Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Ciberseguridad

Metodología para la Implementación Segura de Tesorería de Criptomonedas en las Organizaciones

Trabajo de Fin de Máster presentado por:	Carlos Mario Alba Rodriguez
Tipo de trabajo:	Desarrollo de metodologías
Director:	Antoni Manel Ferragut Amengual
Fecha:	24 de diciembre de 2022

Agradecimientos

Gracias a los mentores que me han cambiado la perspectiva de lo que es posible.

A quienes me impulsan a seguir avanzando en las diferentes variables, un bloque a la vez.

El futuro se ve brillante.

Resumen

Alrededor del mundo existen organizaciones que han decidido afrontar el reto de innovación tecnológica que implica contar con cripto activos en su tesorería.

Por tal motivo, este trabajo pretende ofrecer la metodología para la implementación segura de tesorería de criptomonedas en las organizaciones. Su objetivo es guiar a cualquier organización que decida enfrentarse a este reto, hacia el método de implementación que mejor se ajuste a sus necesidades, recursos y objetivos empresariales.

En este se identifican las medidas y controles de ciberseguridad generales y específicos que son requeridos antes, durante y después de la implementación. Se identifican los tipos de ciber ataques a los que se puede enfrentar y qué hacer en caso de presentarse un ciber incidente.

Adicionalmente, se provee una lista de verificación para auditar la seguridad de la implementación, de modo que las empresas puedan tomar acción efectiva sobre la seguridad de su tesorería de cripto activos.

Palabras clave: ciberseguridad, cripto, criptoactivos, criptomonedas, empresa, tesorería.

Abstract

Around the world there are organizations that have decided to face the challenge of technological innovation that implies having crypto assets in their treasury.

For this reason, this work aims to offer the methodology for the secure implementation of cryptocurrency treasury in organizations. Its goal is to guide any organization that decides to face this challenge, towards the implementation method that best suits their needs, resources and business objectives.

It identifies the general and specific cybersecurity measures and controls that are required before, during and after implementation, the types of cyber-attacks that can be faced and what to do in the event of a related incident.

Additionally, a checklist is provided to audit the security of the implementation, so that companies can take effective action on the security of their crypto asset treasury.

Keywords: cybersecurity, crypto, assets, cryptocurrency, organization, treasury.

Índice de contenidos

Índice de tablas

Índice de figuras

Introducción

El surgimiento de la tecnología *blockchain* (Hayes, 2022) ha revolucionado el mundo en diferentes sectores, uno de ellos ha sido la industria financiera. Debido a sus características, esta tecnología tiene la capacidad de aumentar la confianza, seguridad, transparencia y la trazabilidad de la información en la red, al mismo tiempo que ofrece ahorro de costos con nuevas eficiencias.

En la actualidad cada vez son más las personas, empresas e incluso gobiernos que deciden implementar la adopción de criptomonedas en sus actividades financieras. Según un estudio realizado por Chainalysis, al analizar datos de 154 países fue posible evidenciar que se generó un incremento del 881% en la adopción global en 2021.

Dicho estudio, sugiere que las razones de este incremento en la adopción pueden ser diversas alrededor del mundo:

- En las economías emergentes muchos recurren a las criptomonedas para preservar sus ahorros frente a la devaluación de la moneda local, envío y recepción de remesas y realizar transacciones comerciales. El principal motivo de estos usos es debido al relativamente bajo porcentaje de bancarización que existe en la región.
- La adopción en Asia Oriental, Europa Occidental y América del Norte durante el último año, se ha visto impulsada mayoritariamente por inversión institucional (Coinbase, 2022).

1.1. Motivación

Según un estudio realizado por CoinShares en el 2022, entre las razones por las que los inversionistas han decidido añadir cripto activos a sus portafolios se encuentran:

- Razón Número 1: Su buen valor (25%)
- Razón Número 2: Demanda de los clientes (24%)
- Razón Número 3: Diversificación (20%)

No obstante, la custodia segura de los activos se identifica como la tercera razón principal por la que los inversionistas no han incluido cripto activos en sus portafolios, siendo la segunda

razón la volatilidad de este tipo de activos y la primera la incertidumbre regulatoria (Butterfill, 2022).

Con base en los datos de crecimiento en la adopción de criptomonedas alrededor del mundo, y la preocupación generalizada por la custodia segura de este tipo de activos, el presente proyecto pretende generar una metodología, que permita a las organizaciones implementar de manera segura el almacenamiento digital de un porcentaje de sus activos financieros en criptomonedas.

Dicha metodología será puesta a prueba a través del desarrollo de un piloto experimental sobre una organización real, sobre la cual se cuenta con la respectiva autorización por parte del personal directivo para hacerlo posible.

Adicionalmente, este proyecto tiene especial énfasis en la perspectiva de los jefes y directores de tecnología de las organizaciones, los cuales cada año se enfrentan a un escenario tecnológico que constantemente evoluciona y un genera un gran abanico de tecnologías emergentes. Con base en este trabajo será posible implementar desde cero y de manera gratuita dichas tecnologías, facilitando el proceso de los tomadores de decisiones al minimizar el riesgo y tiempo a invertir en una implementación segura.

Por otro lado, es relevante destacar que la línea de trabajo de este proyecto de fin de máster tiene afinidad con la Gestión de la seguridad y algunos conceptos de cifrado de llave pública, relacionados con la Criptografía y mecanismos de seguridad.

1.2. Planteamiento del trabajo

Dado el contexto y las necesidades evidenciadas, podemos sostener que un procedimiento que permita a las organizaciones adoptar cripto activos, de manera digitalmente segura dentro de su portafolio de tesorería sería una solución plausible y necesaria.

Por tal motivo, el fin del presente trabajo será la documentación de una serie de pasos y uso de tecnologías, que permitan a las organizaciones tener cripto activos en sus portafolios de tesorería, de manera digitalmente segura.

1.3 Estructura del trabajo

La estructura del presente trabajo se distribuye de la siguiente manera:

Capítulo 1: Introducción. Este apartado describe de manera general la necesidad que busca resolver el trabajo de fin de máster.

Capítulo 2: Contexto y estado del arte. Este apartado detalla el estado actual de las soluciones que se han generado, con base en la necesidad anteriormente descrita.

Capítulo 3: Objetivos y metodología de trabajo. Este apartado describe los objetivos generales y específicos a alcanzar, y documenta la serie de fases que se llevarán a cabo para hacer posible el piloto experimental.

Capítulo 4: Desarrollo específico de la contribución. Este apartado contiene el detalle de la propuesta. Contendrá el método que mejor se ajuste a los requerimientos de la organización, sobre la cual se desarrollará el piloto experimental, los elementos de la propuesta y las tecnologías que se usarán.

Capítulo 5: Implementación con base en Metamask. En este capítulo se explora el detalle de la pre-implementación, implementación y pos-implementación con Metamask.

Capítulo 6: Implementación con base en Qredo. En este capítulo se explora el detalle de la pre-implementación, implementación y pos-implementación con Qredo.

Capítulo 7: Implementación con base en Ledger. En este capítulo se explora el detalle de la pre-implementación, implementación y pos-implementación con Ledger.

Capítulo 8: Implementación con base en plataforma de intercambio. En este capítulo se detallan las medidas de seguridad en la implementación con plataforma de intercambio.

Capítulo 9: Medidas de seguridad generales. En este apartado se identifican las medidas que cualquier método de implementación debe tener presente.

Capítulo 10. Phishing y tipos de estafas a identificar. Este apartado describe los principales tipos de ataques y como evitarlos.

Capítulo 11. En caso fe ser hackeado. Este capítulo describe las medidas a tomar en caso de llegar a ser víctima de un ciberataque o estafa.

Capítulo 12. Lista de verificación de auditoría de seguridad. Este capítulo entrega diversas listas de controles a tener presente para validar una implementación segura para cualquier método elegido.

Capítulo 13: Resultados de auditoría sobre Aidel Corp. Este apartado detalla el resultado de la aplicación de la auditoría del capítulo anterior sobre la implementación realizada en Aidel Corp.

Capítulo 13: Evaluación y resultados con base en la auditoría sobre Aidel Corp. Este capítulo detalla los principales hallazgos identificados en la evaluación del proceso con base en los resultados obtenidos.

Capítulo 14. Conclusiones de la prueba piloto. Este apartado detalla las principales conclusiones sobre la implementación con base en la evaluación realizada y la metodología implementada.

Capítulo 15. Conclusiones y futuras líneas de desarrollo. En este último apartado se definen las conclusiones generadas por la experiencia adquirida en el lanzamiento del piloto y, adicionalmente se listará una serie de líneas de desarrollo futuro posibles respecto al presente trabajo.

2. Contexto y estado del arte

2.1. Introducción

2.1.1. Regulación

Para empezar, es necesario tener presente que no todos los gobiernos ven con agrado el uso de cripto activos como medio de intercambio, transferencia o almacenamiento de valor. A finales de 2022 existe una lista de 17 países, en donde el uso de cripto activos es restringido o ilegal (Orji, 2022).

Esto implicaría que el intento de implementación del contenido del presente trabajo en dichas regiones podría generar inconvenientes con las autoridades locales.

- Argelia – Ilegal
- Bangladesh – Restringido
- Bolivia – Ilegal
- China – Ilegal
- Egipto – Restringido
- Indonesia – Ilegal
- Ghana – Ilegal
- Irán – Restringido
- India – Restringido
- Irak – Restringido
- Kosovo – Restringido
- México – Restringido
- Nepal – Ilegal
- Macedonia del Norte – Ilegal
- Rusia – Restringido
- Turquía – Restringido
- Vietnam – Restringido

Antes de continuar, es necesario validar que la organización en la que se implemente dicha metodología, no se encuentre bajo la jurisdicción de ningún país mencionado en la anterior lista, y si es así, validar la posibilidad de implementación teniendo presentes las restricciones existentes.

2.1.2. Organizaciones a la vanguardia

En la actualidad existen 23 compañías públicas listadas en diversas bolsas del mundo, que poseen parte de su tesorería en cripto activos como bitcoin. Entre las principales se

encuentran: MicroStrategy Inc., Marathon Digital Holdings, Coinbase y Square Inc. (Coingecko, 2022).

Dichas compañías serán identificadas posteriormente como “organizaciones a la vanguardia”, ya que sus trabajos serán tenidos en cuenta como precedentes para el desarrollo del presente trabajo.

2.1.3. Almacenamiento

La capacidad de poseer cripto activos, se da a través de una *crypto wallet* o cripto billetera. La cual puede ser un dispositivo, programa o servicio que almacena las llaves públicas y privadas para realizar transacciones en cripto monedas. Más adelante entraremos en detalle sobre estas tecnologías, pero por ahora solo es necesario tener presente la necesidad de una cripto billetera para el almacenamiento de dichos activos.

