cifra.

Tu primera wallet segura, paso a paso.

La guía práctica para proteger tus criptomonedas sin palabras complicadas. Para gente real, con plata real, que no quiere perderla por un descuido.

Tus cripto, claras.

Guía educativa gratuita · Cifra Cripto · Colombia · 2026

Lo que vas a aprender

Esta guía está pensada para leerse en orden, pero cada capítulo funciona solo. Si ya tienes wallet y solo quieres revisar tu seguridad, salta directo al Capítulo 4.

ANTES DE EMPEZAR

Una sola cosa te pedimos: **ve despacio**. En cripto, la prisa es el error número uno. Nada de lo que hay aquí requiere actuar hoy mismo. Lee, entiende, y después actúa. Si llegas al final de esta guía habiendo hecho una sola cosa bien —guardar tu frase de recuperación en papel— ya estás por delante de la mayoría.

01

Antes de tocar nada: los conceptos que hay que tener claros

Nadie pierde sus cripto por no saber programar. Las pierde por no entender cuatro ideas básicas. Este capítulo te las explica con ejemplos de la vida diaria, y al terminar vas a entender más de seguridad cripto que la mayoría de gente que lleva años "invirtiendo".

¿Qué es una wallet, realmente?

Empecemos por desarmar el nombre, porque confunde. "Wallet" significa billetera, pero una wallet **no guarda tus criptomonedas adentro**, como una billetera guarda billetes. Tus cripto viven en la blockchain —piénsala como un libro de contabilidad público y gigante, copiado en miles de computadores del mundo, donde quedan anotadas todas las transacciones y nadie puede borrar ni alterar lo que ya quedó escrito.

Lo que tu wallet guarda son **las llaves**. Es decir: la wallet es más parecida al llavero de tu casa que a tu billetera. La casa (tus cripto) está en otra parte; lo que tú cargas es la llave que demuestra que es tuya y te deja entrar. Quien tenga la llave, controla la casa. Sin excepciones, sin "olvidé mi contraseña", sin línea de atención al cliente.

> **CONCEPTO CLAVE**
>
> Una wallet no guarda monedas: guarda llaves. Proteger tus cripto es, en realidad, proteger unas llaves. Toda esta guía se reduce a eso.

Exchange vs. wallet propia: el banco y la caja fuerte

Si compraste cripto en Binance, Bitso, Coinbase o Lemon, hoy tus cripto están en un **exchange**: una empresa que compra, vende y guarda cripto por ti. Funciona parecido a un banco: tú tienes una cuenta, ellos custodian la plata, y tú confías en que estará ahí cuando la pidas.

Eso es cómodo y, para empezar, razonable. Pero hay una diferencia enorme con un banco colombiano: **los exchanges no están cubiertos por Fogafín ni vigilados como entidades financieras**. Si el exchange quiebra, es hackeado o congela retiros, no hay seguro de depósitos que te responda. Ha pasado: en 2022, FTX —uno de los exchanges más grandes del mundo, con publicidad en estadios y celebridades— colapsó en una semana y millones de usuarios quedaron sin acceso a su dinero.

Una **wallet propia**, en cambio, es como pasar la plata del banco a una caja fuerte en tu casa: nadie más puede congelarla ni perderla por ti... pero ahora la responsabilidad de la llave es tuya. Ese es el intercambio honesto: *menos dependencia de terceros, más responsabilidad personal*. Esta guía existe para que esa responsabilidad no te quede grande.

Custodial vs. non-custodial: "si no es tu llave, no es tu cripto"

En el mundo cripto hay una frase repetida hasta el cansancio, y por una vez la repetición está justificada: *"not your keys, not your coins"* — si no es tu llave, no es tu cripto.

- **Custodial** (custodiada): otro guarda las llaves por ti. Es el caso del exchange. Tú ves un saldo en pantalla, pero técnicamente lo que tienes es una promesa de la empresa.
- **Non-custodial** (no custodiada): tú guardas las llaves. Nadie —ni la app, ni el fabricante, ni Cifra— puede mover tus cripto ni recuperarlas si pierdes la llave. Control total, responsabilidad total.

