafas románticas de inversión (pig butchering)

Un nuevo amigo o pareja comparte su éxito haciendo trading con cripto, que a menudo atribuye a un familiar o mentor, y se ofrece a enseñarte. Te guía hacia una plataforma o app concreta, donde tu saldo crece rápido, hasta que intentas retirar.

**Ejemplo:** Un match en una app de citas lleva la conversación a una app de mensajería, habla de la estrategia de trading de su tío y te ayuda a abrir una cuenta en una plataforma de la que nunca has oído hablar.

### Señales de alerta

- Un contacto nuevo que enseguida habla de ganancias con cripto.
- Una plataforma o app concreta que debes usar.
- Pequeños retiros iniciales que funcionan, seguidos de presión para invertir más.

### Cómo evitarlo

- Nunca inviertas en una plataforma sugerida por alguien a quien solo conoces en línea.
- Mantén el dinero y el romance separados, siempre.
- Aplica la regla del retiro: si tienes que pagar para retirar, es una estafa.

## 2. Peticiones de emergencia y de regalos

Después de crear cercanía, al estafador le surge un problema repentino: una factura médica, una cuenta bloqueada, gastos de viaje, tasas de aduana por un regalo que te envió. Pide cripto porque es “más rápido”.

**Ejemplo:** Una pareja a la que nunca has visto en persona está atrapada en un aeropuerto y necesita cripto para pagar una multa antes de poder viajar a verte.

### Señales de alerta

- Emergencias que solo el dinero puede resolver, una y otra vez.
- Peticiones de cripto o tarjetas de regalo.
- Motivos por los que no puede hacer una videollamada ni verte en persona.

### Cómo evitarlo

- No envíes dinero a alguien a quien no has visto en persona.
- Habla con un amigo o familiar antes de enviar nada.

## 3. Acercamientos de “número equivocado” y de amistad

Llega un mensaje “por error”, o un desconocido inicia una conversación amistosa en redes sociales. La cortesía se convierte en charlas habituales, luego en amistad, mentoría o romance y, finalmente, en cripto.

**Ejemplo:** Un mensaje de texto dirigido a otra persona se disculpa por el error y luego continúa: “Ya que estamos hablando…”

### Señales de alerta

- Un desconocido que sigue la conversación después de un error.
- Fotos atractivas, un estilo de vida exitoso y mucho tiempo libre.
- Un cambio rápido de una app a otra.

### Cómo evitarlo

- No continúes conversaciones que empiezan por error.
- Haz una búsqueda inversa de las fotos de perfil.
- Desconfía de cualquiera que lleve rápido la conversación a una app privada.

## 4. Identidades falsas y catfishing

Los estafadores usan fotos robadas, historias de vida inventadas y, cada vez más, imágenes y videos generados con IA para parecer reales. Algunos aceptan videollamadas cortas usando herramientas de intercambio de rostros.

**Ejemplo:** Una pareja por fin acepta una videollamada. La imagen está borrosa, la llamada es corta y, después, las peticiones de dinero continúan.

### Señales de alerta

- Perfiles con pocas conexiones reales o poca actividad reciente.
- Videollamadas que siempre son cortas, oscuras o “fallan”.
- Historias que cambian cuando haces preguntas.

### Cómo evitarlo

- Haz una búsqueda inversa de las fotos y busca incoherencias.
- Recuerda que una videollamada ya no es prueba de identidad.
- Pide a alguien de confianza que revise el perfil contigo.

| Tipo | Cómo se pide el dinero | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Inversión romántica | Invertir en su plataforma | Una plataforma que debes usar | Nunca inviertas a través de un contacto en línea |
| Emergencia o regalo | Ayuda urgente o tasas | Emergencias de dinero repetidas | Nunca envíes dinero sin haberla visto en persona |
| Número equivocado o amistad | Más adelante, a través de la mentoría | La conversación continúa después de un error | No continúes esas conversaciones |
| Identidad falsa | Cualquiera de los anteriores | Videollamadas cortas o de mala calidad | Haz una búsqueda inversa; pide ayuda a alguien de confianza |

*Tabla 10.1: Estafas románticas que debes conocer*

## 10.2 Las etapas de una estafa romántica de inversión

| Etapa | Qué pasa | Qué puedes notar |
|---|---|---|
| 1. Contacto | Match en una app de citas, mensaje en redes sociales o mensaje de texto de número equivocado. | Un desconocido con un interés inusual en seguir hablando. |
| 2. Cercanía | Mensajes diarios, planes compartidos, halagos, paso a una app privada. | Velocidad: intimidad en cuestión de días o semanas. |
| 3. Presentación | Habla de éxito en el trading, de un familiar o mentor con un sistema. | El dinero entra en una relación personal. |
| 4. Pequeñas ganancias | Abres una cuenta en su plataforma; los depósitos pequeños crecen y un retiro pequeño funciona. | La plataforma vino de esa persona, no de tu investigación. |
| 5. Gran empujón | Una oportunidad especial, un plazo, ánimos para pedir dinero prestado o vender activos. | Presión para invertir más de lo que habías planeado. |
| 6. Bloqueo | Retiros bloqueados por impuestos, comisiones o cuentas “congeladas”; la pareja te insiste en que pagues. | Pagar para retirar: la estafa ya es segura. |
| 7. Nuevo ataque | Servicios de “recuperación” o supuestas autoridades se ofrecen a recuperar tu dinero a cambio de una comisión. | Capítulo 13: una segunda estafa. |

*Tabla 10.2: Etapas de una estafa romántica de inversión*

## 10.3 Escenario ilustrativo: el número equivocado

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

Daniel recibe un mensaje amistoso dirigido a otra persona. Responde con cortesía, y la remitente, que dice trabajar en finanzas, sigue conversando. Durante las semanas siguientes hablan todos los días. Ella menciona que su tío tiene una estrategia de trading que le ha dado

una vida cómoda a su familia y se ofrece a mostrarle a Daniel cómo funciona.