Por otro lado, existen dos formas principales a través de las cuales una organización puede poseer cripto activos, dependiendo de la decisión de tomar o no la responsabilidad del almacenamiento de los activos: billeteras custodiadas y billeteras auto custodiadas.

- Billeteras custodiadas: Una billetera custodiada es una billetera en la que la llave privada es retenida por una tercera parte, normalmente una organización especializada en el manejo de este tipo de activos, con el fin de administrar los activos en su nombre.

  El uso de una billetera custodiada normalmente implica que la organización tiene que pasar a través de un proceso de *KYC* (*Know Your Customer/*Conozca a su Cliente), y enviar diversos documentos oficiales para identificar y confirmar que es quien dice ser, para posteriormente permitirle acceso al servicio de almacenamiento de cripto activos.
- Billeteras auto custodiadas: Una billetera auto custodiada es una billetera en la que las llaves privadas son almacenadas localmente en su dispositivo, dando al propietario control total sobre los activos. Normalmente, una frase de recuperación de 12 - 24 palabras permite al propietario acceder y administrar los activos y la billetera. Esta frase debe ser guardada de forma segura y nunca debe compartirse con ninguna otra parte.

  Cualquier persona o entidad puede crear una billetera auto custodiada, incluso sin hacer registro de un correo electrónico, datos personales o cuenta de banco. Ya que

implementan el concepto de *permissionless*, es decir, no requieren autorización de ninguna parte. (Wikiwand, 2022).

2.2. Investigaciones relacionadas y casos precedentes

2.2.1. Investigaciones relacionadas

- IMPACTO DEL BLOCKCHAIN Y LAS CRIPTOMONEDAS EN LAS ENTIDADES FINANCIERAS

  Hasta la fecha no se evidencian investigaciones directamente relacionadas con el presente proyecto. No obstante, se identifican algunos trabajos de investigación con temática relacionada que puede ser considerada relevante para el alcance de este trabajo.

  En el artículo de Orbe Catalán, 2019, se habla de que la descentralización de la banca a través de la tecnología entre pares y cripto activos trae consigo multitud de beneficios, “entre los que cabe destacar la extinción de la burocracia y la falta de ataduras geográfica que hace que puedan llegar a cualquier parte del mundo”. (de Orbe Catalán, 2019).

- CRIPTOMONEDAS Y LIBERTAD DE EMPRESA

  Por otro lado, es necesario tener en cuenta un punto de especial atención respecto al uso de cripto activos en las organizaciones.

  En el artículo de Hermosilla Castillo, 2019, se remarca que, “El desarrollo de las criptomonedas se ha visto opacado por hechos delictivos, los cuales, constituyen una de las barreras más relevantes, a efectos de su introducción a los mercados. Con todo, estos hechos no deben ser percibidos como defectos de la criptomoneda, sino que como manipulaciones fraudulentas de personas inescrupulosas, que se aprovechan de la creación de nuevas tecnologías para la comisión de delitos, situación que se ha repetido en la historia desde la creación de la imprenta. Debido a esto, se requiere para el desarrollo y estudio de los cripto activos y tecnologías asociadas, considerar desde un punto de vista favorable los riesgos asociados con las cripto monedas, mejorable, al igual que toda innovación tecnológica que tenga como fin facilitar la vida y en este caso, los intercambios económicos.”. (Hermosilla Castillo, 2019).

2.2.2. Empresas que han implementado tesorería de criptomonedas

Como es posible evidenciar, en la actualidad existen pocas organizaciones que cuentan con tesorería de criptomonedas, y son aún menos aquellas que han decidido compartir documentación o detalle de como lo han logrado.

Sin embargo, existen algunos casos de implementación que hasta el momento se pueden considerar como exitosos, a continuación, se hablará de estos casos de éxito, los cuales se plantearán como la base para el desarrollo del objetivo de este trabajo.

2.2.3. Caso Square

El 7 de octubre de 2020, Square, Inc. Realizó una compra estimada en 4709 bitcoins, siendo 50 millones de dólares el precio de compra total. Decidiendo posteriormente hacer pública la documentación de dicho proceso para organizaciones que consideran hacer movimientos similares (Square, Inc., 2019).

La aproximación utilizada para el almacenamiento de los activos fue el desarrollo de una tecnología llamada *Sub-zero*. La cual es una solución de almacenamiento en frio con el fin de reducir la superficie de ataque al no estar conectado a internet. Esta solución hace uso de un dispositivo de *hardware* especializado, denominado HSM.

Square comenta que HSM está programado para que sus billeteras frías solo puedan transferir fondos a billeteras calientes de Square, con el fin de añadir otra capa de defensa. La firma también informa que ha añadido una protección multi firma, en la cual los participantes deben usar una combinación de tarjetas inteligentes y contraseñas para autenticar transferencias.

Adicionalmente, se utilizan códigos QR para intercambiar la mínima cantidad de datos entre el mundo en línea y el no conectado a internet (Huillet, 2018).

Sin embargo, en su documentación informan que existe un listado de organizaciones disponibles para aquellas empresas que busquen tercerizar la custodia (Natalie, 2020)

2.2.4. Caso plataformas de intercambio centralizado

Entre las organizaciones más reconocidas por sus procesos de almacenamiento seguro de cripto activos se encuentran los “exchanges” o plataformas de intercambio centralizado.

Estas plataformas son un negocio que permite a sus clientes intercambiar criptomonedas o monedas digitales por otros activos, como dinero fiduciario convencional u otras monedas digitales (Wikimedia, 2022).

No obstante, este tipo de organizaciones suelen minimizar la información de almacenamiento de sus activos por motivos de seguridad. No obstante, a continuación, se listarán los hallazgos más relevantes respecto a algunas de estas plataformas:

- Binance Exchange: Binance solo posee un pequeño porcentaje de criptomonedas en sus billeteras calientes. El resto se mantiene en almacenamiento en frío, desconectado de Internet (Binance, 2022)
- BitGo Exchange: Bitgo ofrece a sus clientes custodiar sus cripto activos a través de seguridad multi llave. Esta aproximación permite aplicar controles y políticas de seguridad mediante listas blancas, límites de velocidad y aprobaciones administrativas (BitGo, 2022).

  La forma de implementarlo es a través de tres tipos de llaves:
  - Llave del cliente: Es generada y almacenada por el cliente. Se usa para iniciar todas las interacciones.
  - Llave de respaldo: Es generada y almacenada fuera de línea por el cliente con el objetivo de ser usada en recuperación de desastres.
  - Llave BitGo: Se usa para co-firmar todas las transacciones si y solo si los controles de las políticas establecidos por el cliente han sido cumplidos.

- Coinbase Vault: La plataforma de intercambios Coinbase ofrece el servicio vault, el cual es un tipo de custodia que permite almacenar los activos fuera de línea bajo la protección del mismo Exchange. Este servicio está pensado para grandes cantidades de activos que planean ser almacenados por largos periodos de tiempo.

  La diferencia entre un almacenamiento común y este tipo de almacenamiento es equivalente a la diferencia entre tener dinero en una cuenta bancaria, fácilmente

accesible y gastable, a tenerlo en una caja de seguridad que es más difícil de acceder y requiere una llave.

Adicionalmente, ofrecen medidas de seguridad extendidas, como periodos de espera antes del retiro de los fondos y el poder añadir medidas de seguridad adicionales para aprobar un retiro de activos (Marquit, 2022).

Ventajas

- El almacenamiento fuera de línea es más seguro que mantener los activos en una cuenta de plataforma de intercambios o una billetera caliente
- Se requiere aprobación por parte de los copropietarios para retirar los fondos
- Provee una forma de almacenar los cripto activos por un largo plazo

Desventajas

- El acceso a los cripto activos se hace mucho más difícil
- No se tiene el mismo control que se podría tener en una billetera fría o en una billetera de papel
- La organización tercera, el custodio, aún tiene control sobre los activos, y aunque no puede administrarlos directamente, es cierto que puede congelar la cuenta del usuario e impedirle el retiro de estos.

Un punto en común que se ha identificado es que, si bien es cierto que dichas plataformas de intercambio no hacen pública la información del procedimiento de almacenamiento, también es cierto que suelen hacer énfasis en: 1) cuentan con seguros financieros para protegerse ante un ataque y 2) son regulados por instituciones que validan que cumplan con buenas prácticas de seguridad (Binance, 2021).

2.3. Tecnologías base

2.3.1. Criptografía de cifrado asimétrico

La criptografía de llave pública, o criptografía asimétrica, es un sistema criptográfico que utiliza pares de llaves. Cada par consta de:

- Una llave pública (que puede ser conocida por otros)

- Una llave privada (que no debe ser conocida por nadie excepto por el propietario)

La generación de dichos pares de llaves depende de algoritmos criptográficos que se basan en problemas matemáticos denominados funciones unidireccionales.

La seguridad de esta tecnología tiene como requerimiento el mantener en secreto la llave privada; mientras que la llave pública se puede distribuir abiertamente sin comprometer la seguridad (Binance Academy, 2022).

2.3.2. Blockchain

Una *blockchain* es una base de datos distribuida o un libro mayor que es compartido entre los nodos de una red informática. Al igual que una base de datos, una blockchain almacena información en formato digital.

La tecnología *blockchain* juega un papel fundamental en los criptoactivos, ya que permite mantener un registro de transacciones seguro y descentralizado. La *blockchain* garantiza la fidelidad y seguridad de un registro de datos y genera confianza sin necesidad de confiar directamente en un intermediario o tercero.

Una diferencia fundamental entre una *blockchain* y una base de datos común es la forma en la cual los datos son estructurados. Una *blockchain* suele recopilar información en grupos, los cuales se denominan bloques y contienen conjuntos de información. Los bloques tienen ciertas capacidades de almacenamiento, y cuando se llenan, se cierran y se enlazan al bloque anteriormente lleno, formando una cadena de datos conocida como la *blockchain*. Toda la información nueva que sigue a ese bloque recién agregado se compila en un nuevo bloque recién formado, el cual posteriormente se agregará a la cadena una vez que se llene.

Diferencia principal entre una blockchain y una base de datos tradicional

Una base de datos normalmente estructura sus datos en tablas, mientras que la *blockchain* lo hace en fragmentos llamados “bloques”, que se unen entre sí. Esta estructura de datos crea inherentemente una línea de tiempo de datos que es irreversible cuando se implementa de una manera descentralizada.

Una vez se llena y se valida un bloque, este se graba en piedra y se convierte en parte de la línea de tiempo de la *blockchain*. Cada bloque de la cadena recibe una marca de tiempo exacta cuando se agrega a esta. (Binance, 2022).