EJEMPLO COTIDIANO

Piensa en el parqueadero del centro comercial con valet parking. Entregas las llaves del carro y te dan un ticket. Mientras el negocio funcione bien, todo perfecto. Pero el carro lo mueve quien tiene las llaves, no quien tiene el ticket. Un exchange es el valet parking; el saldo que ves en la app de Binance es el ticket.

Hot wallet vs. cold wallet: el bolsillo y la caja fuerte

Dentro de las wallets propias hay dos familias, y la diferencia es una sola: **si la llave toca internet o no**.

- **Hot wallet** (caliente): una app en tu celular o computador, conectada a internet. Ejemplos: Trust Wallet, MetaMask, Phantom. Es como el efectivo que llevas en el bolsillo: práctico para el día a día, pero no cargarías ahí los ahorros de tu vida.
- **Cold wallet** (fría): un aparato físico —parecido a una USB— que guarda la llave sin conexión a internet. Ejemplos: Ledger, Trezor. Es la caja fuerte: menos cómoda para el uso diario, mucho más difícil de robar a distancia.

¿Cuándo usar cada una? Una regla simple y honesta: **en la hot wallet solo lo que te dolería perder como te dolería perder la billetera en un bus**. Lo demás, en frío. En el Capítulo 2 te damos un criterio con números.

La frase de recuperación: el concepto más importante de toda la guía

Cuando crees tu primera wallet, la app te va a mostrar **12 o 24 palabras en inglés**, en un orden específico. Se llama frase de recuperación, frase semilla o *seed phrase*. Parecen inofensivas —palabras

como *apple, river, motor*— pero son literalmente las llaves de tu casa: cualquiera que las tenga, entra. Y quien las tenga puede reconstruir tu wallet completa en cualquier celular del mundo, sin pedirte permiso, sin que te llegue una notificación.

Por eso van **en papel y bajo llave**. No en una nota del celular, no en una foto, no en un correo a ti mismo, no en un WhatsApp para "no perderlas". En papel.

> **ADVERTENCIA CRÍTICA**
>
> La mayoría de robos de cripto a personas comunes no son hackeos de película. Son esto: alguien encontró la frase de recuperación en una foto de la galería, en una nota de iCloud o porque la víctima la escribió en una página falsa. Si solo recuerdas una cosa de esta guía, que sea esta: **la frase de recuperación nunca se digita en internet y nunca se guarda en digital. Nunca.**

Y la otra cara de la moneda: si pierdes el papel y se daña tu celular, **no hay botón de "olvidé mi contraseña"**. Las cripto quedan ahí, en la blockchain, intactas y visibles... e inalcanzables para siempre. Se estima que millones de bitcoins —una porción significativa de todos los que existen— están perdidos así, no robados: simplemente sus dueños perdieron las llaves.

Ya tienes el mapa: llaves, custodia, caliente, frío, frase de recuperación. Ahora viene la primera decisión real: ¿cuál wallet elegir? Spoiler: la respuesta depende de cuánta plata estamos hablando, y te lo contamos sin venderte nada.

02

Elegir tu primera wallet (sin equivocarte)

Aquí no hay marca patrocinada ni link de afiliado. Solo las opciones que, en 2026, tienen trayectoria, mantenimiento activo y comunidad grande. La elección correcta depende de una sola pregunta: ¿cuánto te dolería perder lo que vas a guardar?

Para empezar con montos pequeños: software wallets

Si estás moviendo montos que equivalen a "la plata del mercado del mes" o menos, una software wallet (hot wallet) bien configurada es un punto de partida razonable. Las tres con mejor reputación y soporte:

- **Trust Wallet** — la más amigable para empezar. Soporta muchas redes (Bitcoin, Ethereum, BNB y más) en una sola app. Será nuestro ejemplo paso a paso en el Capítulo 3.
- **MetaMask** — el estándar para Ethereum y redes compatibles (las llamadas EVM). Más usada por quienes interactúan con aplicaciones en esas redes.
- **Phantom** — la referencia para la red Solana, con una de las mejores experiencias de uso.