Ella lo ayuda a abrir una cuenta en una plataforma de aspecto profesional. Su primer depósito pequeño crece rápido, y un pequeño retiro llega a su billetera. Animado, invierte la mayor parte de sus ahorros. Cuando intenta retirar, le dicen que primero debe pagar un impuesto sobre sus ganancias. Ella le insiste en que lo pague y se ofrece a prestarle parte del importe.

### Qué pasó

El contacto, la plataforma y el "impuesto" formaban parte de una misma operación. El retiro inicial se pagó para generar confianza, y la oferta de ayudarlo con el impuesto estaba pensada para que pagara.

### Conclusiones clave

- El dinero y las nuevas relaciones en línea no se mezclan.
- Un pequeño retiro que funciona es parte del guion.
- Que la pareja insista en que pagues la comisión es la prueba más clara de la estafa.

## 10.4 Cómo protegerte

1. **Nunca inviertas, hagas trading ni envíes cripto porque te lo sugiera alguien a quien conociste en línea.**
2. **Nunca uses una plataforma o app elegida por un contacto en línea.** Usa solo servicios que hayas encontrado y verificado tú mismo (Capítulo 8).
3. **No continúes conversaciones de "número equivocado".**
4. **Haz una búsqueda inversa de las fotos** y recuerda que el video se puede falsificar.
5. **Habla con alguien de confianza** antes de enviar dinero. Los estafadores se esfuerzan por aislarte; una segunda opinión rompe ese aislamiento.
6. **Después de una pérdida, es probable que recibas ofertas de recuperación**; no les hagas caso (Capítulo 13).

## 10.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-006

**Desconfía de la urgencia, la euforia y las ganancias garantizadas.**

Nunca envíes cripto ni inviertas en una plataforma sugerida por alguien a quien solo conoces en línea.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | Toda estafa romántica empieza con un contacto que no buscaste. |
| SDR-004 | Verifica las identidades fuera del canal del mensaje | Una persona real puede verificarse fuera del chat; un estafador lo evita. |
| SDR-003 | Nunca pagues para desbloquear o retirar fondos | La etapa de bloqueo depende de que pagues para retirar. |

*Tabla 10.3: Reglas CSF complementarias*

## 10.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: enviaste dinero o cripto a un estafador, una plataforma dice que debes pagar antes de poder retirar, alguien se ofrece a recuperar tus pérdidas. Luego añade los pasos para tu situación:

| Si… | Haz esto ahora |
|---|---|
| te piden pagar antes de poder retirar | Deja de pagar y deja de depositar. No confrontes todavía al contacto; primero guarda los chats, los perfiles, las direcciones de la plataforma y los hashes de las transacciones. |
| enviaste cripto a través de un exchange | Contacta con ese exchange y facilítale los hashes de las transacciones y las direcciones de depósito de la plataforma. |

| Si… | Haz esto ahora |
|---|---|
| enviaste dinero por transferencia bancaria o con tarjeta | Contacta con tu banco de inmediato. |
| compartiste documentos de identidad o datos personales | Vigila cualquier uso indebido de tu identidad y considera una alerta de identidad si tu país la ofrece. |
| sientes vergüenza o te están presionando | No tienes la culpa: estas operaciones las dirigen profesionales. Habla con alguien de confianza y denúncialo a la policía. |

*Tabla 10.4: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/romance-scams-crypto-web3/

CAPÍTULO 11

# Estafas de empleo y tareas

*“La oportunidad puede ser real. El empleador puede no serlo.”*

*Figura 11.1: Estafas de empleo y tareas de un vistazo*

Las estafas de empleo y tareas se dirigen a personas que buscan trabajo o un dinero extra. Algunas usan un empleo falso en cripto o Web3 para que instales malware, compartas tus documentos de identidad o ejecutes acciones en tu billetera. Otras son esquemas de “tareas”: trabajo sencillo en línea, como valorar productos u “optimizar” aplicaciones, donde tus ganancias crecen en pantalla hasta que debes depositar tu propio dinero para desbloquearlas.

El hilo común: **un empleador real nunca te pide que pagues, deposites cripto o instales software desconocido para contratarte o para pagarte.**

EN ESTE CAPÍTULO


- 11.1 Estafas de empleo y tareas que debes conocer
- 11.2 Cómo te atrapan las estafas de tareas
- 11.3 Escenario ilustrativo: el trabajo de optimización
- 11.4 Cómo protegerte
- 11.5 Reglas CSF de este capítulo
- 11.6 Si esto te acaba de pasar


# 11.1 Estafas de empleo y tareas que debes conocer

## 1. Esquemas de tareas y de “optimización”

Te ofrecen un trabajo pagado y fácil: dar “me gusta” a publicaciones, valorar productos, “impulsar” aplicaciones o completar series de pedidos. Un panel muestra comisiones. Luego, una “tarea combinada” deja tu cuenta con saldo negativo y debes depositar cripto para continuar y desbloquear tus ganancias.

**Ejemplo:** Un reclutador en una aplicación de mensajería ofrece un pago diario por 30 minutos de “optimización” de aplicaciones. Tras unos días, una tarea especial requiere un depósito para completarse.

### Señales de alerta

- Un pago por simples clics que parece demasiado generoso.
- Ganancias que solo puedes ver en un panel.
- Depósitos necesarios para continuar o para retirar.

