ZNTRPHY

Manual de uso: generador air-gapped de claves Bitcoin

ZNTRPHY

Manual de uso: generador air-gapped de claves Bitcoin

Gracias por confiar en ZNTRPHY para generar tus claves de Bitcoin. Este manual te va a guiar paso a paso. Léelo completo antes de generar claves que vayan a custodiar fondos reales: hay pasos en los que solo tienes una oportunidad de hacerlo bien.

---

1. Qué es ZNTRPHY y por qué "air-gapped" importa

ZNTRPHY genera semillas Bitcoin (frases de 12 a 24 palabras), passphrases opcionales, y configuraciones de billeteras single-sig o multisig, todo **sin conectarse nunca a internet**.

"Air-gapped" (con espacio de aire) significa que la máquina donde generas tus claves nunca toca una red. Esto importa porque:

- Una clave privada de Bitcoin que nunca existió en una máquina conectada a internet no puede ser robada por malware que intercepte tráfico de red, ni filtrada por una app maliciosa que "llame a casa".
- La mayoría de los robos de fondos de autocustodia no ocurren por romper la criptografía de Bitcoin (eso es prácticamente imposible con los parámetros correctos); ocurren porque la clave privada pasó, en algún momento, por una máquina conectada a internet, o fue tecleada en un sitio falso.

Recomendación fuerte: genera tus claves en una máquina dedicada, arrancada desde un sistema operativo "live" (por ejemplo, Tails o Ubuntu ejecutándose desde un USB, sin instalar nada en el disco) que jamás se conecte a internet. Si no tienes esa posibilidad, como mínimo desconecta el cable de red y apaga el wifi antes de abrir la app.

2. Antes de empezar: verifica que el archivo es genuino

Los estafadores a veces distribuyen copias modificadas de billeteras de Bitcoin con puertas traseras. Antes de ejecutar ZNTRPHY por primera vez:

1. **Verifica el hash SHA-256** del archivo contra el que figura en `packaging/SHA256SUMS.txt` (o el que te haya compartido quien te vendió el producto, por un canal distinto al de descarga del archivo). En macOS/Linux: `shasum -a 256 ZNTRPHY` (o `sha256sum` en Linux). En Windows (PowerShell): `Get-FileHash ZNTRPHY.exe -Algorithm SHA256`.
2. Si el hash no coincide exactamente, **no lo uses**: puede haber sido modificado. Contacta a quien te lo vendió por otro medio para confirmar.
3. Desconfía de copias encontradas en buscadores, foros o enlaces no oficiales: usa siempre el canal de descarga original.

El código fuente completo está incluido junto con este manual precisamente para que tú, o cualquier persona de tu confianza que sepa programar, puedas revisar exactamente qué hace el programa antes de confiarle fondos reales. Ver `SECURITY.md` para instrucciones detalladas de cómo verificar, entre otras cosas, que la app nunca se conecta a internet.

3. Generar una billetera single-sig (una sola clave)

Este es el camino más simple: una sola semilla controla los fondos.

1. Abre la app y elige **"Billetera single-sig"**.
2. **Entropía adicional (opcional).** La app ya usa el generador de números aleatorios seguro del sistema operativo: eso alcanza por sí solo. Si además quieres aportar tiradas de dado o mover el ratón, puedes hacerlo aquí: se combina de forma que **solo puede sumar seguridad, nunca restarla**. Elige también cuántas palabras quieres (24 es lo más seguro; 12 es el mínimo del estándar BIP39).
3. **Tu frase semilla.** La app te muestra las palabras numeradas. **Anótalas a mano, en papel (o metal), en el orden exacto.** Nunca las escribas en un ordenador, no las fotografíes con el móvil, no las subas a ningún servicio en la nube, no se las envíes a nadie por ningún medio digital. Quien tenga estas palabras controla los fondos, sin excepción: ni tú vas a poder recuperar el acceso si las pierdes.
4. **Passphrase opcional ("palabra 25").** Es una capa extra de protección: incluso si alguien encuentra tus palabras anotadas, sin esta passphrase no puede acceder a los fondos. Es completamente opcional, pero si la activas, anótala **en un lugar distinto** de donde anotaste las palabras, y ten en cuenta que si la olvidas, los fondos se pierden para siempre. No hay forma de recuperarla: ni la app, ni nosotros, ni nadie puede.
5. **Resumen.** Vas a ver el fingerprint de tu clave, el xpub de la cuenta, los descriptors de recepción y cambio, y un par de direcciones de ejemplo. **Importa el descriptor de recepción en tu wallet** (Sparrow, Electrum, o la que uses) y confirma que las direcciones que genera coinciden con las que te muestra ZNTRPHY, antes de recibir fondos reales.

4. Generar una billetera multisig (varias claves)

Un multisig necesita `m` de n firmas para gastar fondos (por ejemplo, "2 de 3"). Hay dos formas de armarlo:

Modo coordinador (recomendado)

Cada vez que ejecutas la app en este modo, se genera **un solo firmante**. Para armar el multisig final, reúnes la información **pública** (nunca la semilla) de cada firmante.

1. Elige **"Billetera multisig"** → **"Generar un firmante ahora"**.
2. Sigue los mismos pasos que en single-sig (entropía, semilla, passphrase). Esta semilla es la de ESTE firmante únicamente.

