

LA BASE ANTES DE TU PRIMERA ACCIÓN

Seguridad cripto

Protege el acceso. Revisa las solicitudes.
Decide sin prisas.

30-45 minutos · 6 módulos · 10 preguntas

Todos los ejercicios se realizan en papel. No hacen falta fondos reales, instalar una cartera, conectarla ni firmar.

Ruta de aprendizaje

- 01 Mapa del curso y práctica segura
- 02 1. Carteras, exchanges y control del acceso
- 03 2. Cuentas, phishing y falsa urgencia
- 04 3. Red, activo, dirección y memo
- 05 4. Conectar, firmar y autorizar son acciones distintas
- 06 5. Plan ante incidentes y comprobación final

LOGRI CRYPTO SECURITY · 2026-10-31

01 / 06

Mapa del curso y práctica segura

Qué aprenderás

Al terminar podrás distinguir una dirección pública de un secreto, reconocer una solicitud peligrosa, comprobar una ruta de transferencia en papel y elegir los primeros pasos ante un incidente. Es una base útil antes de START, HOLD, Radar Practice y GameFi. Calcula unos 30-45 minutos con los ejercicios; puedes avanzar por partes.

Lee cada lección, escribe tu propia solución y consulta después la explicación. Los nombres de plataformas A y B, las direcciones como «DIRECCIÓN-A» y los importes de los ejercicios son ficticios. No necesitas instalar una cartera, registrarte en un exchange, conectar una dapp, firmar un mensaje, reclamar tokens ni realizar transferencias. Nunca envíes frases de recuperación, contraseñas, códigos o claves a la Academia.

Tu nota de aprendizaje

Crea cinco filas: qué protejo; quién controla el acceso; qué compruebo antes de actuar; un motivo para detenerme; dónde buscaría ayuda. Anota categorías y decisiones, no secretos reales ni direcciones de tus cuentas. Completa una fila después de cada lección. El resultado será un procedimiento personal que puedas repetir sin indicaciones.

El examen tiene 10 preguntas, incluidos dos ejercicios situacionales obligatorios. Para aprobar necesitas al menos el 70% y ambos ejercicios obligatorios correctos. La lectura y práctica son gratuitas. Inicia sesión en tu cuenta LOGRI verificada para guardar la finalización y obtener un certificado.

Cómo encaja GitBook

La referencia de carteras LOGRI ayuda a encontrar más adelante una guía para la red elegida: <https://gamefi-40.gitbook.io/gamefi-40+-docs/wallets>. La sección de seguridad está en <https://gamefi-40.gitbook.io/gamefi-40+-docs/bezopasnost-i-skam>. Esta referencia opcional está parcialmente en ruso; todas las lecciones obligatorias y el examen se ofrecen aquí en el idioma elegido. No necesitas comprar ni instalar las carteras enumeradas para aprobar.

02 / 06

1. Carteras, exchanges y control del acceso

Identifica primero el modelo de custodia

En un servicio con custodia, el operador suele controlar las claves y tu acceso depende de sus normas y de la protección de la cuenta. En una cartera convencional de autocustodia, el acceso depende de las claves y del método de recuperación. Algunas aplicaciones permiten entrar con Google, Apple u otros modelos de copia de seguridad: lee primero las normas oficiales de tu configuración concreta. Las instrucciones de una cartera no sirven automáticamente para todas las demás.

Una dirección pública permite recibir fondos y consultar el historial público. No es una contraseña, pero vincularla a una persona expone parte de su privacidad financiera. La frase de recuperación y la clave privada otorgan control. La contraseña de una aplicación puede limitarse a desbloquear el almacenamiento local y no siempre recupera el acceso en otro dispositivo.

Los secretos permanecen con su titular

No envíes una frase de recuperación o clave a un administrador, «soporte», bot o formulario de verificación. No fotografíes ni guardes tu frase en un chat, nota normal o nube sin protección. Si gestionas tu propia frase, planifica una copia protegida sin conexión y considera pérdida, incendio y acceso ajeno. Comprueba una copia real solo con las instrucciones oficiales de tu cartera, nunca como ejercicio de la Academia.

Una cartera física cambia el almacenamiento de claves y la confirmación de acciones; no vuelve segura una firma maliciosa. Una cartera separada para experimentar ayuda a separar actividades, pero no convierte una aplicación desconocida en fiable.

Ejercicio y explicación

Clasifica «dirección pública», «frase de recuperación» y «contraseña del correo» en dos columnas: se puede compartir para recibir una transferencia / no se debe entregar para verificar. Respuesta: solo la dirección, si aceptas las consecuencias para la privacidad. Lo demás son secretos. Explica después por qué cambiar la contraseña de la aplicación no neutraliza una frase ya expuesta: la autoridad de las claves antiguas permanece.