### Cómo evitarlo

- Nunca deposites dinero para ganar dinero.
- Desconfía de cualquier trabajo que se pague a través del panel de una plataforma.
- Aplica la regla de retiro del Capítulo 8.

## 2. Reclutadores falsos y entrevistas con malware

Reclutadores para puestos en cripto o Web3 te piden completar una prueba de programación desde un repositorio, instalar una “aplicación de reuniones” o probar un juego o producto durante la entrevista. El software roba billeteras, contraseñas y datos de sesión.

**Ejemplo:** Un reclutador de una startup Web3 programa una llamada y te pide instalar una aplicación de videollamadas desde un enlace que te envía, porque la habitual “no funciona” en su región.

### Señales de alerta

- Software que debes instalar como parte del proceso de contratación.
- Pruebas de programación que deben ejecutarse en tu propio equipo.
- Entrevistas en plataformas inusuales enviadas por enlace.

### Cómo evitarlo

- Nunca ejecutes código de prueba ni instales software en un dispositivo que contenga cripto.
- Usa aplicaciones de reuniones estándar de las tiendas oficiales.
- Ejecuta cualquier prueba de programación en un entorno aislado, o recházala.

## 3. Empleos con pago por adelantado

Te contratan y luego te piden pagar formación, equipo, un visado de trabajo, una verificación de antecedentes o un “paquete inicial”, a menudo en cripto, con la promesa de un reembolso.

**Ejemplo:** Un nuevo empleador te pide comprar un equipo portátil de trabajo a su proveedor preferido con cripto y promete reembolsarte el dinero con tu primer salario.

### Señales de alerta

- Pagar al empleador antes de recibir un pago.
- Equipo comprado a través de su proveedor.

### Cómo evitarlo

- Los empleadores reales te pagan a ti; tú no les pagas a ellos.
- No compres equipo ni formación a través de un enlace del empleador.

## 4. Recolección de identidades y puestos de procesamiento de pagos

Las solicitudes de empleo falsas recopilan documentos de identidad, datos bancarios y selfies. Algunos “empleos” te piden recibir dinero o cripto y reenviarlo, lo que puede convertirte en parte de un esquema de lavado de dinero.

**Ejemplo:** Un puesto de “agente de pagos” paga una comisión por recibir transferencias en tu cuenta y reenviarlas como cripto.

### Señales de alerta

- Solicitudes de documentos de identidad y datos bancarios antes de cualquier entrevista.
- Empleos que implican mover el dinero de otras personas.

### Cómo evitarlo

- Comparte documentos de identidad solo después de verificar al empleador.
- Nunca recibas ni reenvíes dinero por cuenta de otros. Puede tener consecuencias legales para ti.

| Tipo | Lo que te piden hacer | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Tareas u optimización | Depositar para desbloquear ganancias | Ganancias solo en un panel | Nunca deposites para ganar |
| Reclutador falso con malware | Instalar software o ejecutar código | Software en el proceso de contratación | Nunca en un dispositivo con cripto |
| Empleo con pago por adelantado | Pagar formación o equipo | Pagar al empleador | Los empleadores te pagan a ti |
| Agente de identidad o de pagos | Enviar documentos o mover dinero | Mover el dinero de otras personas | Recházalo; verifica primero al empleador |

*Tabla 11.1: Estafas de empleo y tareas que debes conocer*

## 11.2 Cómo te atrapan las estafas de tareas

1. **Inicio fácil.** Tareas pequeñas y pagos pequeños que realmente llegan, para generar confianza.
2. **Mejora de cuenta.** Comisiones más altas si “mejoras” tu cuenta con un depósito.
3. **Tarea combinada.** Un pedido especial deja tu saldo por debajo de cero; debes depositar para saldarlo.

4. **Bloqueo.** Cada depósito va seguido de otra tarea combinada, una comisión o un problema de “puntuación de crédito”.
5. **Retiro bloqueado.** Las ganancias se quedan en el panel; solo tus depósitos son reales.

Las estafas de tareas son plataformas de inversión falsas (Capítulo 8) disfrazadas de empleo. La misma regla acaba con ellas: nunca pagues para desbloquear o retirar.

## 11.3 Escenario ilustrativo: el trabajo de optimización

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

Un reclutador contacta a Aisha en una aplicación de mensajería y le ofrece trabajo remoto a tiempo parcial: “optimizar” aplicaciones completando series de valoraciones en una plataforma de trabajo. Los primeros días van bien. Completa tareas, ve comisiones y retira una pequeña cantidad.

Luego aparece un “pedido combinado de la suerte” con una comisión más alta, pero deja su saldo en negativo. Para terminarlo, debe depositar cripto. Lo hace, y aparece otro pedido combinado, mayor que el primero. Su supervisor en el chat grupal la anima a seguir para no perder sus ganancias.

### Qué pasó

No había ningún empleo. La plataforma mostraba comisiones inventadas, el pago inicial era un cebo y los pedidos combinados estaban diseñados para exigir depósitos cada vez mayores.

### Lecciones clave

- Un empleo que necesita tu dinero no es un empleo.
- Los primeros pagos reales forman parte del guion.
- Los supervisores y compañeros del chat grupal forman parte de la operación.