2.3.3. Tipos de blockchain

En la actualidad existen 4 tipos de *blockchain* (GeeksforGeeks, 2022):

- *Blockchain* pública: Completamente abierta a seguir la idea de descentralización. No tiene ninguna restricción, cualquiera con un computador e internet puede participar en su red. No es propiedad de nadie. Todos los computadores en la red pueden tener copia de otros nodos o bloques presentes en la red. Es posible verificar las transacciones o registros abiertamente.
- *Blockchain* privada: Solo nodos selectos pueden participar en el proceso, haciendo la blockchain en cierto modo más segura que otras. Es operada en una red cerrada, normalmente dentro de una organización.
- *Blockchain* híbrida: Es una implementación mixta entre *blockchain* pública y privada. Una parte es controlada por una organización y otras partes son visibles al igual que una *blockchain* pública. Los usuarios acceden a la información vía contratos inteligentes.
- *Blockchain* de consorcio: Es una aproximación creativa que resuelve las necesidades de la organización. Esta blockchain valida la transacción y también inicia o recibe transacciones. Una parte es pública y otra privada, al igual que la *blockchain* hibrida. En este tipo más de una organización administra la *blockchain*.

2.3.4. Protocolos de blockchain usados

Los protocolos de *blockchain* comúnmente utilizados para la posesión de cripto activos son *blockchain* abiertas. Entre estos protocolos se encuentran:

- *Blockchain* de Bitcoin: La *blockchain* de Bitcoin es mucho más que una criptomoneda: es la tecnología en la que se basan la mayoría de las criptomonedas, incluido Bitcoin. La *blockchain* de Bitcoin es única, debido a su capacidad de garantizar que la totalidad de las transacciones sean precisas.

Cada acción en la misma es registrada y nada queda fuera de la red. Una vez que una acción se registra y almacena en uno de los bloques de información, se marca la hora y se asegura, de modo que el registro completo está disponible para cualquier persona en el sistema.

Bitcoin representa una forma de dinero digital y un movimiento para descentralizar los servicios financieros. Antes de Bitcoin, era necesario que un tercero de confianza llevara un libro de contabilidad, o un sistema de mantenimiento de registros de los datos financieros de una empresa o persona, para registrar quién poseía cuánto. Todo el mundo tiene una copia de este libro mayor con la red Bitcoin, por lo que no hay necesidad de terceros. (Cointelegraph, 2022).

- *Blockchain* de Ethereum: Ethereum es una plataforma *blockchain* descentralizada que establece una red entre pares la cual ejecuta y verifica de forma segura el código de la aplicación, llamados contratos inteligentes. Los contratos inteligentes permiten a los participantes realizar transacciones entre ellos sin una autoridad central de confianza. Los registros de transacciones son inmutables, verificables y se distribuyen de forma segura a través de la red, lo que brinda a los participantes total propiedad y visibilidad de los datos de las transacciones. Las transacciones son enviadas y recibidas por cuentas Ethereum creadas por el usuario. Un remitente debe firmar transacciones y gastar Ether, la criptomoneda nativa de Ethereum, como costo de procesamiento de transacciones en la red. (Cointelegraph, 2022).
- Blockchain de *BNB*: Lanzado por la plataforma de intercambio de criptomonedas Binance, BNB Smart Chain (BSC), anteriormente Binance Smart Chain, es una *blockchain* híbrida. Admite contratos inteligentes y aplicaciones descentralizadas (DApps). BSC se ejecuta junto con la Cadena BNB, anteriormente Cadena Binance. El primero admite contratos inteligentes, mientras que el segundo permite un alto volumen de transacciones con un tiempo de bloque de 3 segundos. Ambas cadenas de bloques juntas forman Binance Chain. (Scorechain, 2021).
- *Blockchain* de Solana: Solana es una *blockchain* pública diseñada para alojar aplicaciones descentralizadas y escalables.

Solana es mucho más rápida en términos de la cantidad de transacciones que puede procesar y tiene tarifas de transacción significativamente más bajas que las *blockchains* rivales como Ethereum.

Solana es una cadena de bloques de prueba de participación (PoS), pero la mejora con un mecanismo llamado prueba de historial (PoH), que utiliza marcas de tiempo codificadas para verificar cuándo ocurren las transacciones. (Picardo, 2022)

- *Blockchain* de Polygon: Polygon es una criptomoneda, con el símbolo MATIC, y también una plataforma tecnológica que permite que las redes *blockchain* se conecten y escalen.

  La plataforma Polygon opera utilizando la *blockchain* de Ethereum y conecta proyectos basados en Ethereum. El uso de la plataforma Polygon puede aumentar la flexibilidad, la escalabilidad y la soberanía de un proyecto de *blockchain* sin dejar de ofrecer la interoperabilidad, seguridad y en general los beneficios estructurales de la *blockchain* de Ethereum.

  MATIC es un token ERC-20, esto significa que es un token que cuenta con compatibilidad con otras monedas digitales basadas en Ethereum. MATIC se utiliza para gobernar y proteger la red Polygon y para pagar las tarifas de transacción de la red. (Kraken 2021)

2.3.5. Cripto billeteras: llaves públicas y privadas

La frase “Si no son tus llaves, no son tus monedas”, es conocida como una de las reglas más importantes en la comunidad cripto (Moreland, 2022). Para entenderla mejor, es necesario profundizar un poco más en la definición de “llaves”.

Cada billetera cuenta con una llave pública y una privada. Una llave pública (también conocida como una dirección de billetera), es utilizada para recibir fondos y puede ser compartida con cualquier persona como se mencionó anteriormente. Una llave pública de Bitcoin se ve algo así: 2FktbJKD7uzSgzQX2YT9uzE6MaSw2MRiAX.

Una llave privada es usada para controlar los fondos en la llave pública. Cualquier persona con la llave privada puede acceder a los fondos en la billetera, y, por lo tanto, esta no debe ser compartida con nadie. Las llaves privadas pueden expresarse en

formato alfanumérico (similar a la llave pública anteriormente mencionada) o más comúnmente, en la forma de una frase semilla, la cual es una lista de típicamente 12 o 24 palabras ordenadas secuencialmente en inglés.

Cuando se crea una nueva billetera, normalmente se tiene acceso a la frase semilla para la billetera. La mayoría de los individuos eligen grabar la frase semilla en una pieza de papel y almacenarla en un lugar seguro, aunque algunos eligen opciones más duraderas, como grabar las palabras en una placa de titanio. Sea cual sea la opción elegida, lo prioritario es guardarla en un lugar seguro en el que nadie más tenga acceso (Binance, 2021).

2.3.6. Tipos de billeteras

Anteriormente se mencionó el concepto de cripto billeteras, a continuación, se identificarán los diversos tipos de billeteras existentes.

- **Billeteras frías:** Las billeteras frías son reconocidas como la opción más segura para almacenar cripto activos. La billetera fría es aquella que no se conecta a Internet, por lo que tiene riesgos mínimos de verse comprometida. Las personas también se refieren a estas billeteras como billeteras de *hardware* o carteras fuera de línea.

  Estas billeteras permiten que la clave privada y la dirección de un usuario se almacenen en un componente que no se conecta a Internet. Por lo general, viene con un software que funciona en paralelo para que el usuario revise su billetera sin poner en riesgo la clave privada (Binance, 2022).

  - Billeteras de *hardware*: Las billeteras de *hardware* son dispositivos electrónicos físicos que utilizan un generador de números aleatorios (RNG) para generar claves públicas y privadas. Posteriormente, estas claves son almacenadas en el propio dispositivo, que no cuenta con conexión a Internet.

    Si bien estas billeteras ofrecen niveles más altos de seguridad contra los ataques en línea, pueden presentar riesgos si la implementación del *firmware* no se realiza correctamente. Además, las billeteras de *hardware* tienden a ser menos fáciles de usar y los fondos son más difíciles de acceder en comparación con las billeteras calientes.

Usualmente, se considera usar una billetera de *hardware* cuando se planea mantener los cripto activos durante mucho tiempo, o si se cuenta con grandes cantidades de criptomonedas. Actualmente, la mayoría de las billeteras de *hardware* permiten configurar un código PIN para proteger el dispositivo, así como una frase de recuperación, que se puede usar en caso de que se pierda la billetera (Binance, 2022).

- Billeteras de papel: Una billetera de papel es una hoja de papel en la que se imprimen físicamente la dirección de la billetera o llave pública, y su llave privada en forma de códigos QR. Tales códigos pueden ser escaneados para realizar transacciones de cripto monedas.

  Algunos portales web de billeteras de papel dan autorización para realizar descargas de su código, con el objetivo de generar nuevas direcciones y claves mientras está desconectado. Estas billeteras son altamente resistentes a los ataques de *hackers* en línea y pueden considerarse una alternativa a las billeteras de *hardware* (Binance, 2022).

- **Billeteras calientes**: Una billetera caliente es cualquier billetera que está conectada de alguna manera a Internet. Estas billeteras son bastante fáciles de configurar y se puede acceder rápidamente a los fondos, lo que las hace convenientes para los comerciantes y otros usuarios frecuentes.

  Las billeteras activas como las billeteras móviles y de escritorio, son billeteras que generan y almacenan sus llaves privadas en línea. Estar conectado a internet hace que las transacciones con billeteras calientes sean rápidas y fáciles, sin embargo, estas billeteras deben tratarse de manera similar a las billeteras de cuero clásicas, en el sentido de que solo se deben almacenar pequeñas cantidades en ellas (Binance, 2022)

  - Billeteras de escritorio: Como su nombre lo indica, una billetera de escritorio es un software que se descarga y se ejecuta localmente en la computadora de quien lo instale.

    A diferencia de algunas versiones basadas en la web, las billeteras de escritorio ofrecen control total sobre las llaves y fondos. Cuando se genera una nueva billetera de escritorio, un archivo llamado "wallet.dat" se almacena localmente

dentro de la computadora. Este archivo contiene la información de la clave privada utilizada para acceder a las direcciones de criptomonedas, por lo que es necesario cifrarlo con una contraseña personal.

Si se cifra la billetera de escritorio, será necesario proporcionar la contraseña cada vez que ejecute el software para que se pueda leer el archivo wallet.dat. Si se pierde este archivo o se olvida la contraseña, lo más probable es que se pierda el acceso a los fondos.

En general, las billeteras de escritorio pueden considerarse más seguras que la mayoría de las versiones web, pero es crucial asegurarse de que la computadora en la que se instale esté libre de virus y programas malignos, antes de configurar y usar una cripto billetera (Binance, 2022)

- Billeteras para dispositivos móviles: Las billeteras móviles funcionan de manera muy similar a sus contrapartes de escritorio, pero están diseñadas específicamente como aplicaciones para teléfonos inteligentes. Estas son bastante convenientes ya que permiten enviar y recibir criptomonedas mediante el uso de códigos QR.

  Sin embargo, al igual que las computadoras, los dispositivos móviles son vulnerables a aplicaciones maliciosas e infecciones de programas malignos. Por lo tanto, se recomienda cifrar la billetera móvil con una contraseña y hacer una copia de seguridad de sus claves privadas (o frase inicial), en caso de que el teléfono inteligente se pierda o se dañe (Binance, 2022).

