Three-Wallet Toolkit

Hojas de trabajo y listas de verificación prácticas para configurar y mantener tu Three-Wallet Model®

Complemento de The Three-Wallet Model®: guía práctica, Edición 2026

Crypto Safety First

CryptoSafetyFirst.com

Tu Three-Wallet Model® de un vistazo

El Three-Wallet Model® (Modelo de Tres Billeteras) separa tu actividad cripto en tres billeteras con propósitos y niveles de exposición distintos.

El objetivo es sencillo: no expongas todo lo que tienes a los mismos riesgos.

Billetera Bóveda

Propósito: almacenamiento a largo plazo y máxima protección.

Usa tu Bóveda para los activos cripto que no necesites para transacciones habituales.

Lo esencial de la configuración

- Usa una billetera de hardware (hardware wallet).
- Compra el dispositivo directamente en la tienda oficial del fabricante. Nunca uses un dispositivo que llegue ya configurado, con un PIN o con una frase semilla (frase de recuperación) incluida.
- Revisa el embalaje y el dispositivo en busca de señales de manipulación.
- Guarda tu frase semilla de forma segura sin conexión (offline).
- Para tus fondos importantes, guarda más de una copia de seguridad (backup) física protegida.
- Haz una prueba de recuperación **antes de cargar la Bóveda**.
- Si usas una passphrase, inclúyela en la planificación de tu recuperación.
- Ningún agente de soporte legítimo, sitio web ni aviso inesperado te pedirá nunca tu frase semilla: quien lo haga es un estafador. Introduce la frase semilla de una billetera de hardware solo en el propio dispositivo.

Mantén tu Bóveda aislada:

No conectes la Bóveda directamente a DApps ni la uses para transacciones rutinarias.

Billetera de Uso Frecuente

Propósito: actividad cripto habitual con exposición controlada.

Úsala para transferencias rutinarias, DApps consolidadas y otra actividad Web3 habitual.

Lo esencial de la configuración

- Guarda solo la cantidad necesaria para tu actividad habitual.
- Haz una copia de seguridad segura de la frase semilla.
- Guarda las direcciones de confianza en una libreta de direcciones, si tu billetera la admite.
- Nunca copies una dirección de destino del historial de transacciones.
- Lee lo que firmas.
- Revisa y revoca las aprobaciones de tokens que ya no necesites.

Piensa en ella como tu billetera de trabajo:

Debe contener lo suficiente para tu actividad normal, pero no tus fondos a largo plazo.

Billetera Desechable

Propósito: aislar la actividad temporal o de mayor riesgo.

Úsala para DApps desconocidas, mints nuevos, airdrops y otras interacciones en las que quieras una separación adicional de tus billeteras principales.

Lo esencial de la configuración

- Guarda solo la cantidad necesaria para la interacción prevista.
- Lee lo que firmas.
- Evita las aprobaciones de tokens innecesarias o ilimitadas.
- Revoca las aprobaciones después de la interacción, cuando corresponda.
- Sustituye la billetera cuando haya cumplido su propósito o después de exponerla a algo que no sea de confianza.

Recuerda:

Una billetera Desechable puede limitar lo que queda expuesto. No hace que una transacción de riesgo sea segura.

El modelo en una línea

Bóveda → proteger | Uso Frecuente → operar | Desechable → aislar

La fortaleza del Three-Wallet Model® está en mantener separadas estas funciones y en conservarlas así a lo largo del tiempo.

Registro de metadatos de billeteras

Usa este registro para llevar el control de tus billeteras sin anotar información de recuperación sensible.

Nunca anotes en este registro tu frase semilla, tu clave privada, tu PIN ni tu passphrase.

Información de la billetera

Etiqueta de la billetera	Tipo de billetera	Dirección pública (completa)	Dispositivo / billetera	Red(es)

Registro de recuperación y propósito

Etiqueta de la billetera	Propósito	Fecha de creación	Tipo de copia	Ubicación de la copia

Etiqueta de la billetera	Propósito	Fecha de creación	Tipo de copia	Ubicación de la copia

Conexiones y aprobaciones

Etiqueta de la billetera	DApps / herramientas conectadas	Aprobaciones de tokens activas	Última revisión

Recordatorio de seguridad

Guarda este registro separado de tus copias de seguridad. Describe las ubicaciones de las copias de forma que solo tú y tus herederos las entiendan.

No anotes información que pueda usarse para acceder a tus cripto o recuperarlas, como frases semilla, claves privadas, PIN o passphrases.

Tabla de planificación de copias de seguridad

Usa esta hoja de trabajo para documentar **cómo están protegidas las copias de seguridad de tus billeteras y dónde están guardadas**. No escribas en esta tabla la frase semilla, la clave privada ni la passphrase en sí. Multisig (multifirma): anota también dónde está la copia del archivo de configuración de la billetera (descriptor); es posible que las claves por sí solas no permitan restaurar la billetera.