3. La app te muestra un bloque de texto con el fingerprint, el xpub y la ruta de derivación de este firmante: **esto es lo único que hace falta compartir** con quien va a ensamblar el multisig. Cópialo o guárdalo en un archivo de texto.
4. Repite este proceso una vez por cada firmante que necesites (en ejecuciones separadas y, si es posible, en máquinas separadas para cada persona o dispositivo).
5. En la pantalla de **"Ensamblar multisig"**, pega la información pública de cada firmante, elige cuántas firmas hacen falta (`m`), y la app arma el descriptor final `wsh(sortedmulti(...))`.

Con este modo, **ninguna ejecución individual de la app llega a ver más de una semilla**: es la forma más segura si los firmantes son personas o dispositivos distintos.

Modo conveniencia

Genera **todas** las semillas de una sola vez, en la misma ejecución. Útil solo si una única persona controla todos los dispositivos o firmantes (por ejemplo, tus propios tres ordenadores o hardware wallets). **No lo uses** si los firmantes son personas distintas que no deberían compartir la misma máquina: en ese caso, una máquina comprometida vería todas las semillas generadas, aunque sea de forma transitoria.

5. Completar una semilla generada a mano

Si generaste tus propias palabras por tu cuenta (por ejemplo, tirando dados físicos y usando tu propia tabla de conversión) y te falta la última palabra, la pantalla **"Completar semilla"** (accesible desde el inicio) la calcula por ti.

Cómo funciona: en una semilla BIP39, la última palabra no es completamente libre, una parte de sus bits es un checksum matemático que depende de todas las palabras anteriores. Dadas las primeras N-1 palabras (por ejemplo, 23 de 24), solo hay un puñado de palabras finales que dan un checksum válido (8 en el caso de 24 palabras). La app calcula esas opciones y te deja elegir una (o elegir una al azar, con el mismo generador seguro que usa el resto de la app).

Importante: esto no recupera una semilla perdida ni ajena. Solo funciona si ya tienes tus propias N-1 palabras, reales y en el orden correcto. No genera entropía nueva por sí sola, ni sirve para adivinar una semilla que no sea tuya.

Una vez elegida la palabra final, puedes continuar el mismo flujo que si la hubieras generado normalmente: como billetera single-sig, o como firmante de un multisig.

6. Verificar tu backup

Antes de confiar fondos reales a cualquier billetera generada aquí:

1. Anota las palabras exactamente como se muestran, en el orden mostrado.
2. Vuelve a leerlas en voz alta comparando con lo anotado, palabra por palabra.
3. Importa el descriptor (single-sig o multisig) en una wallet de buena reputación (Sparrow Wallet, Electrum) y confirma que las direcciones generadas coinciden con las que muestra ZNTRPHY.

4. Considera probar primero con un monto pequeño antes de mover fondos grandes, sobre todo la primera vez que usas un multisig.

ZNTRPHY Verify (la app web/móvil que acompaña al producto) sirve para esta misma comprobación desde el móvil: pegas el descriptor público (nunca la semilla) y confirmas que las direcciones coinciden, sin necesidad de instalar una wallet completa. Al igual que la app de escritorio, nunca pide ni maneja semillas.

7. Exportar cifrado con PIN

Desde la pantalla de resumen puedes exportar la información a un archivo, protegido con un PIN que tú eliges (cifrado con Argon2id y AES-256-GCM).

- El PIN **no reemplaza** anotar la semilla a mano: es una capa adicional para quien además quiera un respaldo digital cifrado.
- Guarda el PIN en un lugar **distinto** de donde guardas el archivo exportado.
- Si pierdes el PIN, el archivo es inútil: ni la app puede ayudarte a recuperarlo.
- Nada se escribe a disco hasta que llegas a esta pantalla y confirmas explícitamente la exportación.

8. Avisos de phishing y copias falsas

- Verifica siempre el hash del archivo (sección 2) antes de usarlo.
- ZNTRPHY **nunca** te va a pedir tu semilla, tu passphrase, ni tu PIN por ningún canal (email, chat, redes sociales, formulario web). Si alguien te lo pide haciéndose pasar por el vendedor o por soporte, es un intento de estafa.
- Esta app no tiene ninguna función de "recuperación en la nube" ni "sincronización": cualquier oferta de ese tipo relacionada con el producto es falsa.
- Descarga siempre desde el canal oficial que te indicó quien te vendió el producto, nunca desde un enlace de búsqueda o de un tercero.

9. Preguntas frecuentes

¿Puedo usar ZNTRPHY en una máquina con internet? Técnicamente sí, la app funciona igual, pero para máxima seguridad, la recomendación es siempre generar claves en una máquina desconectada de la red.

¿Qué pasa si pierdo mis palabras semilla? Pierdes el acceso a los fondos para siempre. No hay forma de recuperarlas: ni ZNTRPHY, ni nosotros, ni nadie.

¿Puedo agregar más firmantes a un multisig después de crearlo? No: el número de firmantes (n) y el umbral (`m`) de un multisig se fijan al crearlo. Para cambiarlos hace falta crear un multisig nuevo y mover los fondos.

¿Esta app guarda algo en internet o en la nube? No, nunca. Ver `SECURITY.md` para cómo verificar esto tú mismo.

Este manual y el software que acompaña se entregan sin garantías más allá de las que la ley exija. La responsabilidad de resguardar tus palabras semilla, tu passphrase y tu PIN es exclusivamente tuya.