- Billeteras de extensión de navegador: Es posible usar billeteras web para acceder a los cripto activos a través de una interfaz de navegador, sin tener que descargar ni instalar nada. Esto incluye tanto las billeteras de plataformas de intercambio como otros proveedores basados en navegador. En la mayoría de los casos, se puede crear una nueva billetera y establecer una contraseña personal para acceder a la misma (Binance, 2022).

2.4. Investigaciones relacionadas

De acuerdo con una encuesta de Gartner, en 2021 el 5% de los directores y líderes financieros senior, dijeron que tenían planeado mantener cripto activos como bitcoin en sus balances. No obstante, la mayor parte de la tecnología de custodia y almacenamiento seguro de estos

activos todavía tiene dificultades para garantizar la seguridad y la liquidez de estos, y tiene dificultades aún peores para automatizar los flujos de trabajo, administrar la liquidez y generar informes. (Gartner, 2021).

Como resultado, los encargados de la tesorería corporativa que poseen criptomonedas suelen confiar en un conjunto fragmentado de herramientas para administrar tales activos digitales.

Por lo generar, utilizan una combinación de billeteras calientes y frías para administrar el capital, lo cual crea riesgos de seguridad operativos considerables y hace más complejos los informes.

Esta infraestructura de custodia a menudo se implementa en uno de estos tres métodos: auto custodia, custodia colaborativa y custodia de terceros. Como se puede evidenciar en la siguiente gráfica (Qredo, 2021).

Tabla 1 *Tipos de custodias y sus principales características*

Tipo de custodia	**Ventajas**	**Desventajas**	**Mecanismo de almacenamiento**	**Tiempo de liquidación (Bitcoin)**	**Reporte de transacciones**
Auto custodia	Control completo	Al perder las llaves se pierden los activos	Almacenamiento en frio	10 min – 2h	Manual
Custodia colaborativa	Riesgo reducido de pérdida de llaves	Riesgo de colusión	Almacenamiento frio multi firma	10 min – 2h	Manual
Custodia de terceros	No requiere conocimiento técnico	Riesgo de fallas por parte del custodio	Almacenamiento frio	10 min – 2h	Manual

(Fuente: Elaborado por el autor)

2.4.1. Auto custodia

A diferencia de inversionistas institucionales que están atados por normativas que hacen obligatorio usar un custodio cualificado, los tesoreros corporativos pueden seguir la visión de Satoshi Nakamoto de soberanía financiera (Norge, 2022) y tomar control total de sus activos digitales.

Este método es como administrar oro en una bóveda personal. Las empresas pequeñas pueden implementar la auto custodia, al almacenar los activos digitales en una billetera fría de una sola firma. La llave privada es almacenada en un enclave seguro en una USB, el cual puede ser conectado a escritorios o smartphones para firmar transacciones.

Ventajas

- Las billeteras de firma única confieren un control completo sobre los activos, lo que permite que un director ejecutivo o un oficial financiero realice transacciones rápidamente.

Desventajas

- Para todas las organizaciones, excepto las más pequeñas, es insostenible que un solo ejecutivo participe en cada transacción. Es posible compartir una billetera con diferentes miembros del personal, pero es engorroso y elimina la responsabilidad, ya que se vuelve difícil saber quién ha firmado cada transacción.
- Las billeteras de firma única crean un importante punto único de falla. Cualquiera que tenga la llave privada de la billetera podría morir y llevarse los fondos a la tumba, huir con los activos o ser víctima de un ataque de llave inglesa (Mg. 2021).

2.4.2. Multi firma

Si las billeteras de firma única son el equivalente a una bóveda de oro con una sola clave, las billeteras criptográficas multi firma son como una caja de seguridad con un número definido de llaves (M), de las cuales se necesita un número definido (N) para desbloquear la caja.

Esto normalmente se conoce como “M de N”, donde M es el número total de claves y N es el número requerido para autorizar transacciones. Por lo general 2 de 3 o 4 de 5 firmantes deben estar de acuerdo antes de que se apruebe una transacción.

Ventajas

- Las billeteras multi firma se pueden configurar con diferentes niveles de permiso, lo que permite que las claves se distribuyan entre los miembros principales del personal en esquemas de aprobación de varios pasos.

Desventajas

- Entre más firmas se necesiten para aprobar una transacción, más engorroso, lento y costoso se vuelve el proceso. Las transacciones en la cadena pueden tardar horas en liquidarse en *blockchains* congestionadas e incurrir en tarifas de dos o tres dígitos por tareas rutinarias simples.
- Las transacciones multifirma se pueden ver públicamente en la *blockchain*. Entonces, si se comparte la dirección (o llave privada), la cadena de transacciones queda expuesta. Esto podría revelar esquemas de firma y flujos de trabajo confidenciales a posibles atacantes.

2.4.3. Custodia colaborativa

La custodia colaborativa implica delegar permisos a un tercero que actúa como respaldo o cosignatario activo.

Los arreglos comunes de custodia colaborativa requieren que el propietario mantenga dos claves privadas en su posesión, cediendo la tercera a un servicio de semicustodia para reducir el riesgo de falla en un punto único.

Custodia colaborativa en cadena con multi firma

En un acuerdo de custodia colaborativa que utiliza una billetera criptográfica multifirma, un tesorero corporativo puede tener dos de las tres claves y darle una a un tercero.

Ventajas

- Mejora la seguridad operativa al compartir la carga de la administración de claves entre varias partes.

Desventajas

- Comparte las mismas desventajas que el multi firma ordinario y agrega un agujero de seguridad adicional en la forma de un tercero confiable.

2.4.4. Custodia de terceros

Los activos son depositados con un tercero de confianza. Los encargados de la tesorería corporativa pueden optar por delegar la custodia. Esto es el equivalente a depositar oro en una empresa de bóvedas y, por lo general, se logra utilizando billeteras criptográficas multisig (de múltiples firmas) controladas por un tercero.

Ventajas

- Entregar el cuidado de activos digitales a un custodio significa que no se necesitan conocimientos técnicos.

Desventajas

- Entregar activos a un tercero que puede congelarlos o restringir el acceso reduce el atractivo de refugio seguro de los cripto activos. Los activos pueden ser incautados o hackeados, lo que erosiona su capacidad para ofrecer a la empresa soberanía individual y privacidad financiera.
- En lugar de almacenar activos en cuentas segregadas, los cripto custodios a menudo mezclan activos en cuentas ómnibus opacas. Esto obliga a los propietarios de activos a confiar en el tercero, en lugar de poder verificar la posesión de los activos en la *blockchain*.
- La lista de cripto custodios insolventes crece cada año. Son diversos los casos en los que los custodios deciden realizar operaciones riesgosas, que pueden conducir a perder los fondos de sus clientes (Rosenberg, 2022) y posteriormente declararse en bancarrota sin ofrecer garantías de recuperación.

2.4.5. Conclusiones de las investigaciones relacionadas

Con base en la información evidenciada, es posible concluir que ningún método actual se puede considerar como el más apropiado para implementar la tesorería de criptomonedas en las organizaciones, de manera totalmente segura.

Sin embargo, al tener presente cada uno de estos métodos, es posible generar un potencial modelo de implementación híbrido, el cual puede contar con la capacidad de diversificar los riesgos operacionales que implica la custodia de dichos activos.

3. OBJETIVOS CONCRETOS Y METODOLOGÍA DE TRABAJO

En este capítulo se presenta la unión entre la problemática evidenciada y la contribución a realizar. A continuación, se describen los objetivos generales y específicos, y la metodología de trabajo a realizar para dar desarrollo al objetivo del proyecto.

3.1. Objetivo general

Documentar una serie de pasos y uso de tecnologías que permitan a las organizaciones tener cripto activos en sus portafolios de tesorería de manera digitalmente segura.

3.2. Objetivos específicos

- Estudiar las tecnologías que pueden hacer posible la custodia segura de cripto activos en las organizaciones
- Analizar los métodos que actualmente hacen posible la custodia segura de cripto activos en las organizaciones
- Facilitar el proceso de identificación de la categoría a la que una organización pertenece, respecto a sus capacidades y requerimientos de implementación
- Diseñar una serie de pasos y uso de tecnologías, que permitan a las organizaciones contar con custodia segura de cripto activos con base en sus necesidades y capacidades
- Implementar una prueba piloto de la implementación sobre una organización real
- Evaluar el nivel de la ciberseguridad de la implementación a través de una auditoría de controles y medidas ejecutadas

3.3. Metodología del trabajo

Este trabajo se enfoca en el desarrollo de una prueba piloto, que pueda ser implementada y probada en una organización real. Dicha prueba piloto será desarrollada sobre la organización AIDEL CORP SAS, establecida en Bogotá, Colombia. Tal procedimiento ha sido aprobado y autorizado por el representante legal de la organización, y cuenta con el apoyo del director de tecnología y director de finanzas de la compañía.

Debido a que existe la necesidad de realizar la implementación desde cero, la metodología del trabajo tiene presente 6 fases, que permitirán llevar a la organización desde un punto de

conocimiento reducido o nulo, hasta una implementación funcional con base en sus requerimientos.

- Fase 1: Identificación del contexto de la organización, con el fin de reconocer las capacidades y requerimientos de la organización
- Fase 2: Selección del método de implementación que satisfaga de mejor manera los requerimientos identificados en la Fase 1
- Fase 3: Elección de tecnologías necesarias para realizar la implementación, con base en el método seleccionado
- Fase 4: Puesta en marcha de las tecnologías elegidas
- Fase 5: Uso práctico de la tecnología que se ha puesto en marcha
- Fase 6: Conclusiones de la prueba piloto

4. Desarrollo específico de la contribución

4.1. Identificación del contexto de la organización

Para empezar, es necesario identificar cual es el tipo de organización sobre la cual se implementará la metodología. En este trabajo se identifican cuatro tipos de organizaciones que dependen de 1 variable cuantitativa y 2 cualitativas (Ministerio de comercio, industria y turismo, 2019), tales como:

Tabla 2 *Tipos de organizaciones y sus principales características*

Tipo de organización	Cantidad de empleados	Nivel de regulación	Velocidad de adopción de innovación
Startup	2-10	Muy bajo	Muy alto
Empresa pequeña	11-50	Bajo	Alto
Empresa mediana	51-200	Medio - Alto	Bajo - Medio
Empresa grande	>200	Alto	Bajo

(Fuente: Elaborado por el autor)

Una vez se haya identificado el tipo de organización objetivo, es necesario que el personal que implementará la solución tenga presentes las siguientes características que ofrecen las billeteras custodiadas y no custodiadas (Team T. B. P. , 2022):