Cómo verificar que descargas la app oficial (esto importa más de lo que crees)

Existen copias falsas de estas apps, idénticas a la original, cuyo único propósito es robarte la frase de recuperación. La regla:

1. **Nunca llegues a la descarga desde un link**: ni de Google, ni de un anuncio, ni de un mensaje, ni de un video de YouTube. Los anuncios falsos pagan por aparecer de primeros.
2. Escribe tú mismo la dirección oficial en el navegador (**trustwallet.com**, **metamask.io**, **phantom.com**) y desde ahí deja que el sitio te lleve a la tienda de aplicaciones.
3. Ya en App Store o Google Play, **verifica el desarrollador**: que sea la empresa oficial, con millones de descargas y años de reseñas. Una app "nueva" con 500 descargas y el mismo logo es una trampa.

CASO REAL (TIPO DE ESTAFA DOCUMENTADA EN COLOMBIA)

Una persona busca "MetaMask" en Google y entra al primer resultado, que es un anuncio pagado con un dominio casi idéntico (metamask-**app**.io, por ejemplo). Descarga la "app", crea su wallet, transfiere desde Binance… y a los minutos el saldo está en cero. La app falsa envió la frase de recuperación al estafador en el momento en que se generó. Este patrón se repite cada semana en grupos de cripto colombianos. La defensa es aburrida y efectiva: escribir la URL a mano.

Para montos serios: hardware wallets

Cuando lo que guardas ya representa varios meses de ahorro —o simplemente una cifra que te quitaría el sueño perder— el estándar es una hardware wallet. Las dos opciones honestas del mercado, con años de trayectoria y auditorías:

- **Ledger Nano S Plus** — el modelo de entrada de Ledger (Francia). Precio de fábrica alrededor de 79 USD; puesto en Colombia, con envío e impuestos, calcula entre **$400.000 y $550.000 COP aproximados** según la tasa de cambio del momento.
- **Trezor Safe 3** — el modelo de entrada de Trezor (República Checa), pionera del sector. Rango de precio similar.

¿Vale la pena pagar eso? Hazte la cuenta al revés: si guardas el equivalente a $20 millones de pesos, el dispositivo cuesta menos del 3% de lo que protege. Es el candado más barato en proporción a la puerta.

Cómo comprarla desde Colombia sin caer en estafas

REGLA INNEGOCIABLE

Una hardware wallet se compra **únicamente en el sitio oficial del fabricante** (ledger.com o trezor.io) o en los distribuidores autorizados que esos mismos sitios listan. Nunca en Mercado Libre, nunca usada, nunca "sellada, casi nueva", nunca a un conocido. Un dispositivo manipulado puede venir con una frase de recuperación pre-generada que el vendedor ya conoce: tú depositas, él retira.

Pistas de que un dispositivo fue manipulado: viene con la frase de recuperación ya impresa "para tu comodidad", el empaque trae una "tarjeta de regalo con la frase incluida", o el dispositivo no te pide generar una frase nueva al encenderlo por primera vez. Una hardware wallet legítima **siempre** te obliga a generar tu propia frase en la primera configuración.

Cuadro comparativo honesto

	Exchange (Binance, Bitso...)	Software wallet (Trust, MetaMask...)	Hardware wallet (Ledger, Trezor)
¿Quién tiene la llave?	La empresa	Tú	Tú
Costo	Gratis (cobran comisiones)	Gratis	$400.000–$550.000 COP aprox.
Comodidad	Muy alta	Alta	Media
Riesgo principal	Quiebra, hackeo o congelamiento del exchange	Malware en tu celular, phishing, descuido con la frase	Perder dispositivo Y frase a la vez; comprar uno manipulado
¿Recuperable si pierdes acceso?	Sí, con soporte al cliente	Solo con tu frase en papel	Solo con tu frase en papel
Ideal para	Comprar/vender y montos pequeños transitorios	Uso frecuente, montos moderados	Ahorro de largo plazo, montos serios

Fíjate que ninguna columna gana en todo. No existe la opción perfecta; existe la opción adecuada *para cada monto y cada uso*. La mayoría de gente termina usando una combinación: algo en el exchange para operar, una hot wallet para el día a día y —cuando el monto lo justifica— una fría para el ahorro.

Ya sabes qué elegir. Ahora viene la parte donde la mayoría comete el error que no tiene reversa: la configuración. Vamos despacio, paso a paso, y con la frase de recuperación tratada como lo que es: lo más valioso del proceso.

