

Plantilla de Guía Para Acceder a Mis Bitcoins (Plan de Herencia)

“Esta es una plantilla creada por la comunidad Barcelona Bitcoin Only. Personalízala con tus propios datos y configuración. Todo el texto en [CORCHETES] debe ser reemplazado con tu información personal.

Querida familia:

He preparado esta guía para ayudarles a acceder a mis bitcoins en caso de que yo no esté disponible. Este documento contiene información muy valiosa que les permitirá acceder a un patrimonio digital que he ido construyendo con el tiempo.

Bitcoin es un tipo especial de dinero digital que, a diferencia de propiedades, efectivo o cuentas bancarias:

- No depende de terceros como bancos o gobiernos
- Puede transferirse fácilmente sin importar fronteras o distancias
- Es resistente a la inflación porque tiene una cantidad limitada (solo existirán 21 millones)
- Ha funcionado de manera ininterrumpida desde 2009, demostrando su durabilidad

Lo más importante que deben entender es que **las semillas (palabras secretas) son la verdadera llave de acceso a los bitcoins**, no las aplicaciones o billeteras que se usan para verlos. Este documento les explicará cómo usar estas "llaves" para acceder a este patrimonio digital.

Consideraciones Importantes

- **Las palabras semilla son como llaves de una caja fuerte:** Quien tiene estas palabras, tiene acceso completo a los fondos.
- **Nunca compartan estas palabras con nadie.**

- **No tomen fotos de las palabras semilla.**
- **No guarden estas palabras en documentos digitales, emails o en la nube.**
- **Actúen con calma y sin prisa cuando sigan estas instrucciones.**
- **Responsabilidad:** Con Bitcoin, ustedes son los únicos responsables de sus fondos. No hay servicio al cliente ni forma de recuperar acceso si pierden las semillas.

Nota Importante sobre la Naturaleza de esta Herencia

Este plan de herencia funciona fuera del sistema financiero tradicional. Es importante que entiendan que:

1. **No involucra instituciones financieras ni abogados:** Los bitcoins se transfieren directamente a ustedes a través del conocimiento que proporciona esta guía.
2. **Comunidad como recurso:** Si necesitan ayuda, la comunidad Bitcoin puede ser más valiosa que asesores tradicionales. Les recomiendo que conozcan a otros bitcoiners y asistan a grupos locales.
3. **Compromiso necesario:** Entender y gestionar bitcoin requiere cierto esfuerzo y aprendizaje de su parte. Este "regalo" viene con la responsabilidad de aprender lo básico para manejarlo adecuadamente.

Estructura de Mis Bitcoins (*sistema ideal!*)

He organizado mis bitcoins en tres niveles de seguridad diferentes según las semillas que los protegen:

Nivel 1: Semilla Básica (Acceso Rápido)

Esta semilla protege cantidades menores de bitcoin para uso cotidiano.

Lo que necesitarán:

- El respaldo metálico de la semilla de Nivel 1 (ubicado en [UBICACIÓN_SEGURA_1])

Datos específicos de esta semilla:

- **Master Fingerprint:** [FINGERPRINT_NIVEL_1] (ejemplo: 3ab4c7d9)
- **Derivation Path:** m/84'/0'/0'
- **XPUB:** [XPUB_NIVEL_1] (ejemplo:
xpub6CzDREPtPt5vqyMT9U5TxUR6KtHBsVBqzWKMrMKx8qWQoqVZF...)

Nivel 2: Semilla con Passphrase (Seguridad Mejorada)

Esta semilla protege cantidades mayores y tiene una capa adicional de seguridad mediante una passphrase.

Lo que necesitarán:

- El respaldo metálico de la semilla de Nivel 2 (ubicado en [UBICACIÓN_SEGURA_2])
- La passphrase adicional (guardada en [UBICACIÓN_PASSPHRASE] o memorizada por [PERSONA_DE_CONFIANZA_1])
- [OPCIONAL: Mi hardware wallet modelo X] (ya tiene la semilla cargada)

Datos específicos de esta semilla:

- **Master Fingerprint:** [FINGERPRINT_NIVEL_2] (ejemplo: 2cb8a3f5)
- **Derivation Path:** m/84'/0'/0'
- **XPUB:** [XPUB_NIVEL_2] (ejemplo: xpub6BmTPtYQZ81MR7Jx4ajVzRh9N...)
- **NOTA:** La passphrase crea una wallet completamente diferente a partir de la misma semilla. Sin la passphrase correcta, no verán los fondos.