Billetera	Objetivo de la copia	Método de almacenamiento	Número de copias	Ubicación(es) de las copias	Última comprobación
Bóveda	Proteger el acceso y la recuperación a largo plazo				
Uso Frecuente	Mantener un acceso seguro para la recuperación				
Desechable	Recuperación solo si se necesita para su uso previsto				

Revisión de las copias

Para cada billetera importante, confirma:

1. Sé dónde está guardada la copia.
2. La copia es legible y está protegida físicamente.
3. Las billeteras importantes tienen más de una copia física protegida.
4. Las copias no están guardadas juntas en un lugar donde un solo incidente pueda destruirlas o exponerlas todas.
5. No he guardado frases semilla ni claves privadas en este Toolkit (kit de herramientas).
6. Mi información de recuperación es comprensible para la persona que pueda necesitarla en una emergencia.

Importante

Una copia de seguridad solo sirve si funciona cuando la necesitas. Mantenla protegida y accesible cuando se necesite legítimamente, y revísala con regularidad. Guarda más de una copia física protegida de tus billeteras importantes.

Lista de verificación de mantenimiento trimestral

Completa esta lista de verificación **cada tres meses** para mantener tu Three-Wallet Model® organizado y seguro.

Comprobación	Acción	Hecho
Inspección de las copias	Comprueba que las copias de seguridad de tus billeteras siguen siendo legibles, están seguras y están guardadas en las ubicaciones previstas.	☐
Aprobaciones de tokens	Revisa las aprobaciones de tokens activas y revoca los permisos que ya no necesites.	☐
Software de billeteras	Actualiza las aplicaciones de billetera, las extensiones del navegador y las aplicaciones móviles a sus últimas versiones desde la tienda oficial.	☐
Billeteras de hardware	Comprueba si hay actualizaciones de firmware relevantes y obtenlas solo a través de los canales oficiales.	☐
Billeteras Desechables	Revisa tus billeteras Desechables y da de baja las que ya no necesites o que hayan cumplido su propósito.	☐
Avisos de seguridad	Consulta los avisos de seguridad oficiales de las billeteras, los dispositivos y los servicios que usas.	☐
Higiene de seguridad	Revisa tus prácticas con las billeteras y corrige cualquier hábito que haya aumentado la exposición sin necesidad.	☐
Conexiones con DApps	Desconecta tus billeteras de las DApps que ya no uses.	☐

Registro de la revisión trimestral

Fecha de revisión	Problemas detectados	Acciones realizadas	Próxima revisión

Importante: instala las aplicaciones de billetera, las extensiones del navegador y las actualizaciones solo desde fuentes oficiales.

Lista de verificación de mantenimiento semestral

Completa esta lista de verificación **cada seis meses** para asegurarte de que tu Three-Wallet Model® sigue reflejando cómo usas realmente tus cripto.

Revisión semestral

Comprobación	Acción	Hecho
Inventario de billeteras	Revisa tu inventario de billeteras y confirma que cada billetera sigue correctamente identificada y etiquetada.	☐
Propósito de cada billetera	Confirma que cada billetera Bóveda, de Uso Frecuente y Desechable se sigue usando para su propósito previsto.	☐
Registro de metadatos	Actualiza tu Registro de metadatos de billeteras con las billeteras creadas, sustituidas o dadas de baja desde la revisión anterior.	☐
Billeteras nuevas	Asegúrate de que todas las billeteras nuevas estén debidamente documentadas y tengan copia de seguridad cuando sea necesario.	☐
Preparación para la herencia	Comprueba si una persona de confianza podría localizar y entender la información necesaria en una emergencia sin exponer innecesariamente tus activos hoy.	☐

Registro de la revisión semestral

Fecha de revisión	Cambios necesarios	Acciones realizadas	Próxima revisión

Lista de verificación de mantenimiento anual

Completa esta lista de verificación una vez al año para confirmar que tu Three-Wallet Model® sigue siendo recuperable, está bien documentado y es adecuado para tu situación actual.

Revisión anual

Comprobación	Acción	Hecho
Proceso de recuperación	Recorre un proceso de recuperación completo para confirmar que tu plan de recuperación es claro y utilizable: con una billetera de hardware, solo en el propio dispositivo (comprobación de copias integrada), nunca introduciendo la frase semilla en un teléfono, un equipo, un sitio web o una aplicación.	☐
Ubicaciones de las copias	Revisa las ubicaciones de tus copias y confirma que siguen siendo seguras, accesibles cuando se necesiten legítimamente y debidamente separadas.	☐
Cambios personales	Valora si los cambios en tu familia, tu lugar de residencia o tus circunstancias personales requieren actualizar tus disposiciones de recuperación o de herencia.	☐
Billeteras sin uso	Identifica las billeteras que ya no necesitas y decide si deben darse de baja.	☐
Dispositivos	Revisa los dispositivos de hardware antiguos o sin uso y asegúrate de que no generen riesgos innecesarios de seguridad o de recuperación.	☐
Asignación a la Bóveda	Confirma que los activos a largo plazo están en la Bóveda, no en billeteras de Uso Frecuente ni Desechables.	☐
Documentación	Actualiza los registros de tus billeteras, la información de las copias de seguridad y la documentación de herencia cuando sea necesario.	☐

Registro de la revisión anual

Fecha de revisión	Cambios necesarios	Acciones realizadas	Próxima revisión anual

Recordatorio de recuperación

Un plan de recuperación debe funcionar antes de que ocurra una emergencia. Tu revisión anual es la oportunidad de confirmar que tu documentación, tus copias de seguridad y tus disposiciones de recuperación siguen coincidiendo con tu configuración real de billeteras.