## 11.4 Cómo protegerte

1. **Nunca pagues, deposites ni compres nada para conseguir un empleo o para que te paguen.**

2. **Verifica a los reclutadores** a través del sitio web oficial de la empresa y su página de empleo, no a través de los enlaces del propio reclutador.
3. **Mantén separado tu dispositivo cripto.** Nunca instales software de entrevistas ni ejecutes código de prueba en un dispositivo que contenga billeteras.
4. **Desconfía de las ofertas de empleo no solicitadas** en aplicaciones de mensajería, sobre todo si ofrecen un pago alto por poco trabajo.
5. **Comparte documentos de identidad solo** después de haber verificado al empleador y el puesto.
6. **Niégate a mover dinero por cuenta de otros.**

## 11.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-002

### Nunca envíes cripto para recibir cripto.

Los empleadores reales nunca te piden que deposites, pagues una comisión ni compres nada para que te paguen.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-003 | Nunca pagues para desbloquear o retirar fondos | La trampa de la tarea combinada es una trampa de retiro. |
| TSR-001 | Nunca instales software cripto de fuentes no oficiales | El software de entrevistas y el código de prueba son una vía común de malware. |
| TSR-006 | Separa dispositivos y cuentas para el uso de cripto | Un dispositivo separado mantiene el malware de la búsqueda de empleo lejos de tus billeteras. |

*Tabla 11.2: Reglas CSF complementarias*

## 11.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: enviaste dinero o cripto a un

estafador, una plataforma dice que debes pagar antes de poder retirar, instalaste software sospechoso. Luego añade los pasos para tu situación:

| Si tú… | Haz esto ahora |
|---|---|
| depositaste dinero para tareas | Deja de depositar. Guarda la dirección de la plataforma, los chats y las transacciones, y denúncialo. Es probable que recibas ofertas de recuperación. |
| instalaste software o ejecutaste código para una entrevista | Sigue la fila de malware desde otro dispositivo. Considera expuesta cualquier billetera usada en ese dispositivo y mueve los fondos a una billetera nueva creada en un dispositivo limpio. |
| pagaste una tarifa por adelantado | Deja de pagar y denuncia al empleador ante la plataforma de empleo y la policía. |
| compartiste documentos de identidad | Vigila el uso indebido de tu identidad y considera activar una alerta de identidad donde esté disponible. |
| recibiste y reenviaste dinero para alguien | Detente de inmediato, conserva todos los registros y contacta a la policía o a un abogado. |

*Tabla 11.3: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/web3-crypto-job-scams/

CAPÍTULO 12

# Estafas de chantaje y extorsión

*“El miedo es el ataque.”*

*Figura 12.1: Estafas de chantaje y extorsión de un vistazo*

Las estafas de chantaje y extorsión usan el miedo para hacerte pagar. El estafador afirma tener algo que puede hacerte daño: una grabación, tus datos personales, acceso a tus cuentas o el poder de causarte problemas. Exige el pago en cripto porque es rápido y difícil de revertir.

La mayoría de estas amenazas son faroles construidos con datos filtrados, pero algunas no lo son. Este capítulo trata las **amenazas a distancia**: correos electrónicos, mensajes y llamadas. Las amenazas físicas y los ataques contra poseedores de cripto en su casa o en persona se tratan en la guía Hackers.

EN ESTE CAPÍTULO


- 12.1 Estafas de chantaje y extorsión que debes conocer
- 12.2 ¿Farol o real? Qué comprobar
- 12.3 Escenario ilustrativo: la contraseña antigua
- 12.4 Cómo protegerte
- 12.5 Reglas CSF de este capítulo
- 12.6 Si esto te acaba de pasar

# 12.1 Estafas de chantaje y extorsión que debes conocer

## 1. Correos de sextorsión del tipo “hackeé tu dispositivo”

Correos masivos afirman que hackearon tu dispositivo y que tu cámara web te grabó, y exigen cripto para borrar la grabación. Para parecer creíbles, muchos incluyen una contraseña antigua o un número de teléfono procedente de una filtración de datos.

**Ejemplo:** Un correo muestra una contraseña que usaste hace años y exige el pago en 48 horas o el “video” se enviará a tus contactos.

### Señales de alerta

- Una contraseña antigua o un número de teléfono como “prueba”.
- Ninguna prueba real de una grabación.
- Una cuenta regresiva y una dirección de billetera.

### Cómo evitarlo

- No respondas ni pagues. Estos correos se envían a miles de personas.
- Cambia la contraseña filtrada en todos los sitios donde todavía la uses y activa la autenticación de dos factores.

## 2. Sextorsión con imágenes reales

Alguien construye una relación, a menudo haciéndose pasar por un interés romántico, convence a la víctima de compartir imágenes íntimas y luego amenaza con enviarlas a su familia o seguidores si no paga. Esta versión es real y se dirige a adultos y adolescentes.

**Ejemplo:** Un nuevo contacto en línea pide fotos, luego envía una lista de los seguidores de la víctima y exige cripto en menos de una hora.

### Señales de alerta

- Intimidad rápida con un nuevo contacto en línea.
- Un cambio repentino a amenazas y plazos.

### Cómo evitarlo

- No pagues: el pago suele llevar a más exigencias.
- Corta el contacto, conserva las pruebas y denuncia la cuenta ante la plataforma y la policía.

- Si la víctima es menor de 18 años, involucra de inmediato a un adulto de confianza y a la policía; hay servicios especializados que pueden ayudar a eliminar las imágenes.

## 3. Amenazas con datos filtrados y doxxing

Los estafadores usan datos personales de filtraciones, como tu nombre, dirección, número de teléfono o historial de compras con una empresa cripto, para amenazarte con exponerte, acosarte o con “consecuencias” si no pagas.

**Ejemplo:** Un mensaje muestra la dirección de tu casa y la billetera de hardware (hardware wallet) que compraste, dice que se conocen tus fondos y exige un pago para mantener la información en privado.

### Señales de alerta

- Datos personales procedentes de una filtración de datos.
- Amenazas vinculadas a tus fondos en cripto.