Nivel 3: Multisig 2-de-3 (Máxima Seguridad)

Este nivel utiliza tres semillas diferentes, requiriendo al menos dos de ellas para mover los fondos. Aquí es donde guardo la mayor parte de mis bitcoins.

Lo que necesitarán:

- Acceso a al menos 2 de las 3 semillas (respaldos metálicos ubicados en [UBICACIONES_MULTISIG])
- El descriptor multisig (incluido más adelante en esta guía)

Datos específicos de la configuración Multisig:

- **Tipo:** P2WSH (Native Segwit Multisig)

- **Descriptor completo:**

```
wsh(sortedmulti(2,[FINGERPRINT_MS1/48'/0'/0'/2']xpub...[XPUB_MS1]/*,[FINGERPRINT_MS2/48'/0'/0'/2']xpub...[XPUB_MS2]/*,[FINGERPRINT_MS3/48'/0'/0'/2']xpub...[XPUB_MS3]/*)
```

Detalles de las 3 semillas para multisig:

1. Semilla 1:

- **Ubicación del respaldo:** [UBICACIÓN_MS1]
- **Master Fingerprint:** [FINGERPRINT_MS1] (ejemplo: a1b2c3d4)
- **Derivation Path:** m/48'/0'/0'/2'
- **XPUB:** [XPUB_MS1] (ejemplo truncado para ilustración: xpub6ERApf...)

2. Semilla 2:

- **Ubicación del respaldo:** [UBICACIÓN_MS2]
- **Master Fingerprint:** [FINGERPRINT_MS2] (ejemplo: e5f6g7h8)
- **Derivation Path:** m/48'/0'/0'/2'
- **XPUB:** [XPUB_MS2]

3. Semilla 3:

- **Ubicación del respaldo:** [UBICACIÓN_MS3]
- **Master Fingerprint:** [FINGERPRINT_MS3] (ejemplo: i9j0k1l2)
- **Derivation Path:** m/48'/0'/0'/2'
- **XPUB:** [XPUB_MS3]

Recuperación de Fondos: Principios Generales

Para recuperar el acceso a los bitcoins, necesitarán seguir estos principios generales, independientemente del software que utilicen:

Para semillas individuales (Nivel 1 y 2)

1. Instalar una billetera Bitcoin:

- Busquen una billetera de Bitcoin confiable y actualizada de la época.
- Las billeteras duraderas incluyen Electrum, Sparrow, y Blue Wallet, pero podrían surgir otras mejores en el futuro.
- Si estas ya no existen, busquen billeteras que admitan el estándar BIP39 (semillas de 12/24 palabras).

2. Crear/restaurar una billetera:

- Elijan la opción de "restaurar desde semilla" o "importar billetera".
- Introduzcan las palabras semilla del respaldo metálico correspondiente.

- Para el Nivel 2, asegúrense de añadir la passphrase cuando se les solicite.

3. **Configuración técnica:**

- Si se les pide un tipo de billetera, elijan "Native Segwit" (también conocido como P2WPKH o BIP84).
- La ruta de derivación debería ser: m/84'/0'/0' para bitcoins individuales.
- Si tienen problemas, pueden usar los datos específicos (XPUB, Fingerprint) que proporcioné para cada nivel.

Para la configuración multisig (Nivel 3)

1. **Instalar una billetera compatible con multisig:**

- Necesitarán un software que admita configuraciones multisig como Sparrow, Electrum o equivalentes futuros.

2. **Crear la billetera multisig:**

- Elijan una opción como "Restaurar desde descriptor" si está disponible.
- Alternativamente, creen una nueva billetera multisig 2-de-3.
- Para cada semilla que tengan disponible, impórtela con la ruta de derivación m/48'/0'/0'/2'.
- Para cualquier semilla que falte, utilicen el XPUB correspondiente de la lista.

3. **Verificación:**

- Confirman que la billetera muestra el saldo esperado.
- Deberían poder ver el historial de transacciones.