Tabla 3 *Tipos de billeteras. Ventajas y desventajas*

Tipo de billetera	Ventajas	Desventajas

No custodiada	El usuario tiene control total de las llaves	Es imposible recuperar los activos si el usuario pierde las llaves privadas o frases de recuperación
	Crear nuevas billeteras es fácil y rápido	Se requiere mayor conocimiento técnico para hacer uso de funcionalidades avanzadas
	Los fondos no se verán impactados en caso de hackeo a un exchange	
	No se necesita seguir procesos de “Conozca a su cliente” o “Antilavado de dinero”	
	Acceso a más funcionalidades que las que ofrecen los servicios de custodia	
Custodiada	Menos responsabilidad por parte de los usuarios	Las llaves privadas son controladas por un tercero
	Uso simple, sencillo e intuitivo para los principiantes	Las billeteras custodiadas son estadísticamente más expuestas a hackeos
	Se puede reiniciar la contraseña para ganar acceso a los activos digitales	Se requiere seguir procesos de “conozca a su cliente” y “antilavado de dinero” para hacer uso de las cuentas

	Acceso y contacto a soporte técnico en caso de inconvenientes	Menos funcionalidades disponibles para usuarios experimentados

(Fuente: Elaborado por el autor)

Adicionalmente, identifican los siguientes 5 factores diferenciadores entre billeteras custodiadas y no custodiadas (Binance, 2022):

Tabla 4 *Diferencias entre billeteras custodiadas y no custodiadas*

	Billetera custodiada	**Billetera no custodiada**
Llave privada	Pertenencia del tercero que hace la custodia	Pertenencia del propietario de los fondos
Accesibilidad	Acceso solo a cuentas registradas	Accesible a cualquiera
Costos de transacción	Típicamente altos	Típicamente bajos
Seguridad	Dependiente de las medidas del tercero custodio	Típicamente alta
Soporte al cliente	Normalmente alto	Normalmente inexistente
Requerimientos de KYC	Si	No

(Fuente: Elaborado por el autor)

4.2. Identificación del método de implementación más adecuado

Una vez se identifique el tipo de organización que más se ajuste a las características mencionadas, y teniendo en cuenta las ventajas y desventajas de los tipos de billeteras

antedichas, es posible identificar en la siguiente tabla cual método de implementación es probablemente el más adecuado para cada caso.

Tabla 5 *Identificación del método de implementación con base en el tipo de organización*

Tipo de organización	Metamask	Qredo multisig	Ledger	Custodio (tercerización)
Startup	Muy recomendable. Apropiado para empresas que están iniciando, tienen nivel adquisitivo bajo y alta velocidad de innovación.	Recomendable. Apropiado para empresas que están iniciando, tienen nivel adquisitivo medio o bajo y alto nivel de innovación, y necesidad adicional de seguridad.	Recomendable. Apropiado para empresas que están iniciando, tienen nivel adquisitivo alto y alto nivel de innovación, y necesidad de diversificar la custodia de sus cripto activos.	No recomendable. La cantidad de burocracia necesaria para abrir cuenta con custodio, contradice la propiedad de alta velocidad de innovación.
Empresa pequeña	Recomendable. Apropiado para lanzar pruebas piloto o si la empresa cuenta con bajo nivel adquisitivo y alta velocidad de innovación.	Muy recomendable. Apropiado si la empresa cuenta con nivel adquisitivo medio y alta velocidad de innovación.	Recomendable. Apropiado si la empresa cuenta con nivel adquisitivo alto y requiere diversificar la custodia de sus cripto activos.	Recomendable. Apropiado si la empresa cuenta con nivel adquisitivo alto y requiere cumplir con normativas de la industria o la región.

Empresa mediana	No recomendable. Útil principalmente para lanzar pruebas piloto a bajo costo. No se recomienda si se van a tratar grandes cantidades de activos.	Recomendable. Apropiado si la empresa cuenta con nivel adquisitivo medio y alta velocidad de innovación.	Muy recomendable. Necesario para diversificar de manera segura la custodia de sus cripto activos.	Recomendable. Apropiado si la empresa cuenta con nivel adquisitivo alto y requiere cumplir con normativas de la industria o la región.
Empresa grande	No recomendable. Útil principalmente para lanzar pruebas piloto a bajo costo. No se recomienda si se van a tratar grandes cantidades de activos.	No recomendable. Útil principalmente para lanzar pruebas piloto a bajo costo o interactuar con cantidades pequeñas de cripto activos.	Recomendable. Necesario para diversificar de manera segura la custodia de sus cripto activos.	Muy recomendable. La empresa cuenta con nivel adquisitivo alto y es casi seguro que requiere cumplir con normativas de la industria o la región.

(Fuente: Elaborado por el autor)

4.3. Descripción de las soluciones de implementación

A continuación, se establece el detalle de cada una de las posibles soluciones de implementación mencionadas en la tabla anterior:

4.3.1. Metamask

MetaMask es una billetera de criptomonedas que permite a los usuarios acceder al ecosistema Web3 de aplicaciones descentralizadas (dapps). MetaMask es una de las cripto billeteras líderes y se basa en la integración del navegador web y un buen diseño para servir como una de las principales puertas de entrada al mundo de Web3, las finanzas descentralizadas (DeFi) y los NFT (Hussey, 2022).

Metamask se considera como una billetera de auto custodia, como se describe en el apartado 2.4.1. Auto custodia, de este documento. Debido a su naturaleza de conexión con internet, se considera como una billetera caliente, como se describe en el apartado 2.3.5. Tipos de billeteras, de este documento.

4.3.2. Qredo Multisig

Qredo es una billetera corporativa la cual hace uso de computación multi parte (MPC) junto con una red de capa 2, Qredo adicionalmente descentraliza las claves privadas. Este enfoque permite que los permisos de acceso a los activos se distribuyan de manera flexible entre los miembros de una organización, sin comprometer la seguridad o la accesibilidad.

Qredo se considera como una billetera multi firma, como se describe en el apartado 2.4.2. Multi firma, de este documento. (Qredo, 2022).

4.3.3. Ledger

Son billeteras que soportan múltiples criptomonedas que se utilizan para almacenar claves privadas para activos fuera de línea.

Tales billeteras se encuentran basadas en dispositivos, lo cual significa que utilizan mecanismos de almacenamiento (unidades USB) para salvaguardar claves privadas, lo cual hace más difícil el trabajo a piratas informáticos que intenten a la clave estando en línea. La billetera de Ledger, se considera como una billetera de auto custodia, como se describe en el apartado 2.4.1. Auto custodia, y debido a su naturaleza fuera de línea se considera un tipo de billetera fría, como se describe en el apartado 2.3.6. Tipos de billeteras. (Binance, 2022).

4.3.4. Custodia de terceros

Como se mencionó en el apartado 2.4.4., en la custodia de terceros, los activos son depositados con un tercero de confianza.

Esta solución contiene ventajas y desventajas que pueden ser validadas en el apartado anteriormente mencionado.

Existen diversos terceros que ofrecen esta implementación, se recomienda contactar al autor del presente trabajo, a través de ceo@aidelcorp.com o visitar el sitio web www.aidelcorp.com, para recibir información de la lista de las mejores instituciones, que actualmente ofrecen dicho servicio.

4.4. Prerrequisitos para una implementación eficaz

Antes de proceder con la implementación, ese necesario que la organización de respuesta a las siguientes preguntas:

- ¿Cuál es el presupuesto de la organización para invertir costos operativos únicos para la implementación?

  Usualmente a menos que se elija un servicio de custodio, el presupuesto será una única inversión, como es el caso de adquirir *hardware* para una billetera fría. Las opciones de Metamask y Qredo Multisig suelen no tener costo.

  El único costo que puede variar son las comisiones cobradas por transacciones sobre los cripto activos.

- ¿Cuál es el porcentaje de la tesorería que se tiene como objetivo para diversificar en cripto activos?

  Si se trata de una empresa que está empezando a familiarizarse con el ecosistema de los cripto activos, y se cuenta con un nivel adquisitivo medio o alto, se recomienda que no se destine un porcentaje mayor al 2% de la tesorería total.

  Este valor puede aumentar si la organización cuenta con un nivel adquisitivo bajo o se encuentra en etapa inicial de fundación.

- ¿Cuál es la persona o las personas responsables de liderar el proceso de implementación?

Al igual que cualquier proyecto, es necesario definir la o las personas que harán parte de dicho proyecto. Esto es fundamental para contar con un compromiso de responsabilidad sobre el equipo que realizará la implementación.

- ¿Qué recursos tecnológicos tiene la organización disponible para realizar el proceso de implementación?

  Normalmente las billeteras calientes como Metamask o Qredo requieren que sean instaladas sobre un computador de escritorio o un ordenador portátil.

  Las frases semilla requieren ser almacenadas de manera física o digitalmente segura, por esto es necesario identificar los recursos tecnológicos que se usaran para dicho propósito.

- ¿Cuál es el método de implementación que más se apega a la situación actual de la organización?

  Con base en la tabla anteriormente definida, la empresa deberá identificar con cual método de implementación encuentra mayor relación teniendo presentes sus capacidades y requerimientos.

4.5. Recomendaciones sobre selección de método de implementación

Una recomendación válida para cualquier tipo de empresa es la aproximación de empezar con el método de implementación más sencillo posible, de acuerdo con los recursos disponibles para implementar y los fondos a depositar.

Es decir, si una empresa es considerada como mediana, pero debido a su velocidad de adopción de tecnología puede llegar a ser considerada como pequeña, entonces se recomienda realizar la implementación con base en el método que mejor se ajuste a dicha categoría. Esto con la finalidad de disminuir los riesgos en los que incurre una compañía al intentar ingresar desde cero a la implementación segura de tesorería de criptomonedas.

Por otro lado, si el objetivo es realizar una custodia por terceros, entonces se recomienda entrar en contacto con ceo@aidelcorp.com o visitar el sitio web www.aidelcorp.com. Con el fin de analizar las opciones de los mejores custodios para ese momento.

Finalmente, sin importar el tipo de método a implementar se recomienda que las primeras transacciones sean fraccionadas, y que se realice una transacción de prueba para validar que se tiene conocimiento apropiado del proceso con poco riesgo.

Ejemplo: Se planea invertir la cantidad de $10.000 dólares en cripto activos.

- Por lo tanto, dicha inversión se realizará en 5 partes, cada una de ellas de un monto de $2.000 dólares.
- Por otro lado, la primera transacción a realizar será una de prueba, por un monto de $100 dólares.

5. Implementación con base en Metamask

5.1. Seguridad pre-implementación

Requerimientos:

- Computador
- Conexión a internet
- Navegador de internet que soporte Metamask: Chrome, Firefox, Brave, Edge, Opera (Metamask. 2022)

1. **Computador nuevo**

   No es necesario adquirir un computador nuevo para dicho propósito, pero puede llegar a ser una opción recomendable para minimizar la probabilidad de existencia de programas maliciosos previamente instalados.