03

Configuración paso a paso: la parte práctica

Reserva 30 minutos sin afán, a solas, con papel y esfero a la mano. No es exageración: la frase que vas a escribir en los próximos minutos vale exactamente lo mismo que todo lo que llegues a guardar en esa wallet.

Setup de una software wallet (ejemplo: Trust Wallet)

Usamos Trust Wallet como ejemplo, pero los pasos son casi idénticos en MetaMask y Phantom. Las pantallas cambian; la lógica no.

1. **Descarga verificada.** Escribe trustwallet.com en el navegador, déjate llevar a la tienda oficial y confirma el desarrollador (Capítulo 2). Instala.
2. **Crea una wallet nueva.** Abre la app y elige "Crear una billetera nueva". No "importar": eso es para cuando ya tienes una frase.
3. **Activa la seguridad de la app.** Configura PIN o biometría para abrir la app. Esto protege el celular perdido, no reemplaza la frase.
4. **Llega el momento importante: la frase de recuperación.** La app te mostrará 12 palabras. Antes de verlas, mira alrededor: nadie debe estar viendo tu pantalla, y tú no debes estar compartiendo pantalla en ninguna videollamada. **Escríbelas a mano, en papel, en orden, con número.** Verifica letra por letra: "there" no es "three".
5. **No tomes captura de pantalla.** La app misma suele bloquearlo. Si tu instinto dice "le tomo una foto por si acaso", ese instinto es exactamente el que vacía wallets.
6. **Confirma la frase.** La app te pedirá repetir algunas palabras en orden. Hazlo leyendo de tu papel, no de memoria: así verificas que lo escrito está bien.
7. **Listo.** Ya tienes una wallet non-custodial. Está vacía, y así debe seguir hasta que termines este capítulo.

Setup de una hardware wallet (ejemplo: Ledger)

1. **Inspecciona el paquete.** Comprado solo en el sitio oficial. Si viene con una frase pre-impresa o el dispositivo no pide configuración inicial, no lo uses: contacta al fabricante.

2. **Ve a la dirección oficial de inicio** (ledger.com/start) escrita a mano en tu navegador, e instala la aplicación oficial de escritorio (Ledger Live).

3. **Configura como dispositivo nuevo.** El aparato te pedirá crear un PIN. Elígelo tú; jamás uses uno que venga sugerido en papel.

4. **El dispositivo —no el computador— te mostrará 24 palabras en su pantallita.** Esto es deliberado: la frase nunca toca el computador ni internet. Escríbelas a mano, en orden, verificando una a una. El dispositivo luego te pedirá confirmarlas.

5. **Regla de oro del mundo Ledger/Trezor:** ningún software legítimo, ningún soporte técnico, ninguna "actualización" te pedirá jamás digitar esas 24 palabras en el computador. Si algo te las pide, es un fraude, sin excepción.

Cómo guardar la frase de recuperación (el paso que define todo)

> **EL MÉTODO SIMPLE QUE FUNCIONA**
>
> **Dos copias en papel, en dos lugares físicos diferentes.** Por ejemplo: una en una caja con llave en tu casa y otra donde un familiar de máxima confianza o en un cajilla de seguridad. Si un incendio, robo o inundación afecta un lugar, el otro te salva.

- **Papel y tinta que aguanten.** No necesitas productos de marca: papel grueso, esfero de tinta permanente, y protege cada copia en una bolsa plástica sellada tipo ziploc. Si quieres ir más allá, existen placas metálicas genéricas para grabar las palabras (resisten fuego y agua); cualquier ferretería de ideas básicas resuelve.
- **Sin pistas en el papel.** No escribas "frase de Trust Wallet" ni tu nombre. Solo las palabras numeradas. Quien no sabe qué es, ve una lista rara; quien sabe, no debe saber de quién es.
- **Nunca en digital. De ninguna forma.** Ni foto, ni nota, ni correo, ni Drive, ni "partida en dos archivos", ni un audio. El papel no se hackea a distancia; todo lo digital, sí.

Verificación: la transacción de prueba

Antes de confiar montos serios, comprueba que todo el circuito funciona:

1. Desde tu exchange, envía un **monto pequeño** a tu nueva wallet — el equivalente a $20.000 o $50.000 COP, lo suficiente para que la prueba sea real y la pérdida, si algo sale mal, sea una lección barata.