03 / 06

2. Cuentas, phishing y falsa urgencia

Protege la cadena de acceso

El correo suele utilizarse para recuperar otras cuentas. Usa contraseñas largas y diferentes, guárdalas en un gestor fiable, activa la autenticación multifactor disponible y revisa las sesiones activas. Prefiere métodos de acceso resistentes al phishing cuando estén disponibles. Un código del autenticador o de SMS también es secreto y pueden engañarte para obtenerlo. No apruebes un acceso inesperado solo porque aparezca un logotipo conocido.

Actualiza el sistema y la cartera desde una fuente verificada. No instales extensiones enviadas por mensaje privado ni concedas acceso remoto a un desconocido. Si necesitas soporte, abre por tu cuenta el sitio oficial, encuentra allí su canal de ayuda y verifica el contacto. Nombre, avatar, cuenta verificada o muchos seguidores no demuestran por separado que un mensaje sea auténtico.

Comprueba la finalidad de la acción

HTTPS indica una conexión cifrada, no la honestidad del propietario. Revisa el dominio completo después de seguir un enlace, no solo el texto de un botón. Los anuncios y primeros resultados de búsqueda pueden conducir a lugares inesperados. Un marcador guardado solo sirve si su dirección original se verificó.

Ejercicio situacional A

Un «administrador» te escribe primero: «Tu certificado está listo. Introduce tu frase de recuperación en la página de verificación en cinco minutos o perderás el bono». Elige tu acción e identifica dos señales de alerta.

Explicación: detenerse, no introducir nada, verificar mediante un canal oficial localizado por tu cuenta y denunciar la suplantación. Las señales incluyen pedir un secreto, un contacto no solicitado y presión con un plazo. El certificado LOGRI nunca necesita tu frase ni acceso a los fondos. Rechazar esta acción completa correctamente el ejercicio; no es perder una oportunidad.

04 / 06

3. Red, activo, dirección y memo

Una dirección no describe toda la ruta

Antes de transferir, establece activo, red, dirección del destinatario y cualquier memo o destination tag exigido por el servicio receptor. Un mismo ticker puede existir en varias redes; un formato de dirección parecido no demuestra compatibilidad con un activo o red. Comprueba condiciones de depósito, mínimos y comisiones en la página actual del receptor. No elijas una red solo porque cobre menos.

Obtén la dirección de una fuente verificada del destinatario. Después de pegarla, compara la dirección completa con la original: los primeros y últimos caracteres permiten detectar algunos errores, pero no sustituyen la revisión completa. El historial puede contener direcciones parecidas introducidas por terceros. Antes de una acción real, revisa también importe, comisiones, estado de la red y disponibilidad del depósito.

Ejercicio situacional B

La plataforma A permite enviar un token ficticio por la red X o Y. La página verificada de depósito de B dice «solo red X; memo OBLIGATORIO». El borrador usa Y y tiene el memo vacío. ¿Se puede enviar si la dirección parece idéntica?

Explicación: no. Detente, comprueba las condiciones de B, cambia la red a X y añade el memo requerido de la fuente verificada. Si X o el campo memo no están disponibles, no transfieras hasta aclararlo. El aspecto idéntico de la dirección no resuelve la incompatibilidad. Es un ejercicio para comprobar condiciones, no una invitación a probar la red Y.

Práctica sin transferencia

Completa una ficha: activo - ficticio; red - X; dirección - DIRECCIÓN-A; memo - MEMO-DE-PRÁCTICA; compatibilidad del receptor - confirmada por el supuesto; acción - verificar la ruta completa. En la realidad, una pequeña transferencia de prueba puede comprobar una ruta concreta, pero no garantiza la seguridad de la siguiente ni elimina mínimos o comisiones. Este curso tampoco exige esa prueba.

05 / 06

4. Conectar, firmar y autorizar son acciones distintas

Lee la solicitud de la cartera

Conectar suele compartir la dirección pública elegida con una aplicación y permitirle solicitar otras acciones. Firmar, aprobar el gasto de tokens y enviar una transacción tienen consecuencias diferentes. Los mecanismos cambian entre redes y tipos de cuenta. No interpretes cualquier firma sin comisión como un acceso normal y seguro: ciertas autorizaciones firmadas pueden utilizarse después.

Antes de confirmar, averigua quién solicita la acción, qué contrato obtiene autoridad, sobre qué token, importe y duración. Compara la solicitud con tu objetivo. Si la interfaz no explica los datos o no los entiendes, rechaza la solicitud y busca la explicación oficial. Un límite grande o ilimitado aumenta el daño posible. Un nombre de proyecto conocido no elimina la comprobación del permiso concreto.