### Cómo evitarlo

- No pagues ni negocies. Guarda el mensaje y denúncialo ante la policía.
- Revisa tu seguridad física y mantén tus fondos en privado (consulta la guía Hackers).

## 4. Amenazas legales y de autoridades falsas

Los mensajes afirman que te enfrentas a un arresto, una demanda, sanciones fiscales o la incautación de tu cuenta si no pagas un acuerdo en cripto. Esto se solapa con la suplantación de identidad de autoridades (Capítulo 2).

**Ejemplo:** Un correo que parece una notificación judicial dice que debes pagar un acuerdo en cripto para evitar ser procesado por “trading ilegal”.

### Señales de alerta

- Amenazas legales enviadas por correo electrónico o chat.
- Acuerdos que se pagan en cripto.

### Cómo evitarlo

- Los tribunales y las autoridades no resuelven casos en cripto por correo electrónico.

- Consulta directamente con la autoridad, usando los datos de contacto de su sitio web oficial.

| Tipo | La amenaza | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Correo de “dispositivo hackeado” | Una grabación que no existe | Contraseña antigua como prueba | No respondas; cambia la contraseña |
| Sextorsión con imágenes reales | Compartir imágenes íntimas | Intimidad rápida, luego amenazas | No pagues; denuncia; busca apoyo |
| Datos filtrados y doxxing | Exposición o acoso | Datos filtrados sobre tus criptomonedas | No pagues; denuncia; revisa tu seguridad |
| Amenaza legal falsa | Arresto, demanda, incautación | Acuerdo que se paga en cripto | Verifica con la autoridad real |

*Tabla 12.1: Estafas de chantaje y extorsión que debes conocer*

## 12.2 ¿Farol o real? Qué comprobar

| Pregunta | Si la respuesta es sí |
|---|---|
| ¿El mensaje contiene solo datos que ya se filtraron antes (contraseña antigua, correo, teléfono)? | Muy probablemente es un farol masivo. |
| ¿Hay pruebas concretas y verificables (una imagen real que compartiste, detalles que solo conoce una persona)? | Trátalo como real: no pagues, conserva las pruebas y denúncialo ante la policía. |
| ¿Hay alguna amenaza contra tu seguridad física o tu familia? | Contacta a la policía de inmediato. |
| ¿El remitente ofrece “borrarlo todo” tras un solo pago? | Pagar rara vez pone fin a esto; te marca como alguien que paga. |

*Tabla 12.2: Farol o real: qué comprobar*

## 12.3 Escenario ilustrativo: la contraseña antigua

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

Priya recibe un correo con un asunto que contiene una contraseña que usó hace años. El remitente dice que un malware en su equipo la grabó a través de la cámara web y amenaza con enviar el video a todos sus contactos si no paga en Bitcoin en 48 horas.

Se asusta porque la contraseña es real. En lugar de pagar, busca la primera línea del correo y encuentra a cientos de personas que recibieron el mismo mensaje.

### Qué pasó

La contraseña procedía de una antigua filtración de datos. No había malware ni grabación. El mismo correo se había enviado a miles de direcciones de la misma lista filtrada.

### Conclusiones clave

- Una contraseña antigua real demuestra una filtración de datos, no un dispositivo hackeado.
- Los correos de extorsión masivos se basan en el miedo y en un plazo corto.
- La respuesta correcta es cambiar la contraseña, no pagar.

## 12.4 Cómo protegerte

1. **No pagues y no negocies.** Pagar rara vez pone fin a la extorsión.
2. **Cambia las contraseñas filtradas** en todos los sitios donde todavía las uses, usa un gestor de contraseñas y activa la autenticación de dos factores.
3. **Mantén en privado tus fondos en cripto.** No compartas públicamente saldos, compras ni direcciones de billetera.
4. **Ten cuidado con las imágenes íntimas** y con los nuevos contactos en línea que insisten en pedirlas.
5. **Conserva las pruebas** y denuncia ante la plataforma y la policía.
6. **Toma en serio las amenazas contra tu seguridad física** y llama a la policía de inmediato.

## 12.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · GR-005

**Nunca sigas instrucciones urgentes de soporte o seguridad. Sal del canal y vuelve a entrar por la app o la URL oficial.**

No pagues ni negocies. Conserva las pruebas y denúncialo. Si tu seguridad está en riesgo, contacta a la policía.

| Regla | Enunciado | Por qué se aplica aquí |
|---|---|---|
| SDR-004 | Verifica las identidades fuera del canal del mensaje | Las amenazas legales y de autoridades deben comprobarse con la autoridad real. |
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | La extorsión llega como un contacto que no esperabas. |

*Tabla 12.3: Reglas CSF complementarias*

## 12.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: te están amenazando o extorsionando, cuenta comprometida. Luego añade los pasos para tu situación:

| Si tú… | Haz esto ahora |
|---|---|
| recibiste un correo de “dispositivo hackeado” | No respondas. Cambia la contraseña filtrada en todos los sitios donde la uses y activa la autenticación de dos factores. Elimina o denuncia el correo. |
| te están amenazando con imágenes reales | Corta el contacto, no pagues, guarda las pruebas y denuncia la cuenta y la amenaza ante la plataforma y la policía. Habla con alguien de confianza. |
| ya pagaste | Deja de pagar. Más pagos suelen traer más exigencias. Denuncia la dirección y los mensajes ante la policía. |

| Si tú… | Haz esto ahora |
|---|---|
| te amenazan con daño físico | Contacta a la policía de inmediato y sigue las indicaciones de seguridad física de la guía Hackers. |

*Tabla 12.4: Primeras acciones específicas del capítulo*

**DESPUÉS DE UNA PÉRDIDA**

Es probable que recibas ofertas para recuperar tu dinero. Son una segunda estafa. Consulta el Capítulo 13, Estafas de recuperación.