2. **Formateo de computador**

   Si el computador sobre el cual se realizará la implementación ha sido usado para descargar, almacenar o ejecutar programas crackeados o pirateados, es necesario realizar un formateo para minimizar la probabilidad de existencia de programas maliciosos previamente instalados.

3. **Actualización de sistema operativo**

   Actualizar el sistema operativo del computador a su última versión a través de la herramienta nativa del sistema.

4. **Antivirus**

   Si el computador no cuenta con antivirus, es necesario realizar la instalación de alguno.

   Existen diversas opciones en el mercado y a lo mejor la organización actualmente cuente con licencias para tal tipo de software, sin embargo, si ese no es el caso, se recomienda la solución de antivirus de Sophos Home con versión gratuita https://my.sophos.com/es-es/download/ (Sophos, 2022).

5. **Manejador de contraseñas**

   Para almacenar de manera segura las contraseñas necesarias para acceder a la solución de Metamask, se recomienda fuertemente hacer uso de un manejador de contraseñas.

Existen diversas opciones en el mercado y a lo mejor la organización actualmente cuente con licencias para tal tipo de software, sin embargo, si ese no es el caso, se recomienda la solución de manejador de contraseñas de Bitwarden con versión gratuita https://bitwarden.com/download/ (Bitwarden, 2022)

Contraseña del manejador de contraseñas

Es necesario asignar una contraseña al manejador de contraseñas, si la contraseña asignada no es segura, entonces esta se convierte en una potencial vulnerabilidad y punto único de fallo.

Como buena práctica se recomienda usar como contraseña una frase larga, compleja, pero sobre todo fácil de recordar. De modo que para quien se encarga de administrar la solución no tenga la necesidad de apuntar la contraseña en texto plano, creando así otra potencial vulnerabilidad.

6. **Protecciones sobre WiFi**
   - Se recomienda cambiar la clave de la red WiFi que viene configurada por defecto
   - También se recomienda cambiar las credenciales por defecto de administración del router de WiFi si aún no se ha hecho
   - Adicionalmente, es recomendable desactivar la red WiFi y acceder a internet solo a través de la conexión de un cable de Ethernet
   - Finalmente, si es posible se recomienda actualizar el *firmware* del router para disminuir potenciales superficies de ataque
7. **DNS seguro**

   Se recomienda hacer uso de un DNS seguro, esto con el fin de evitar ataques de suplantación y sitios maliciosos cuando se navega a través de internet. Existen diversas opciones de configuración, pero entre las más populares se encuentra la de Cloudflare, usando los servidores 1.1.1.2 y 1.0.0.2 (Helena, 2020).

   Para realizar esta configuración, se recomienda el siguiente paso a paso: https://developers.cloudflare.com/1.1.1.1/setup/windows/

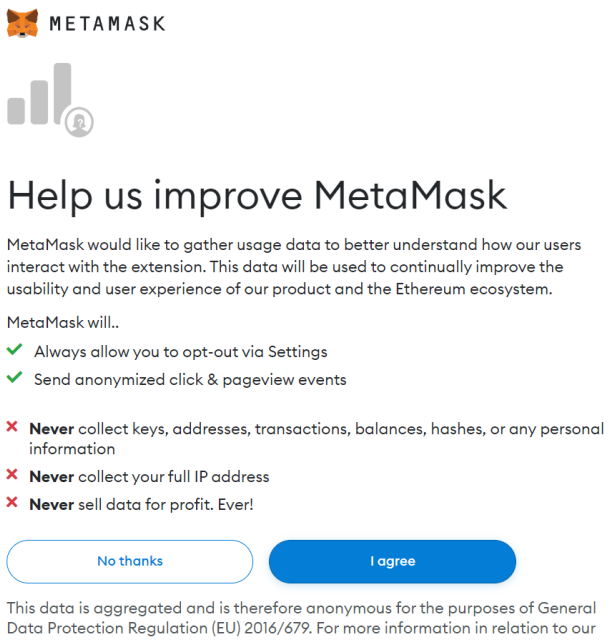
5.2. Seguridad implementación

1. Instalación de Metamask en el navegador

Acceda desde el computador al sitio web https://metamask.io/download/ e instale la extensión de Metamask para su navegador de internet.

2. Creación de cripto billetera
    a. Una vez se instale la extensión de navegador, se abrirá la siguiente ventana, seleccione la opción que prefiera

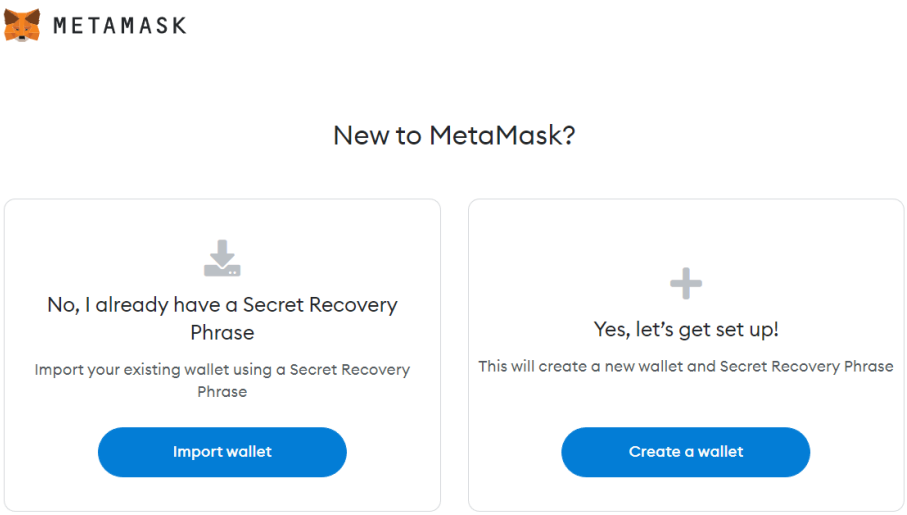
Ilustración 1 *Términos y condiciones de Metamask*



(Fuente: Metamask 2022)

    b. Seleccione la opción de crear una billetera. Create a wallet.

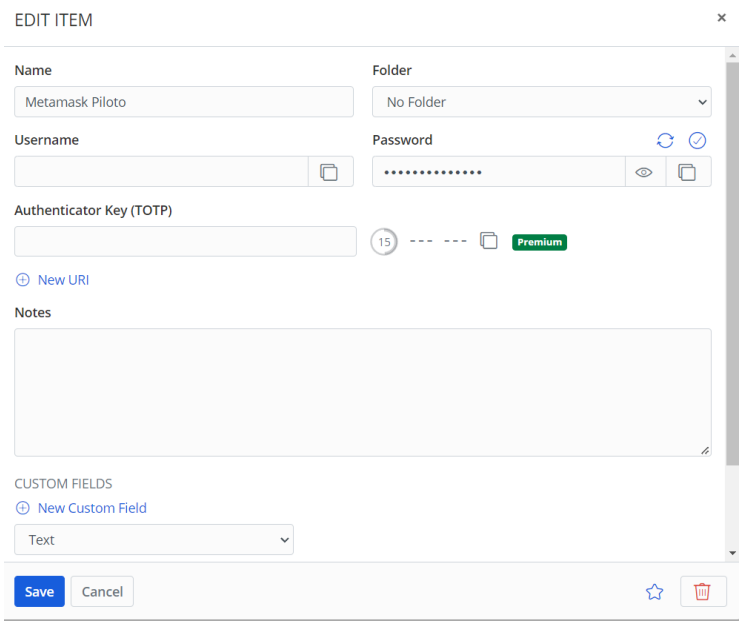
Ilustración 2 *Creación de billetera de Metamask*



(Fuente: Metamask 2022)

3. Use el manejador de contraseñas para crear una nueva contraseña que será utilizada en la billetera de cripto.

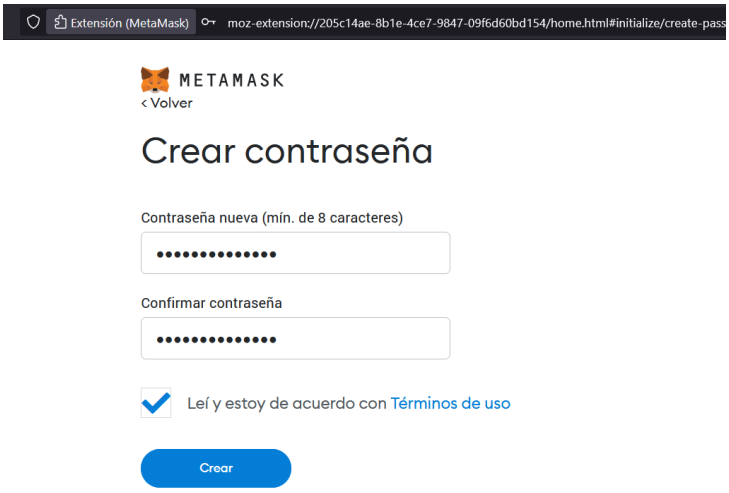
Ilustración 3 *Creación de nueva contraseña segura*



(Fuente: Bitwarden (2022))

Ingrese con la contraseña creada y continue con el proceso.

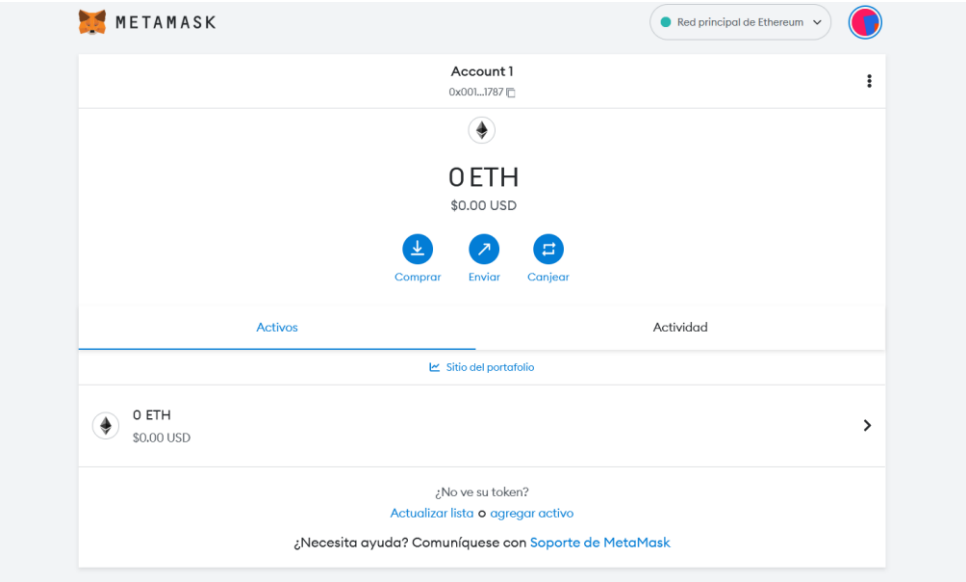
Ilustración 4 *Asignación de nueva contraseña segura*



(Fuente: Metamask (2022))

4. Apunte la frase secreta de recuperación creada por la herramienta, se recomienda usar el mismo administrador de contraseñas Bitwarden, para almacenar dicha información de manera segura.