Verificación de Software: Evitar Malware y Phishing

Este es un paso crítico que muchas personas omiten. El software malicioso diseñado para robar bitcoins es cada vez más sofisticado, por lo que deben asegurarse de descargar aplicaciones legítimas:

Verificación de Integridad del Software

1. **Usar fuentes oficiales:**

- Siempre descarguen software de los sitios web oficiales, nunca de enlaces en correos electrónicos o mensajes.
- Verifiquen que la URL sea correcta y esté utilizando HTTPS (candado en el navegador).

2. **Verificación de firmas digitales:**

- Las billeteras Bitcoin legítimas proporcionan firmas digitales para verificar la autenticidad del software.
- Proceso básico de verificación (varía según el software):
 - Descarguen el archivo de instalación Y el archivo de firma (normalmente con extensión .asc o .sig).
 - Descarguen e instalen GnuPG (o herramienta equivalente de la época).
 - Importen la clave pública del desarrollador.
 - Ejecuten el comando de verificación (ejemplo para Sparrow: `gpg --verify sparrow-x.x.x.jar.asc sparrow-x.x.x.jar`).
 - Confirмен que la verificación sea exitosa.

3. Verificación de hashes:

- Alternativamente, pueden verificar el hash (huella digital) del archivo:
 - Descarguen el hash oficial junto con el software.
 - Calculen el hash del archivo descargado.
 - Comparen que ambos coincidan exactamente.

4. Red Tor para mayor seguridad:

- Consideren usar el navegador Tor para descargar software sensible.
- Algunos desarrolladores proporcionan sitios .onion oficiales (por ejemplo, `electrum6noe2dc.onion` para Electrum).

5. Señales de advertencia:

- Software que solicita las 24 palabras inmediatamente.
- Aplicaciones que piden enviar fondos a una dirección para "activar" la wallet.
- Pop-ups o advertencias inusuales durante la instalación.
- Versiones gratuitas de software de pago.

Recuerden: Nunca introduzcan sus semillas en un dispositivo comprometido. En caso de duda, utilicen un sistema operativo limpio o una billetera hardware.

Almacenamiento Seguro de Esta Guía

Este documento contiene información sensible que podría comprometer la seguridad de sus bitcoins si cae en manos equivocadas. Siguen estas recomendaciones para su almacenamiento:

Opciones de Almacenamiento Físico

1. Caja de seguridad personal:

- Guarden una copia impresa en una caja fuerte resistente al fuego.
- La caja debe estar anclada o ser lo suficientemente pesada para evitar su sustracción.

- Consideren guardar este documento separado de las semillas para minimizar riesgos.

2. **Protección contra elementos:**

- Utilicen papel archival de alta calidad (no se amarillenta con el tiempo).
- Consideren laminación de alta calidad o mangas protectoras.
- Almacenen en contenedores sellados con sobres de gel de sílice para proteger contra la humedad.

3. **Opción avanzada - Grabado en metal:**

- Para máxima durabilidad, consideren grabar información crítica en placas de acero inoxidable o titanio.
- Estas placas resisten fuego, agua y deterioro por tiempo.
- Productos comerciales como Cryptosteel o placas grabadas a láser pueden ser opciones.

Control de Acceso

1. **Lista de custodios confiables:**

- Identifiquen claramente quién debe tener acceso a esta guía.
- Establezcan condiciones específicas bajo las cuales se debe acceder.
- Consideren requerir múltiples custodios para acceder a la información completa.

2. **Instrucciones legales:**

- Incluyan referencias a este documento en su testamento sin revelar el contenido completo.
- Su abogado puede mantener instrucciones selladas sobre cómo acceder a esta guía.

3. **Actualización periódica:**

- Revisen y actualicen este documento al menos una vez al año.
- Documenten la fecha de la última actualización.
- Reemplacen todas las copias anteriores cuando realicen actualizaciones.

Nota importante: A diferencia de las semillas, este documento puede ser reemplazado si se pierde. Sin embargo, contiene información sensible que debe protegerse adecuadamente.

Ejemplos con Software Actual (2025)

A continuación incluyo ejemplos usando software disponible actualmente. Aunque estas aplicaciones podrían no existir en el futuro, los principios y pasos son similares para cualquier software compatible con Bitcoin.