2. Verifica que llegó (puede tardar de segundos a varios minutos según la red).

3. **Prueba el camino de regreso:** envía una parte de vuelta al exchange. Saber recibir es la mitad; saber enviar es la otra.
4. Solo cuando el viaje de ida y vuelta funcionó, mueve montos mayores — y aún así, en partes, no todo de una.

Una verificación adicional que vale oro: **borra la app y restáurala con tu frase en papel** (con la wallet aún casi vacía). Si la restauración funciona, tu papel está bien escrito. Descubrirlo ahora, con $50.000, es infinitamente mejor que descubrir un error de copia dentro de tres años, con todos tus ahorros.

Wallet creada, frase en papel, prueba superada. Ahora viene la vida real: enviar, recibir y esquivar a los que viven de los descuidos ajenos. El siguiente capítulo es el que vas a releer más veces.

04

El día a día sin sustos

Las transacciones cripto no tienen reversa: no hay banco al cual llamar, no hay "disputa de la transacción". Eso suena aterrador, pero con tres hábitos simples el riesgo del día a día se reduce drásticamente. Aquí están.

Cómo enviar cripto sin perderlas en el camino

1. Verifica la red antes que todo

Este es el error técnico más común. Una misma moneda puede viajar por redes distintas, y **la red de salida debe coincidir con la red de llegada**. Enviar USDT por la red equivocada es como enviar una encomienda con la transportadora equivocada a una oficina que no trabaja con ella: el paquete puede no llegar jamás.

EJEMPLO CONCRETO

Vas a retirar USDT de Binance hacia tu Trust Wallet. Binance te pregunta por cuál red: ERC-20 (Ethereum), TRC-20 (Tron), BEP-20 (BNB)... En tu Trust Wallet, al recibir, también eliges la red. **Si en Binance eliges TRC-20, en Trust Wallet debes copiar la dirección de USDT en la red Tron.** Misma moneda, distinta carretera. Cuando dudes, la transacción de prueba pequeña responde la duda por ti.

2. Copia y pega la dirección. Nunca la escribas a mano

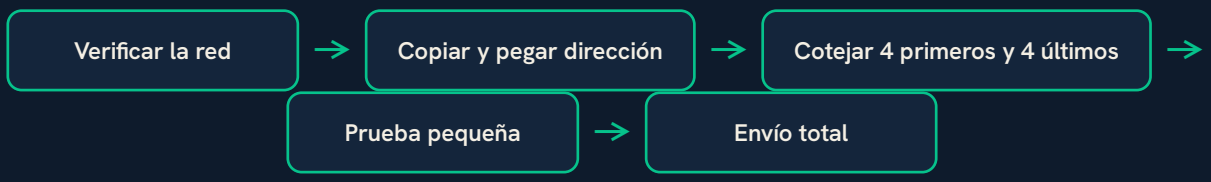
Una dirección cripto se ve así: *0x4f3a...c91B* — 30 o 40 caracteres sin lógica humana. Un solo carácter mal y la plata sale hacia una dirección que probablemente no es de nadie. Copia y pega, siempre.

3. Verifica los primeros 4 y los últimos 4 caracteres

¿Por qué, si ya copiaste y pegaste? Porque existe malware que **cambia la dirección en el portapapeles**: tú copias la tuya, el virus pega la del ladrón. Comparar el inicio y el final de la dirección pegada contra la original toma cinco segundos y anula ese ataque.

4. Si el monto es grande, primero una prueba pequeña

Sí, pagas dos veces la comisión de red. Considéralo el seguro más barato del mundo financiero.



El ritual de envío seguro. Cinco pasos, dos minutos, cero sustos.

Cómo recibir cripto sin riesgo

- En tu wallet, elige la moneda **y la red correcta**, y comparte la dirección desde el botón de "Recibir" (copiar o código QR). Nunca la dictes por teléfono ni la transcribas de oído.
- Tu dirección de recepción **no es secreta** —compartirla no te pone en riesgo—, pero confírmale al que envía la red exacta.
- Desconfía de depósitos que no esperabas: tokens desconocidos que aparecen solos en tu wallet suelen ser carnada de estafa. **No los toques, no los "reclames", no visites el sitio que mencionan.** Ignorarlos no tiene costo.