**CONTINÚA EN CRYPTOSAFETYFIRST.COM**

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/blackmail-extortion-scams-crypto-web3/

CAPÍTULO 13

# Estafas de recuperación

*“La segunda estafa apunta a la primera pérdida.”*

*Figura 13.1: Estafas de recuperación de un vistazo*

Después de una pérdida, muchas víctimas buscan ayuda, publican lo que les pasó o presentan denuncias. Los estafadores de recuperación están atentos precisamente a eso. Se hacen pasar por empresas de recuperación, abogados, “hackers éticos”, investigadores de blockchain o incluso unidades policiales, y prometen rastrear, congelar o devolverte tus criptomonedas. Luego cobran tarifas, piden acceso a tu billetera, o ambas cosas.

Las estafas de recuperación golpean a las personas cuando son más vulnerables y, a menudo, les quitan más que la estafa original. Este capítulo explica cómo funcionan, cómo es la ayuda legítima y qué hacer si ya pagaste.

EN ESTE CAPÍTULO


- 13.1 Estafas de recuperación que debes conocer
- 13.2 Cómo es la ayuda legítima
- 13.3 Escenario ilustrativo: el panel de recuperación
- 13.4 Cómo protegerte
- 13.5 Reglas CSF de este capítulo
- 13.6 Si esto te acaba de pasar


# 13.1 Estafas de recuperación que debes conocer

## 1. Empresas de recuperación falsas y servicios de “recuperación de fondos”

Sitios web y anuncios de aspecto profesional que afirman tener una alta tasa de éxito en la recuperación de criptomonedas robadas. Después de una “evaluación” gratuita, piden una tarifa por adelantado y luego más tarifas por “gastos legales”, “rastreo en la blockchain” o “impuestos de liberación”.

**Ejemplo:** Tras buscar ayuda, una víctima encuentra una empresa con testimonios y una garantía de recuperación. Le pide el 10% de la cantidad perdida por adelantado para iniciar el caso.

### Señales de alerta

- Recuperación garantizada o casi garantizada.
- Tarifas pagadas por adelantado, sobre todo en cripto.
- Testimonios que no puedes verificar.

### Cómo evitarlo

- Considera cualquier garantía de recuperación como una señal de alerta.
- Nunca pagues por adelantado para recuperar cripto.
- Denuncia primero ante la policía; deja que los procesos oficiales sigan su curso.

## 2. “Hackers éticos” y recuperación en las respuestas

Hay cuentas que responden debajo de publicaciones sobre pérdidas, o en chats de grupo, recomendando a un “hacker” que “recuperó mis fondos”. Varias cuentas pueden respaldar al mismo contacto.

**Ejemplo:** Debajo de una publicación pública sobre una billetera robada, tres cuentas recomiendan al mismo “experto en blockchain” y comparten un nombre de usuario de mensajería.

### Señales de alerta

- Recomendaciones no solicitadas debajo de tu publicación.
- Varias cuentas que elogian a la misma persona.
- Afirmaciones de que pueden hackear a los estafadores o la blockchain para recuperar los fondos.

### Cómo evitarlo

- No hagas caso a estas respuestas y denúncialas.
- Recuerda que nadie puede hackear una blockchain para revertir una transferencia.
- No compartas públicamente los detalles de tu pérdida junto con tus datos de contacto.

## 3. Policías, reguladores y abogados falsos

Los estafadores se hacen pasar por unidades de policía, agencias internacionales, reguladores o despachos de abogados. Dicen que encontraron tus fondos o que arrestaron a los delincuentes, y que se necesita una tarifa, un impuesto o un depósito para liberarte el dinero.

**Ejemplo:** Un correo electrónico con aspecto oficial dice que una unidad de ciberdelincuencia recuperó tu cripto y que debes pagar una tarifa de tramitación a una billetera antes de que te lo devuelvan.

### Señales de alerta

- Un mensaje de recuperación que no solicitaste, de parte de una “autoridad”.
- Tarifas para liberar el dinero recuperado.
- Documentos de aspecto oficial enviados por correo o chat.

### Cómo evitarlo

- La policía no cobra a las víctimas por investigar un caso ni por devolver fondos.
- Ponte en contacto con la agencia a través de su sitio web oficial para verificar cualquier mensaje.
- Si necesitas un abogado, búscalo tú mismo a través del colegio de abogados de tu país.

## 4. Recuperación a través de la estafa original

La plataforma o el contacto original vuelve con una nueva historia: un “departamento de retiros”, un “programa de compensación” o un “reembolso” para víctimas, y cada uno exige primero un pago.

**Ejemplo:** Semanas después de que una plataforma falsa bloqueara los retiros, un “responsable de cumplimiento” de la misma plataforma ofrece un reembolso una vez que se pague una última “tarifa de liquidación”.

### Señales de alerta

- Contacto de la plataforma o de la persona que causó la pérdida.
- Un reembolso o compensación que exige primero un pago.

### Cómo evitarlo

- Considera cualquier contacto de la estafa original como parte de ella.
- Detén todos los pagos y guarda los mensajes para tu denuncia.

## 5. Solicitudes de acceso a la billetera

Algunos estafadores de recuperación te piden tu frase semilla (frase de recuperación), que conectes tu billetera a una “herramienta de recuperación” o que instales software de acceso remoto “para rastrear los fondos”. El objetivo es lo que todavía te queda.

**Ejemplo:** Un “analista forense” te pide que conectes tu billetera a un sitio de rastreo para que el software pueda “cotejar tus transacciones”. El sitio solicita una aprobación de tokens.