Ilustración 5 *Visualización de cuenta creada*



(Fuente: Metamask (2022))

5. Es necesario tener presente que la llave privada, conocida como frase de recuperación no se puede recuperar o cambiar por ningún motivo ya que es la información que da acceso total a la billetera, en caso de extraviarla será equivalente a perder todos los fondos depositados en la billetera.

Finalmente, ya que se trata de información sensible, se resalta la importancia de tener cuidados adicionales al crear la billetera y obtener la frase semilla. Estos cuidados son similares a los que se tendrían con el PIN de una cuenta bancaria, entre ellos:

- Tener cuidado al digital la frase semilla y la contraseña, ya que una persona que se encuentre cerca puede llegar a visualizarla
- Nunca comparta su frase semilla o contraseña con terceros, recuerde que ninguna institución o persona le solicitará esta información

5.3. Seguridad pos-implementación

1. **Uso de VPN**

   Se recomienda el uso de servicios de VPN con el fin de cifrar la información que se transmite en internet. Es una medida que se debe considerar seriamente si se cuentan con transacciones de alto volumen o alta frecuenta.

   Por otro lado, el uso de VPN es indispensable si se están haciendo operaciones desde un país con regulaciones en contra de los cripto activos o las finanzas descentralizadas.

2. **Nunca acceder a conexiones a través de redes WiFi-públicas**

   Las redes de WiFi públicas son el medio principal a través del cual los cibercriminales logran ataques de hombre en el medio. Conectarse a una red de WiFi pública se debe considerar como una actividad altamente riesgosa, y por lo tanto nunca se debe considerar sobre un dispositivo que se utiliza para la implementación de tesorería de criptoactivos.

3. **Conexiones a internet desde cable**

   Debido a la naturaleza de la información transmitida, se recomienda eliminar el uso de conexiones a internet a través de redes WiFi, aún dentro de la propia oficina, y fomentar el uso de conexiones a internet a través de cable, las cuales no son susceptibles a ser interceptadas por atacantes con dispositivos de escucha de redes inalámbricas.

6. Implementación con base en Qredo

6.1. Seguridad pre-implementación

Requerimientos:

- Computador
- Conexión a internet
- Al menos 2 direcciones de correo electrónico de diferentes propietarios
- Navegador de internet, posibles opciones: Chrome, Firefox, Brave, Edge, Opera
- Al menos 2 smartphones de diferentes propietarios

Direcciones de correo electrónico relacionadas

Se menciona el requerimiento de 2 direcciones de correo electrónico de diferentes propietarios, ya que esta implementación está enfocada en múltiples firmas para autorizar las operaciones, por tal motivo, solo hace sentido cuando existe más de 1 cuenta relacionada. Por otro lado, se recomienda usar las direcciones de correo electrónico con propósito exclusivo para actividades relacionadas con la implementación. Esto con el fin de intentar reducir la cantidad de ataques que se puedan llegar a presentar en dicho contexto.

Smartphones para utilizar

Adicionalmente, debido a la naturaleza multifirma anteriormente mencionada, se recomienda hacer uso de smartphones seguros, con base en los siguientes criterios:

- Deben contener la mínima cantidad de aplicaciones necesarias para poder funcionar
- Deben utilizarse para actividades relacionadas con la implementación
- Deben estar actualizados a la versión más reciente de su sistema operativo
- En el caso de Android, no deben haber pasado por procesos de *rooting*
- En el caso de iOS, no deben haber pasado por *jailbreaking*

Medidas de seguridad adicionales

Como pasos de seguridad pre-implementación, se recomienda tomar las medidas 1, 2, 3, 4, 5, 6 y 7 del numeral 5.1 perteneciente al capítulo 5: Implementación con Metamask.

6.2. Seguridad implementación

1. **Creación de cuenta en el portal de Qredo**

1.1. Acceda al sitio oficial de registro del portal de Qredo https://qredo.network/register

1.2. Ingrese los datos de un correo electrónico que pueda asegurar que no se haya visto comprometido en ningún ataque o incidente de filtración de datos, que posteriormente pueda afectar la seguridad de la implementación. Se recomienda hacer uso del sitio https://haveibeenpwned.com/ para realizar esta validación.

1.3. Ingrese una contraseña segura, haciendo uso de un administrador de contraseñas, tal como se menciona en la medida número 5, del numeral 5.1 perteneciente al capítulo 5: Implementación con Metamask.

1.4. Acepte los términos y condiciones

1.5. Valide su dirección de correo electrónico

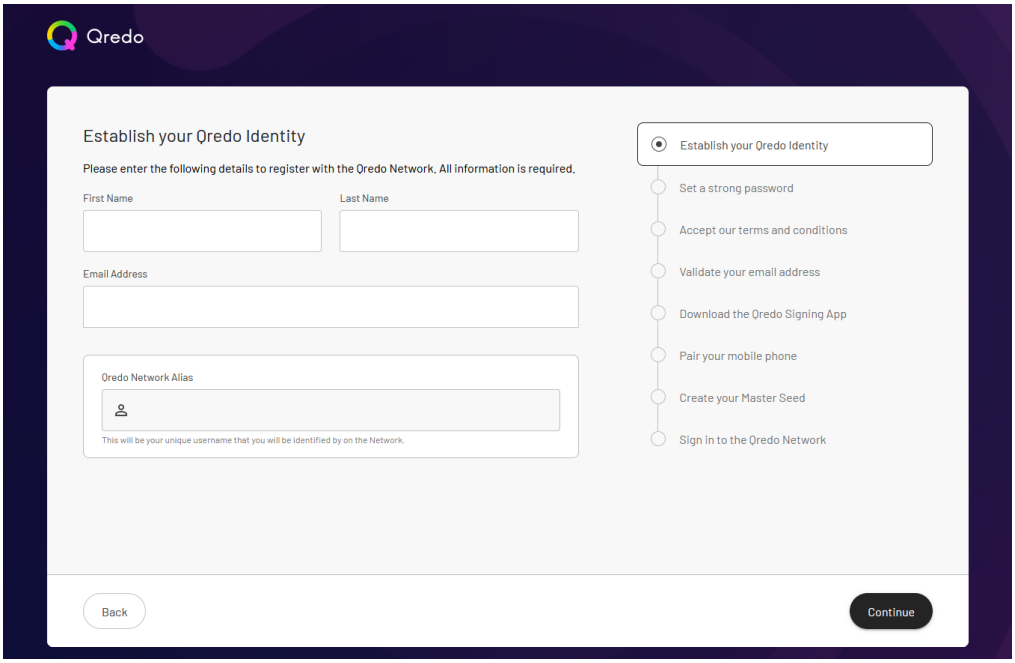
1.6. Descargue la aplicación de inicio de sesión de Qredo en uno de los smartphones mencionados en el apartado de requerimientos pre-implementación

1.7. Empareje su dispositivo móvil

1.8. Cree su semilla maestra para garantizar la seguridad de la cuenta

1.9. Haga inicio de sesión en la red de Qredo

Ilustración 6 *Creación de cuenta en el portal de Qredo*



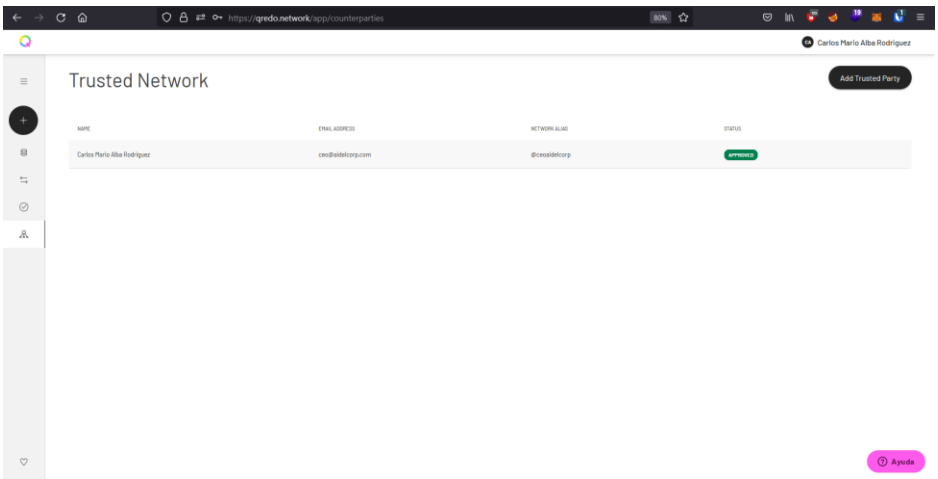
(Fuente: Qredo (2022))

6.3. Seguridad pos-implementación

La seguridad adicional que puede proveer la implementación multifirma de Qredo, depende principalmente de la cantidad de direcciones de billeteras que tengan que firmar una transacción para ser aprobada. Por este motivo se recomienda realizar la siguiente serie de pasos:

1. Una vez creada la cuenta, añada una parte de confianza a la red de confianza

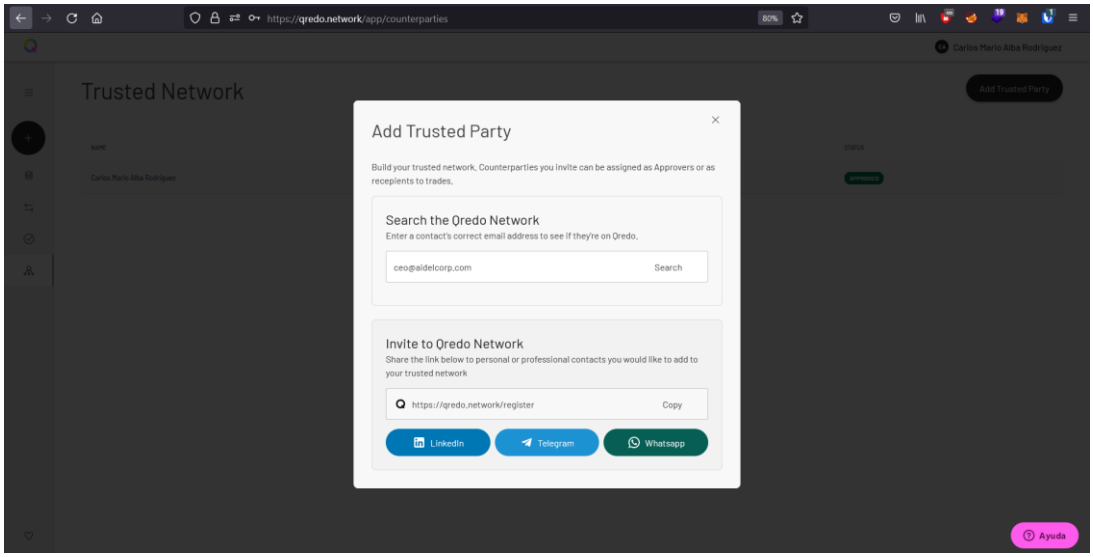
Ilustración 7 *Añadida una parte de confianza en la red*



(Fuente: Qredo (2022))

2. Si la parte de confianza aún no ha creado cuenta en la red de Qredo, es posible enviarle una invitación a través de distintos medios. Una vez la parte de confianza posea una cuenta, ingrese su dirección de correo electrónico y añada su usuario a la red de confianza.