Phishing: cómo detectarlo (con los libretos que circulan en Colombia)

El phishing es suplantación: alguien se hace pasar por una entidad legítima para que tú mismo entregues las llaves. Los libretos más comunes por acá:

- **"Soporte de Binance" por WhatsApp o Telegram:** te escriben porque "detectaron actividad sospechosa" y necesitan "validar tu wallet". Ningún exchange te escribe primero por WhatsApp. Ninguno te pide la frase de recuperación. Jamás.
- **El falso asesor de inversiones:** empieza en redes o citas en línea, gana tu confianza durante semanas, muestra "ganancias" en una plataforma que solo él conoce, y te guía a depositar más. Cuando intentas retirar, aparecen "impuestos" y "comisiones de desbloqueo". Es la estafa conocida como *pig butchering* y ha golpeado fuerte en Colombia. La plataforma entera es falsa desde el día uno.
- **El "error a tu favor":** te llega un mensaje con una frase de recuperación ajena ("mira mi wallet, tiene 5.000 USDT, no sé retirarlos, te doy una parte si me ayudas"). Es una trampa: para "retirar" hay que depositar primero una comisión de red... que va directo al estafador.
- **Sorteos y regalos:** "Binance regala BNB por aniversario, conecta tu wallet aquí". Nadie regala cripto. La página a la que conectas tu wallet la vacía.
- **Y fuera de la pantalla, el riesgo físico:** en ciudades colombianas se han documentado robos y "paseos millonarios" donde las víctimas fueron forzadas a transferir cripto desde sus celulares. La discreción también es seguridad: no presumas tenencias en redes, no cuentes cuánto tienes, no hagas operaciones grandes en público.

EL DETECTOR UNIVERSAL DE PHISHING

Toda estafa cripto, sin importar el disfraz, termina pidiéndote una de tres cosas: **(1) tu frase de recuperación, (2) que conectes tu wallet a un sitio que no buscaste tú, o (3) que envíes plata primero para recibir plata después.** Cuando aparezca cualquiera de las tres, ya tienes la respuesta: es estafa. No necesitas entender el resto del cuento.

Higiene de seguridad básica

- **Nada de wifi público para operaciones.** El wifi del centro comercial o del aeropuerto sirve para ver memes, no para mover plata. Usa tus datos móviles.
- **2FA con aplicación, no con SMS.** Activa la verificación de dos pasos en tus exchanges con una app de códigos (Google Authenticator, Aegis o similar). El SMS es vulnerable al *SIM swapping*: en Colombia se han reportado casos de delincuentes que duplican la SIM de la víctima con documentos falsos y reciben sus códigos de verificación.
- **Navegador limpio.** Las extensiones de navegador pueden leer lo que haces en cada página. Para operaciones cripto, usa un navegador (o un perfil de navegador) sin extensiones, salvo la wallet misma si usas MetaMask.
- **Celular y apps actualizadas.** Las actualizaciones aburridas tapan los huecos por donde entra el malware.

Hasta aquí, todo trata de protegerte de los demás y de tus propios descuidos. El siguiente capítulo trata de algo más incómodo y más importante: proteger a tu familia de un escenario en el que tú no estés para explicarles dónde está nada.

05

Plan de sucesión cripto: lo que casi nadie te cuenta

Este capítulo es corto, incómodo y posiblemente el más valioso de la guía. Porque la seguridad perfecta tiene un efecto secundario del que nadie habla: si nadie más que tú puede acceder a tus cripto... nadie más que tú puede acceder a tus cripto.

Por qué importa

Los análisis del sector estiman que **millones de bitcoins —cerca de una quinta parte de todos los que existen— están en wallets que no se han movido en años y se presumen perdidos**: llaves extraviadas, discos botados, dueños fallecidos sin dejar instrucciones. A diferencia de una cuenta bancaria, donde los herederos pueden reclamar con un proceso de sucesión, una wallet sin frase de recuperación es una bóveda sin combinación: ni el juez más poderoso del mundo puede abrirla.

La paradoja es esta: cuanto mejor hiciste todo lo de los capítulos anteriores, más invisible es tu patrimonio para tu familia. Resolverlo no requiere abogados caros ni tecnología; requiere una carta bien pensada.