Ejemplo con Sparrow Wallet

1. Instalación:

- Descargar de sparrowwallet.com o usar un instalador confiable para su sistema.
- Actualmente (2025) la versión estable es 2.1.3.

2. Para semillas individuales:

- Seleccionar "File" > "New Wallet" o en la pantalla inicial "New Wallet".
- Nombrar la wallet (ejemplo: "Nivel1" o "Nivel2-Con-Passphrase").
- Elegir "New or Imported Software Wallet" y luego "Restore wallet from seed words".
- Introducir las palabras semilla.
- Para el Nivel 2, marcar "BIP39 Passphrase" e introducir la passphrase.
- Seleccionar "Native Segwit (P2WPKH)" como tipo de script.

3. Para multisig:

- Crear una nueva wallet y nombrarla.
- Seleccionar "Policy Type" > "Multi Signature".
- Configurar como "2 of 3".
- Para cada semilla disponible:
 - Seleccionar "Keystores" > "Import Keystore".
 - Elegir "From seed words" e introducir las palabras.
 - Usar la ruta de derivación `m/48'/0'/0'/2'`.
- Para semillas no disponibles:
 - Seleccionar "Keystores" > "Add Keystore" > "Watch Only".
 - Pegar el X PUB y el fingerprint correspondientes.

Ejemplo con Billetera Móvil (BlueWallet)

1. Instalación:

- Descargar desde la App Store o Google Play.

2. Para semillas individuales:

- Seleccionar "Añadir billetera" > "Importar billetera".
- Introducir las palabras semilla.
- Para el Nivel 2, añadir la passphrase cuando se solicite.

Procedimientos de Recuperación en Caso de Pérdida Parcial

Puede darse el caso de que no tengan acceso a todos los componentes del sistema (semillas, passphrase, etc.). Aquí les comparto procedimientos de recuperación para diferentes escenarios:

Si Pierden la Passphrase del Nivel 2

1. **Todavía tienen acceso a los fondos del Nivel 1 y Nivel 3:**

- Prioricen asegurar estos fondos primero, moviéndolos a nuevas billeteras si es necesario.
- Para los fondos del Nivel 2, si no pueden recordar o recuperar la passphrase, consideren estos enfoques:
 - Prueben variaciones comunes que yo podría haber usado (fechas importantes, frases significativas).
 - Consulten con [PERSONA DE CONFIANZA] quien puede conocer la passphrase.
 - Busquen en [UBICACIÓN ALTERNATIVA] donde podría haber dejado una pista.

Si Solo Tienen Acceso a Una Semilla del Multisig (Nivel 3)

1. **Necesitarán encontrar al menos una semilla más:**

- Consulten las ubicaciones de respaldo listadas para cada semilla.
- Si las ubicaciones físicas son inaccesibles, contacten a [CONTACTO DE EMERGENCIA] quien puede tener acceso a una copia de respaldo.

2. **Utilicen los XPUBs para verificación:**

- Aunque no puedan mover los fondos con un solo seed, pueden usar el XPUB correspondiente para verificar el saldo disponible.
- En Sparrow o Electrum, creen una billetera multisig "watch-only" usando los XPUBs proporcionados.

3. **Procedimiento de última instancia:**

- Si solo pueden recuperar una semilla y no hay forma de acceder a las otras, existe un plan de contingencia:
 - Contacten a [PERSONA DE CONFIANZA ADICIONAL] quien tiene instrucciones específicas para esta situación.
 - Alternativamente, busquen en [UBICACIÓN SECRETA ADICIONAL] donde he dejado instrucciones complementarias.

Si Pierden o Dañan los Respaldos Metálicos

1. **Respaldos secundarios:**

- He creado respaldos adicionales de las semillas que están ubicados en:
 - Semilla Nivel 1: Respaldo en [UBICACIÓN ALTERNATIVA 1]
 - Semilla Nivel 2: Respaldo en [UBICACIÓN ALTERNATIVA 2]

- Semillas Multisig: Respaldos en [UBICACIONES ALTERNATIVAS 3, 4, 5]

2. **Recuperación desde dispositivos:**

- Si los respaldos metálicos se han perdido pero aún tienen acceso a mis dispositivos:
 - La ColdCard MK4 contiene la semilla del Nivel 2 (requerirá el PIN: [PISTA PARA EL PIN])
 - El dispositivo [OTRO HARDWARE WALLET] contiene la semilla 1 del multisig (requerirá el PIN: [PISTA PARA EL PIN])

Si El Software Recomendado Ya No Existe

1. **Principios universales:**

- Recuerden que cualquier software que cumpla con los estándares BIP39, BIP44, BIP49 y BIP84 debería funcionar.
- Las rutas de derivación (m/84'/0'/0' para single-sig y m/48'/0'/0'/2' para multisig) son estándares que deberían mantenerse a largo plazo.