### Señales de alerta

- Cualquier solicitud de tu frase semilla.
- Herramientas de recuperación que requieren conectar la billetera o una aprobación.
- Software de acceso remoto para “rastreo”.

### Cómo evitarlo

- Nunca compartas tu frase semilla ni instales software de acceso remoto.
- El rastreo usa datos públicos de la blockchain; nadie necesita tus claves privadas para hacerlo.

| Tipo | Cómo te llega | Señal de alerta clave | Cómo evitarlo |
|---|---|---|---|
| Empresa de recuperación falsa | Resultados de búsqueda y anuncios | Recuperación garantizada a cambio de una tarifa | Nunca pagues por adelantado |
| “Hacker ético” | Respuestas debajo de tus publicaciones | Varias cuentas respaldan a un mismo contacto | No hagas caso y denuncia |
| Policía o abogado falsos | Correo o llamada de aspecto oficial | Tarifa para liberar los fondos recuperados | Verifica a través de los sitios web oficiales |
| La estafa original vuelve | La misma plataforma o contacto | Reembolso que exige un pago | Detén todos los pagos |
| Solicitud de acceso a la billetera | “Herramienta de recuperación” o chat de soporte | Frase semilla, aprobación o acceso remoto | Nunca compartas el acceso |

*Tabla 13.1: Estafas de recuperación que debes conocer*

## 13.2 Cómo es la ayuda legítima

Por lo general, una transferencia confirmada en la blockchain no se puede revertir. Lo que a veces puede ayudar es la acción oficial sobre fondos que pasan por servicios regulados:

| Vía legítima | Qué puede hacer | Qué no puede hacer |
|---|---|---|
| Policía o servicio nacional de ciberdelincuencia | Abrir un caso, trabajar con exchanges (plataformas de intercambio) y otras autoridades y, en algunos casos, incautar fondos. | Prometer la recuperación ni plazos. No te cobran por investigar. |
| El exchange que recibió los fondos | Congelar los fondos que siguen en su plataforma tras una denuncia y compartir datos con las autoridades. | Revertir una transferencia en la blockchain ni actuar sobre fondos que ya salieron. |

| Vía legítima | Qué puede hacer | Qué no puede hacer |
|---|---|---|
| Un abogado que elijas tú mismo | Asesorar sobre reclamaciones civiles y trabajar con las autoridades. | Garantizar la recuperación. Ten cuidado con cualquiera que te haya contactado primero. |

*Tabla 13.2: Vías legítimas después de una pérdida*

Quienes ofrecen ayuda legítima rara vez te contactan primero – la policía real a veces sí lo hace, así que verifica cualquier contacto a través del sitio web oficial de la agencia antes de responder. No garantizan resultados, no piden tu frase semilla ni acceso remoto, y no piden pagos por adelantado en cripto.

## 13.3 Escenario ilustrativo: el panel de recuperación

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

Después de perder dinero en una plataforma de trading falsa, Sarah lo cuenta en un foro. Un día después la contacta una empresa de "recuperación de activos digitales". Le pide los hashes de sus transacciones y pronto le dice que ha rastreado sus fondos.

Obtiene acceso a un panel de cliente que muestra sus fondos como "recuperados" y "pendientes de liberación". Para liberarlos, debe pagar una tarifa de liberación, luego un impuesto y luego un "certificado antilavado de dinero".

### Qué pasó

La empresa de recuperación estaba dirigida por el mismo tipo de estafadores que la plataforma original, posiblemente las mismas personas. El panel era otro saldo falso, y cada tarifa era otro pago para ellos. El patrón es el mismo que el de la trampa de retiros del Capítulo 8.

### Puntos clave

- Un panel que muestra fondos "recuperados" no demuestra nada.
- Pagar para liberar fondos es una señal de estafa, tanto si la plataforma se presenta como un exchange como si se presenta como un servicio de recuperación.

- Cualquier contacto no solicitado después de publicar sobre una pérdida debe tratarse como hostil.

## 13.4 Cómo protegerte

1. **Denuncia primero por los canales oficiales**: la policía, el exchange involucrado y la plataforma donde ocurrió la estafa.
2. **Nunca pagues para recuperar cripto.** Ninguna tarifa, impuesto, depósito ni certificado libera fondos robados.
3. **Nunca compartas tu frase semilla**, no conectes tu billetera ni instales software para una “recuperación”.
4. **Ten cuidado con lo que publicas.** Describe tu pérdida públicamente sin datos de contacto. Es probable que los estafadores respondan.
5. **Busca ayuda por tu cuenta.** Si quieres asesoría legal, busca un abogado a través del colegio de abogados de tu país; nunca recurras a uno que te haya encontrado a ti.
6. **Habla con alguien de confianza.** Las pérdidas duelen, y los estafadores se aprovechan de la urgencia y la vergüenza. Una segunda opinión te protege.