El principio: instrucciones hoy, acceso solo cuando toque

El error sería el extremo opuesto: entregarle la frase de recuperación a tu pareja o a tus hijos "por si acaso". Eso multiplica los puntos de fuga hoy para resolver un problema de mañana. El diseño correcto separa dos cosas:

- **El QUÉ y el DÓNDE** — que tu familia sepa que existen las cripto y dónde están las instrucciones de acceso.
- **El acceso en sí** — la frase en papel, que sigue guardada bajo llave como hasta ahora, sin que nadie la vea.

La "carta sellada": cómo hacerla

Escribe una carta —a mano o impresa— y guárdala en sobre sellado junto a tus documentos importantes (o, mejor, déjala referenciada en tu testamento mediante notaría; en Colombia, un

testamento cerrado ante notario es una figura existente y económica comparada con lo que protege). La carta debe contener:

1. **Qué existe:** "Tengo criptomonedas guardadas en una wallet propia y saldos en los exchanges X y Y." Sin montos exactos si no quieres; la cifra cambia, la existencia no.
2. **Dónde están las llaves:** "La frase de recuperación está escrita en papel, en [lugar 1] y una copia en [lugar 2]." **El lugar, no la frase.**
3. **Cómo usarlas:** instrucciones simples: "con esa frase, descarguen la app oficial Trust Wallet desde trustwallet.com, elijan 'importar wallet' y escriban las palabras en orden". Dos renglones que ahorran semanas de confusión.
4. **A quién acudir:** el nombre de una persona de confianza que entienda del tema y pueda acompañar el proceso sin quedarse con nada (el acceso sigue dependiendo del papel, que está en manos de la familia).
5. **Advertencias mínimas:** "no le entreguen la frase a ningún 'asesor', no la digiten en páginas web, no acepten ayuda de desconocidos en internet". Tu familia heredará también a los estafadores del Capítulo 4.

> **LO QUE LA CARTA NUNCA DEBE CONTENER**
>
> Ni la frase de recuperación, ni contraseñas, ni PINs. La carta dice **dónde** están las llaves, jamás **cuáles** son. Una carta es un documento que pasa por manos: notarios, cajones, familiares. Si contiene la frase, cada una de esas manos es un riesgo. Si contiene solo la ubicación, robarla no sirve de nada sin acceso físico al escondite.

Mantenimiento: revísala una vez al año

Cambiar de wallet, mover el escondite del papel o abrir cuenta en otro exchange vuelve obsoleta la carta. Un recordatorio anual en el calendario —cada cumpleaños, por ejemplo— y diez minutos de actualización bastan. Un plan de sucesión desactualizado da una falsa tranquilidad que es casi peor que no tener ninguno.

Ya tienes el sistema completo: conceptos, elección, configuración, día a día y hasta el plan que protege a los tuyos. Cerremos con un repaso de los errores que más se repiten en Colombia y el criterio para tu siguiente paso.

06

Errores comunes y próximos pasos

Si llegaste hasta aquí, ya no eres principiante en seguridad cripto. Este capítulo es tu lista de chequeo de salida: los errores que vacían wallets en Colombia, el criterio para subir de nivel, y cómo seguir aprendiendo sin caer en manos de gurús.

Los 8 errores más frecuentes (y su antídoto en una línea)

1. **Guardar la frase de recuperación en digital** (foto, nota, WhatsApp). → Papel, dos copias, dos lugares. Si hoy la tienes en una foto: escríbela en papel, borra la foto (también de "eliminados recientes" y de la nube) y, en cuanto puedas, crea una wallet nueva y migra los fondos, porque esa frase ya debe considerarse expuesta.
2. **Digitar la frase en una página o app que la pidió.** → Nadie legítimo la pide. Nunca. Si la digitaste en algún lado, migra a una wallet nueva hoy.
3. **Descargar la wallet desde un link o anuncio.** → URL oficial escrita a mano, desarrollador verificado en la tienda.
4. **Enviar por la red equivocada.** → Confirmar red de salida = red de llegada, y prueba pequeña ante la duda.
5. **Confiar en el "asesor" que llegó por redes sociales.** → Quien te promete rentabilidad garantizada te está describiendo la estafa, no la inversión.
6. **Dejar todo en el exchange indefinidamente.** → El exchange es para operar; el ahorro serio vive en wallet propia. El saldo en exchange es un ticket de valet parking, no la llave del carro.
7. **Comprar hardware wallet usada o por marketplace.** → Solo sitio oficial del fabricante. Sin excepciones de "es que estaba en promoción".
8. **No dejar plan de sucesión.** → Una carta sellada que diga qué existe y dónde están las llaves (no cuáles son). Capítulo 5, una tarde, listo.