2. **Comunidad Bitcoin:**

- Busquen ayuda en comunidades Bitcoin activas de la época.
- Las semillas BIP39 son un estándar que probablemente se mantendrá compatible por décadas.

Firmando Transacciones

Con Hardware Wallet (ColdCard)

Si están usando mi ColdCard MK4:

1. Conectarla a un powerbank (nunca a una computadora).
2. Introducir el PIN.
3. Para el Nivel 2, añadir la passphrase.
4. Usar una tarjeta microSD para transferir la transacción a firmar.
5. Firmar la transacción en la ColdCard.
6. Devolver la microSD a la computadora para transmitir la transacción.

Con Software Wallet

1. Crear la transacción en el software elegido.
2. Para el Nivel 3 (multisig), necesitarán firmar con al menos 2 de las 3 semillas.
3. Verificar cuidadosamente todos los detalles antes de transmitir.

Conexión a Servidores Bitcoin (Nivel Experto)

Para mayor privacidad, pueden conectarse a servidores Bitcoin confiables como los que proporciona Barcelona Bitcoin Only (BBO):

1. Servidor Fulcrum de BBO:

- **Dirección Clearnet:** `electrum.bitcoinbarcelona.xyz`
- **Puerto SSL:** 50002
- **Dirección Tor:**
`u5pfxxolpw5togyg2pc5gpzoo4mzevo5yzthe2cd55haqj7t5hr5phqd.onion`
- **Puerto TCP:** 50001

2. Servidor Fulcrum Personal (si has configurado uno):

- **Dirección:** `[DIRECCIÓN_SERVIDOR_PERSONAL]`
- **Puerto:** `[PUERTO_SERVIDOR_PERSONAL]`
- **Protocolo:** `[PROTOCOLO_SERVIDOR_PERSONAL]`

Servicios adicionales de BBO que pueden ser útiles:

- **Mempool:** `https://mempool.bitcoinbarcelona.xyz/` Útil para monitorear transacciones y actividad en la red en tiempo real.
- **BTC Pay Server:** `btcpay.bitcoinbarcelona.xyz/login` (Tor: `yys2j4k6rvtcp7mvpriunsp7cmkr7vvmxktle4l2qjqzto4w7n2mamid.onion/login`) Para comerciantes o individuos que quieran aceptar pagos en Bitcoin.

Contactos de Emergencia

He designado a las siguientes personas como recursos adicionales si necesitan ayuda:

- **[CONTACTO_TÉCNICO]:** Experto en Bitcoin que puede ayudarles con problemas técnicos.
 - Teléfono: `[TELÉFONO_CONTACTO_TÉCNICO]`
 - Email: `[EMAIL_CONTACTO_TÉCNICO]`
- **[CONTACTO_LEGAL]:** Abogado que conoce mi plan de herencia digital.
 - Teléfono: `[TELÉFONO_CONTACTO_LEGAL]`
 - Email: `[EMAIL_CONTACTO_LEGAL]`

Comunidad de soporte: También pueden buscar ayuda en la comunidad Barcelona Bitcoin Only:

- Sitio web: `https://bitcoinbarcelona.xyz`
- Eventos mensuales donde pueden conocer expertos en persona

- Canal Telegram: <https://t.me/BarcelonaBitcoinOnly>

Consideraciones sobre el Valor a Largo Plazo

Bitcoin tiene características que lo hacen especialmente valioso a largo plazo:

1. **Durabilidad del sistema:** El protocolo Bitcoin está diseñado para funcionar sin cambios drásticos, lo que significa que las semillas que les dejo podrán usarse durante muchos años, incluso décadas.
2. **Escasez real:** A diferencia del dinero tradicional que puede imprimirse indefinidamente, Bitcoin tiene un límite fijo de 21 millones. Con el tiempo, esto lo ha convertido en una forma eficaz de preservar valor.
3. **Independencia:** Los bitcoins no dependen de ninguna institución para existir o funcionar. Mientras exista internet (o incluso formas alternativas de comunicación), Bitcoin seguirá funcionando.
4. **Perspectiva generacional:** Bitcoin está diseñado para funcionar mejor cuando se piensa a largo plazo. Con el tiempo, ha demostrado ser más resistente que muchas otras formas de guardar valor.
5. **Comunidad global:** Existe una comunidad mundial dedicada a mantener y mejorar la red Bitcoin. Esta comunidad garantiza que los métodos para acceder a Bitcoin se mantengan disponibles.

Glosario de Términos

- **Seed Phrase:** Las 12 o 24 palabras que representan la clave maestra de una wallet de Bitcoin.
- **Passphrase:** Contraseña adicional que se combina con la seed phrase para crear una nueva wallet derivada.
- **XPUB:** Clave pública extendida que permite verificar fondos pero no gastarlos.
- **Fingerprint:** Identificador único de una clave maestra, útil para verificar la identidad de una semilla.
- **Multisig:** Configuración que requiere múltiples claves para autorizar una transacción.
- **Derivation Path:** Ruta que determina qué direcciones se generan desde una semilla.
- **Descriptor:** Formato estándar que describe completamente una wallet de Bitcoin.
- **PSBT:** Partially Signed Bitcoin Transaction, formato para transacciones multifirma.
- **Airgap:** Método de seguridad donde el dispositivo de firma nunca se conecta a internet.

Consejos Finales

- **Las palabras semilla son lo más importante** - pueden usar cualquier aplicación compatible con ellas para recuperar los bitcoins.
- **Practiquen estos procedimientos** mientras yo esté disponible para ayudarles.
- **Prueben primero con pequeñas cantidades** para asegurarse de que todo funciona correctamente.
- **Guarden esta guía en un lugar seguro** donde solo ustedes puedan acceder.
- **Si tienen dudas, contacten a las personas de confianza** que mencioné anteriormente.
- **Aprendan lo básico sobre Bitcoin:** He dejado algunos libros y recursos que explican los conceptos fundamentales de forma sencilla.
- **Visión a largo plazo:** Bitcoin ha demostrado ser más valioso cuando se mantiene por períodos largos. No se apresuren a venderlo ante las primeras fluctuaciones.

Recuerden que este bitcoin representa no solo valor monetario, sino también independencia financiera. Les permite guardar valor y transferirlo sin depender de intermediarios. Es un patrimonio digital que, bien cuidado, puede beneficiar no solo a ustedes sino potencialmente a las próximas generaciones.

Espero que este legado no se convierta en una carga, sino en una oportunidad para explorar una nueva forma de pensar sobre el dinero y el valor. Si deciden involucrarse más en la comunidad Bitcoin, descubrirán personas que comparten esta visión y pueden ayudarles en su camino.

Con cariño, [TU_NOMBRE]

Notas para completar esta plantilla

Esta sección es solo para ti, elimínala antes de entregar la guía a tu familia.

1. **Seguridad de la información:** Asegúrate de almacenar este documento completo en un lugar muy seguro. Contiene toda la información necesaria para acceder a tus bitcoins.
2. **Reemplaza todos los marcadores:** Cualquier texto entre [CORCHETES] debe ser reemplazado con tu información personal.
3. **Verifica la guía:** Una vez completada, intenta seguir tus propias instrucciones como lo haría alguien sin conocimientos técnicos para comprobar que están claras.
4. **Actualización periódica:** Revisa este documento al menos una vez al año para asegurarte de que sigue siendo válido.
5. **Comunidad Bitcoin:** Considera unirse a Barcelona Bitcoin Only (BBO) para conocer más sobre prácticas de seguridad y soberanía financiera: <https://bitcoinbarcelona.xyz>

Documento creado con la plantilla de Barcelona Bitcoin Only (BBO). Revisión: Abril 2025.

Revision #3
Created 22 April 2025 23:47:54 by Federico
Updated 22 April 2025 23:53:25 by Federico