Desconectar no equivale a revocar

Cerrar una pestaña o desconectar una dapp de la cartera es diferente de cancelar una autorización de tokens existente. Los permisos se revisan y revocan por separado, siguiendo las instrucciones oficiales de la red. Revocar puede requerir una comisión; no devuelve activos robados ni cambia una clave privada expuesta. No hay una única acción que resuelva todos los casos.

Ejercicio y explicación

Una aplicación ficticia ofrece una imagen gratuita, pero pide acceso ilimitado a una stablecoin ficticia. Después dice: «Si cambias de opinión, basta con cerrar la pestaña». Escribe tu decisión.

Respuesta: rechazar la solicitud desproporcionada y verificar la finalidad del permiso. Cerrar la pestaña no elimina la autoridad concedida. Una firma sin comisión y sin débito inmediato no demuestran ausencia de riesgo. Analizamos una descripción; conectar una cartera, firmar o revocar algo para este ejercicio no está permitido ni es necesario.

06 / 06

5. Plan ante incidentes y comprobación final

Identifica qué pudo quedar expuesto

Si sospechas, deja de interactuar con el sitio dudoso y no respondas a «rescatadores» que te escriben sin solicitud. En otra nota, registra hora, dominio, tipo de petición y hash público de transacción si existe. Elimina secretos y datos personales del material que compartas para pedir ayuda. La recuperación no está garantizada; un pago anticipado por «recuperación garantizada» es motivo para detenerse.

Si se expuso una contraseña de cuenta, usa un dispositivo fiable para abrir el servicio oficial, cambiarla, cerrar sesiones desconocidas y revisar recuperación y MFA. Incluye el correo si está afectado. Si concediste un permiso sospechoso, sigue las instrucciones oficiales de la red para revisarlo y revocarlo. Estas medidas resuelven problemas distintos.

Si se expuso una frase de recuperación o clave privada, el acceso anterior no puede considerarse seguro tras cambiar una contraseña o revocar un solo permiso. El plan suele requerir una cartera nueva, creada de forma independiente con claves nuevas, y proteger los activos restantes. No introduces la frase antigua en un formulario «nuevo» de un rescatador. Si observas vaciado automático, no añadas fondos a ciegas a la dirección comprometida para pagar gas: también podrían llevárselos. Un incidente real necesita ayuda verificada y adaptada a la situación.

Ejercicio final

Escribe tres filas: contraseña filtrada / permiso sospechoso / clave expuesta. Añade en cada una la comprobación correspondiente de la lección. Incluye tu regla de parada: «Si no entiendo una solicitud, no confirmo; la urgencia no sustituye la comprobación». Es un ejercicio de planificación, no una orden de realizar operaciones reales.

Antes del examen

Explica dirección frente a secreto, contraseña frente a recuperación y conexión frente a autorización. Repasa los escenarios A y B. El examen evalúa decisiones bajo las condiciones descritas; no audita tus dispositivos ni certifica que una cartera real sea segura.

Fuentes y alcance

Texto educativo original LOGRI; fuentes comprobadas el 31 de octubre de 2026. Las interfaces, recuperación, permisos y condiciones de red cambian: consulta instrucciones oficiales actuales. Los mecanismos EVM no se aplican automáticamente a Solana, TON u otras redes. Ni una cartera ni un examen eliminan todos los riesgos. Las fuentes primarias de abajo están principalmente en inglés; leerlas no sustituye ni bloquea el curso completo en el idioma elegido.

Fuentes primarias

- Ethereum: seguridad de la cartera: <https://ethereum.org/security/>
- MetaMask: recuperación y contraseña: <https://support.metamask.io/start/user-guide-secret-recovery-phrase-password-and-private-keys>
- MetaMask: permisos de tokens:
<https://support.metamask.io/transactions-and-gas/transactions/what-is-a-token-approval/>
- MetaMask: desconexión y revocación:
<https://support.metamask.io/more-web3/dapps/disconnect-wallet-from-a-dapp/>
- Uniswap Labs: firmas peligrosas: <https://support.uniswap.org/hc/en-us/articles/40050562560781-Crypto-Wallet-Signature-Scams>
- Solana: guía de seguridad: <https://solana.com/learn/staying-safe-on-solana>
- Coinbase: memo y destination tag: <https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/destination-tag-memo-faq>
- CISA: protección básica en internet: <https://www.cisa.gov/sites/default/files/2024-09/Secure-Our-World-4-Easy-Ways-Stay-Safe-Online-Tip-Sheet.pdf>