Nunca anotes frases semilla, claves privadas, PIN ni passphrases en este Toolkit.

Si una billetera está comprometida

Actúa rápido, pero sin precipitarte a cometer nuevos errores. Sigue estos pasos en orden, desde un dispositivo de confianza.

1. Detén el daño

- Deja de interactuar con el sitio web, la aplicación o el contrato implicados. Ciérralos y desconecta tu billetera.
- No firmes nada más hasta que sepas qué pasó.
- Si sospechas que hay malware, deja de usar ese equipo o teléfono para cripto. Usa un dispositivo limpio para los pasos siguientes.

2. Averigua qué quedó expuesto

Qué pasó	Qué significa
Firmaste una aprobación o transacción maliciosa	Trata la billetera como comprometida: algunas firmas (delegaciones de cuenta, cambios de propietario o de permisos) dan al atacante el control total de la billetera, no solo de los tokens aprobados.
Introdujiste tu frase semilla en un sitio web o en una aplicación, o la compartiste	La billetera está comprometida de forma permanente, y también todas las cuentas creadas a partir de esa frase semilla.
Tu dispositivo puede estar infectado	Trata como comprometidas todas las billeteras de software de ese dispositivo.

3. Protege lo que queda

- **Aprobación o firma maliciosa: primero traslada los fondos restantes a una billetera nueva con una frase semilla nueva. Revoca las aprobaciones en la dirección antigua solo si tienes que seguir usándola.**
- **Frase semilla expuesta o dispositivo infectado:** crea una billetera nueva con una frase semilla nueva en un dispositivo limpio. Traslada allí los activos que queden. Nunca vuelvas a usar la frase semilla antigua.
- No envíes fondos a una billetera comprometida para pagar comisiones. Los bots automatizados pueden llevárselos en segundos.
- **Tu Bóveda:** una billetera de hardware sigue segura siempre que su frase semilla nunca se haya introducido ni guardado en el dispositivo afectado. Aun así, confirma cada acción en la pantalla del dispositivo. Si la frase semilla de la Bóveda quedó expuesta alguna vez, traslada sus activos a una Bóveda nueva.
- **Billetera Desechable:** abandónala. No la reutilices.

4. Protege tus cuentas

- Desde un dispositivo limpio, cambia las contraseñas de tus cuentas de exchange (plataforma de intercambio) y de correo electrónico, y revisa su configuración de 2FA.

- Revisa tus cuentas de exchange en busca de direcciones de retiro o inicios de sesión desconocidos.

5. Registra y denuncia

- Anota la fecha, las direcciones de billetera implicadas, los ID de transacción y los sitios web o contactos utilizados. Haz capturas de pantalla.
- Si los fondos llegaron a un exchange, ponte en contacto con ese exchange de inmediato y proporciónale los ID de transacción. Es posible que pueda congelarlos.
- Denuncia el robo ante la policía o el servicio nacional de denuncia de ciberdelitos de tu país.

6. Cuidado con las estafas de recuperación

Después de una pérdida, los estafadores suelen ponerse en contacto con las víctimas y ofrecerse a recuperar los fondos: "expertos en recuperación", abogados falsos, autoridades falsas o "investigadores de blockchain".

- Nadie puede revertir una transacción de blockchain por ti a cambio de una comisión.
- Nunca pagues por adelantado por una recuperación y nunca compartas tu frase semilla.
- Trata como estafador a cualquiera que se ponga en contacto contigo primero después de tu pérdida, a menos que lo verifiques mediante datos de contacto oficiales: la policía y los exchanges auténticos nunca piden comisiones, cripto ni tu frase semilla.

7. Reconstruye

- Configura billeteras nuevas siguiendo el Three-Wallet Model® y actualiza tu Registro de metadatos de billeteras.
- Anota qué pasó y qué harás de forma diferente.

© 2025–2026 Juan Pablo Renedo. Todos los derechos reservados. Se puede compartir libremente en su forma completa y sin modificaciones. Three-Wallet Model® es una marca registrada de la UE de Juan Pablo Renedo.

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

Información solo con fines educativos: no constituye asesoramiento financiero, fiscal ni jurídico. En la medida en que lo permita la ley, no se asume ninguna responsabilidad por pérdidas derivadas de su uso; esto no se aplica en casos de dolo, negligencia grave o daños a la vida, la integridad física o la salud.