## 13.5 Reglas CSF de este capítulo

REGLA PRINCIPAL · SDR-010

### Nunca pagues a nadie para recuperar criptomonedas perdidas.

Nadie puede revertir una transferencia en la blockchain a cambio de una tarifa. Denuncia ante la policía y el exchange por los canales oficiales.

| Regla | Enunciado | Por qué aplica aquí |
|---|---|---|
| SDR-003 | Nunca pagues para desbloquear o retirar fondos | Los paneles de recuperación usan la misma trampa de pagar para liberar fondos que las plataformas falsas. |

| Regla | Enunciado | Por qué aplica aquí |
|---|---|---|
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | Los estafadores de recuperación te encuentran después de que publiques o denuncies. |
| GR-001 | Nunca compartas tu frase semilla | Las “herramientas de recuperación” y los “analistas” suelen apuntar a lo que te queda. |
| SDR-004 | Verifica las identidades fuera del canal del mensaje | Los supuestos policías y abogados deben verificarse a través de los sitios web oficiales. |

*Tabla 13.3: Reglas CSF de apoyo*

## 13.6 Si esto te acaba de pasar

Primero busca tu situación en la tabla de triaje (**Empieza aquí**). Las filas que suelen aplicarse a este capítulo son: alguien se ofrece a recuperar tus pérdidas, enviaste dinero a un estafador, frase semilla expuesta. Luego añade los pasos para tu situación:

| Si… | Haz esto ahora |
|---|---|
| pagaste a un servicio de recuperación | Deja de pagar. Guarda todos los mensajes, facturas y datos de pago, y añádelos a tu denuncia policial como un segundo delito. |
| compartiste tu frase semilla o conectaste tu billetera | Sigue ahora las filas de frase semilla o de aprobación, desde un dispositivo limpio. |
| instalaste software para “rastreo” | Sigue la fila de malware y cambia las contraseñas desde otro dispositivo. |
| te contactó una “autoridad” por fondos recuperados | No respondas. Ponte en contacto con la agencia a través de su sitio web oficial y denuncia el mensaje. |
| sigues en contacto con un servicio de recuperación | Corta el contacto. No anuncies que sabes que es una estafa hasta que lo hayas guardado todo. |

*Tabla 13.4: Primeras acciones específicas del capítulo*

CONTINÚA EN CRYPTOSAFETYFIRST.COM

Lee la publicación completa del capítulo sobre este tipo de estafa (en inglés):

cryptosafetyfirst.com/recovery-scams-crypto-web3/

# Índice de reglas CSF

Estas son las reglas de CryptoSafetyFirst que se usan en este libro, con los capítulos en los que se aplican. El conjunto completo de reglas, incluidas las reglas para la configuración de billeteras, las copias de seguridad y la recuperación, se publica en CryptoSafetyFirst.com. Familias de reglas: GR = Reglas de Oro, OR = Reglas Operativas, SDR = Reglas de Defensa contra Estafas, TSR = Reglas de Seguridad Técnica.

| Regla | Enunciado | Capítulos |
|---|---|---|
| GR-001 | Nunca compartas tu frase semilla | 2, 3, 4, 13 |
| GR-002 | Verifica siempre la URL y el dominio completos antes de conectar tu billetera a cualquier sitio web | 3, 5 |
| GR-003 | Usa siempre una billetera de hardware para guardar cripto a largo plazo o de alto valor | 4 |
| GR-004 | Revoca siempre las aprobaciones de tokens que no uses después de interactuar con contratos inteligentes nuevos | 5, 7 |
| GR-005 | Nunca sigas instrucciones urgentes de soporte o seguridad. Sal del canal y vuelve a entrar por la app o la URL oficial | 2, 12 |
| GR-006 | Envía siempre una pequeña transacción de prueba antes de transferir grandes cantidades de cripto | 6 |
| GR-008 | Guarda tus fondos a largo plazo en una billetera bóveda. Usa otra billetera para DApps, trading y Web3 | 5, 7 |
| OR-005 | Verifica siempre el destino antes de enviar cripto | 6 |
| SDR-001 | Nunca confíes en un contacto cripto que no solicitaste | 1, 2, 8, 10, 12, 13 |
| SDR-002 | Nunca envíes cripto para recibir cripto | 1, 7, 11 |
| SDR-003 | Nunca pagues para desbloquear o retirar fondos | 8, 10, 11, 13 |
| SDR-004 | Verifica las identidades fuera del canal del mensaje | 1, 2, 10, 12, 13 |

| Regla | Enunciado | Capítulos |
|---|---|---|
| SDR-005 | Nunca conectes tu billetera a sitios web desconocidos | 3, 5, 7 |
| SDR-006 | Desconfía de la urgencia, la euforia y las ganancias garantizadas | 1, 8, 9, 10 |
| SDR-007 | Verifica los proyectos antes de invertir | 8, 9 |
| SDR-008 | Nunca confíes en la popularidad en redes sociales | 9 |
| SDR-009 | Verifica todos los enlaces antes de iniciar sesión | 3 |
| SDR-010 | Nunca pagues a nadie para recuperar criptomonedas perdidas | 13 |
| TSR-001 | Nunca instales software cripto de fuentes no oficiales | 4, 11 |
| TSR-002 | Da por hecho que tu dispositivo puede estar comprometido | 4 |
| TSR-004 | Usa autenticación de dos factores basada en hardware | 3 |
| TSR-005 | Activa las listas blancas de retiros en los exchanges | 6 |
| TSR-006 | Separa dispositivos y cuentas para el uso de cripto | 4, 11 |
| TSR-007 | Tómate tu tiempo antes de hacer clic o instalar | 1 |

*Reglas CSF usadas en este libro*

# Sigue aprendiendo

Las estafas cambian más rápido que cualquier libro. CryptoSafetyFirst.com mantiene viva esta guía entre ediciones:

- **Una página para cada capítulo, actualizada a medida que cambian las estafas.**
- **Cómo denunciar una estafa cripto**: enlaces de denuncia por país, siempre actualizados.
- **The Three-Wallet Model (Modelo de Tres Billeteras)**: una guía y un kit de herramientas gratuitos para configurar billeteras Bóveda, de Uso Frecuente y Desechables.
- **Las guías de Errores de Usuario y de Hackers**, para las pérdidas que no son estafas.

En cripto y Web3, cruzarse con estafas es inevitable. Convertirse en víctima no lo es. El conocimiento y la conciencia son tu mejor defensa.

**cryptosafetyfirst.com**