¿Notas el patrón? Ninguno de los ocho requiere conocimiento técnico para evitarse. Todos se previenen con hábitos. Esa es la buena noticia de la seguridad cripto: es una disciplina de gente ordenada, no de ingenieros.

¿Cuándo migrar de software wallet a hardware wallet?

Un criterio claro, sin misticismo. Pásate a una hardware wallet cuando se cumpla cualquiera de estas dos condiciones:

> **CRITERIO DE MIGRACIÓN**
>
> **1. El monto guardado supera 10 veces el costo del dispositivo** (es decir, alrededor de $4–5 millones de pesos: el "seguro" cuesta menos del 10% de lo asegurado). **2. Lo que guardas es ahorro de largo plazo que no piensas mover en meses.** Si guardas para no tocar, no tiene sentido que las llaves vivan en un aparato que se conecta a internet 200 veces al día.

Un apunte sobre el contexto colombiano: la DIAN ya recibe reportes

Desde la Resolución 000240 de 2025, los exchanges que operan con usuarios en Colombia reportan información de operaciones a la DIAN. Esto no cambia nada de la seguridad técnica de esta guía, pero sí cambia algo de fondo: **el desorden ya no es solo un riesgo de seguridad, también es un riesgo tributario**. Tener tus wallets identificadas, tus movimientos rastreables por ti mismo y tu historial ordenado dejó de ser opcional. La misma disciplina que protege tus llaves te sirve para tener tus cuentas claras. Orden es orden.

Cómo seguir aprendiendo (sin gurús)

- **Las fuentes oficiales primero:** los centros de ayuda y blogs de los fabricantes y apps que ya usas (Ledger Academy, los centros de soporte de Trezor, Trust Wallet, MetaMask) explican su producto mejor que cualquier youtuber, y no te venden nada adicional.
- **Material educativo de los propios exchanges** (como Binance Academy) para conceptos generales: útil para aprender términos, leyendo con la conciencia de que son empresas con intereses comerciales.
- **El filtro definitivo para cualquier contenido cripto:** si el video, cuenta o "academia" promete rentabilidades, muestra pantallazos de ganancias o mete afán ("últimos cupos", "el tren se va"), ciérralo. El conocimiento real de seguridad es aburrido, gratuito y nunca tiene afán. Como esta guía.

Para terminar: el siguiente paso (solo si te aplica)

Esta guía cubre lo más importante para que no pierdas tus cripto por errores propios. Lo que no cubrimos aquí —porque depende de tu caso particular— es:

- Cómo declarar correctamente tus cripto ante la DIAN.
- Cómo organizar el historial cuando tienes operaciones en varios exchanges.
- Cómo recibir pagos del exterior en stablecoins y reducir comisiones.

Si te aplica alguno de esos puntos, te ofrecemos un **Diagnóstico Cripto de 30 minutos sin costo**. Revisamos tu caso, te decimos honestamente si necesitas servicio o si te alcanza con lo que ya sabes, y tú decides desde ahí.

Escríbenos por DM a **@cifracripto** con la palabra

DIAGNÓSTICO

Antes de cerrar este PDF

Tu checklist de salida. Si puedes marcar las cinco, esta guía cumplió su promesa:

✓ Entiendo que mi wallet guarda llaves, no monedas — y que la frase de recuperación ES la llave.

✓ Mi frase de recuperación está en papel, en dos lugares, y en cero lugares digitales.

✓ Sé verificar app oficial, red correcta y dirección (4 primeros, 4 últimos) antes de cada envío.

✓ Reconozco las tres señales universales de estafa: pedir la frase, conectar la wallet, o pagar para recibir.

✓ Mi familia sabría qué existe y dónde buscar instrucciones si yo no estuviera.

Ve despacio. Ve seguro. Y cuando tengas dudas, vuelve a esta guía: para eso es.

cifra. · Tus cripto, claras.