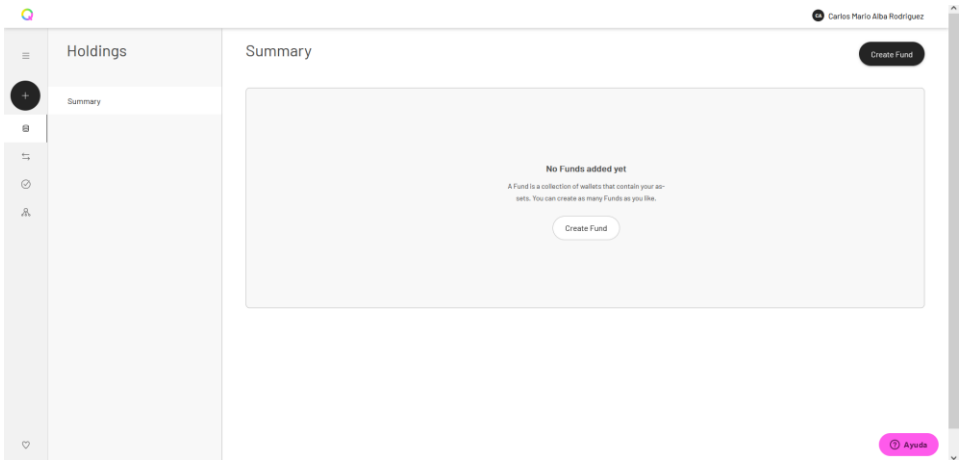
Ilustración 8 *Añada parte confiable o envíe una invitación de acceso*



(Fuente: Qredo (2022))

3. Una vez creada la cuenta, crear un fondo, el cual es una colección de billeteras que contienen los cripto activos

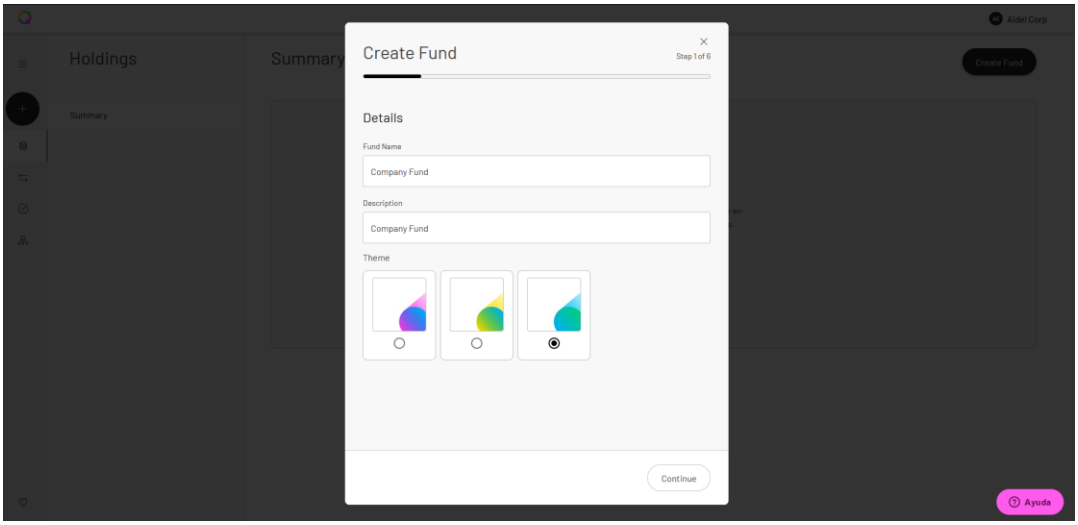
Ilustración 9 *Cree un fondo en la red de Qredo*



(Fuente: Qredo (2022))

4. Ingrese los detalles del fondo a crear

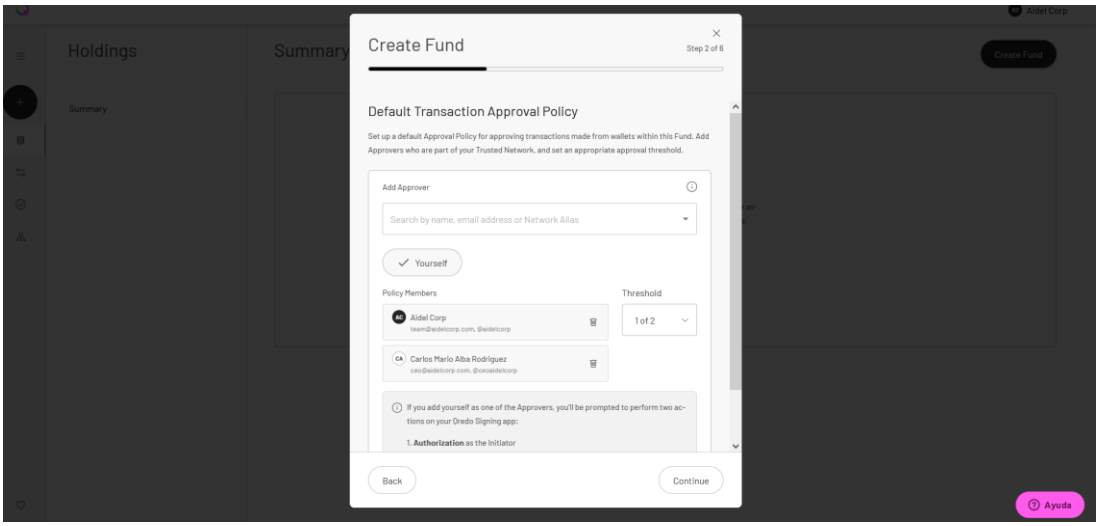
Ilustración 10 *Ingrese los detalles del fondo a crear*



(Fuente: Qredo (2022))

5. Añada en los miembros de la política de transacciones al menos uno de los miembros de su red de confianza. Este es uno de los puntos más cruciales en la seguridad pos-implementación, ya que habilita las funcionalidades de multifirma de cripto billeteras.

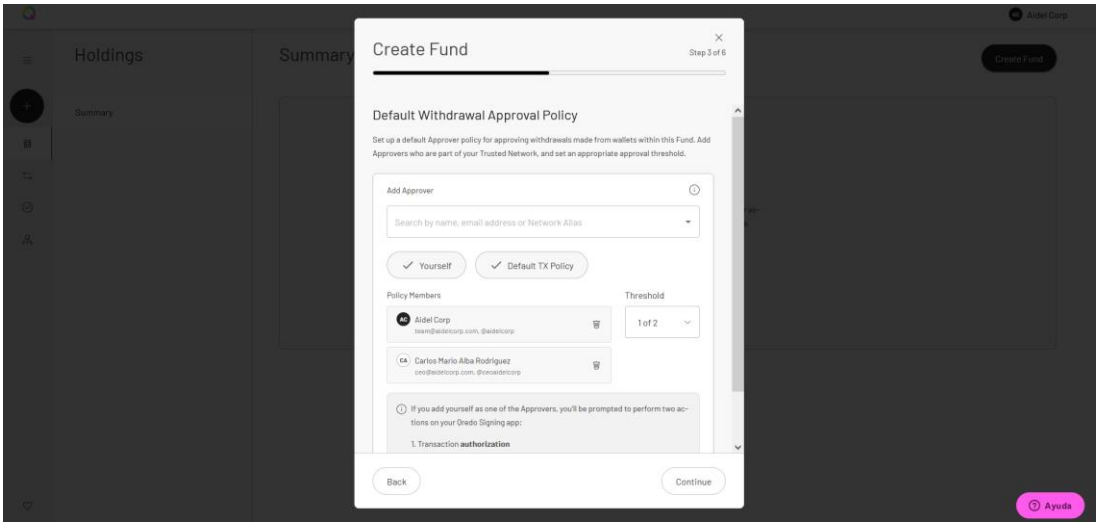
Ilustración 11 *Añada seguridad a la política de transacciones*



(Fuente: Qredo (2022))

6. Adicionalmente, añada también en los miembros de la política de retiros al menos uno de los miembros de su red de confianza.

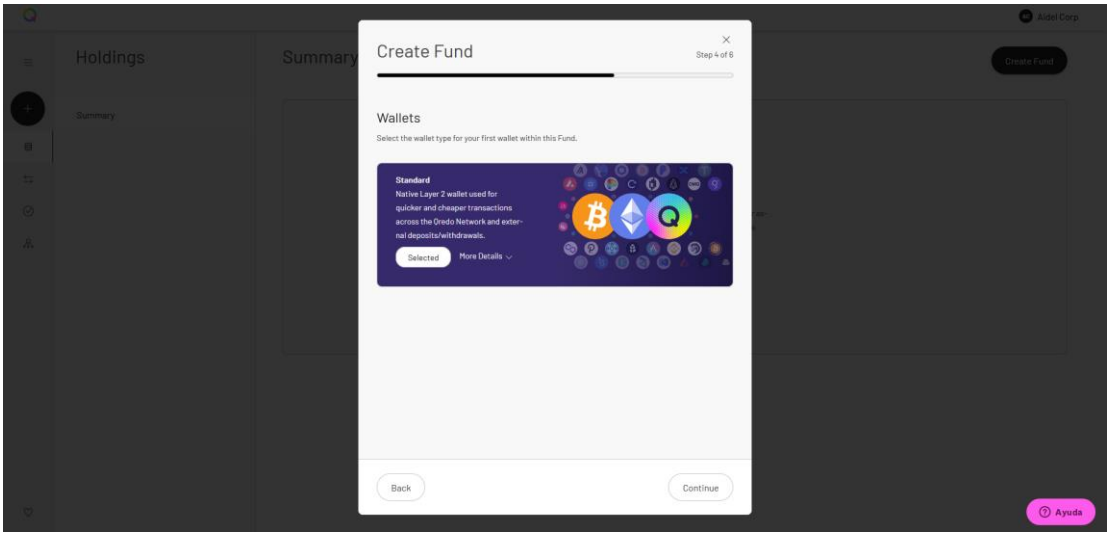
Ilustración 12 *Añada seguridad a la política de retiros*



(Fuente: Qredo (2022))

7. Seleccione la opción estándar en el apartado de creación de billeteras

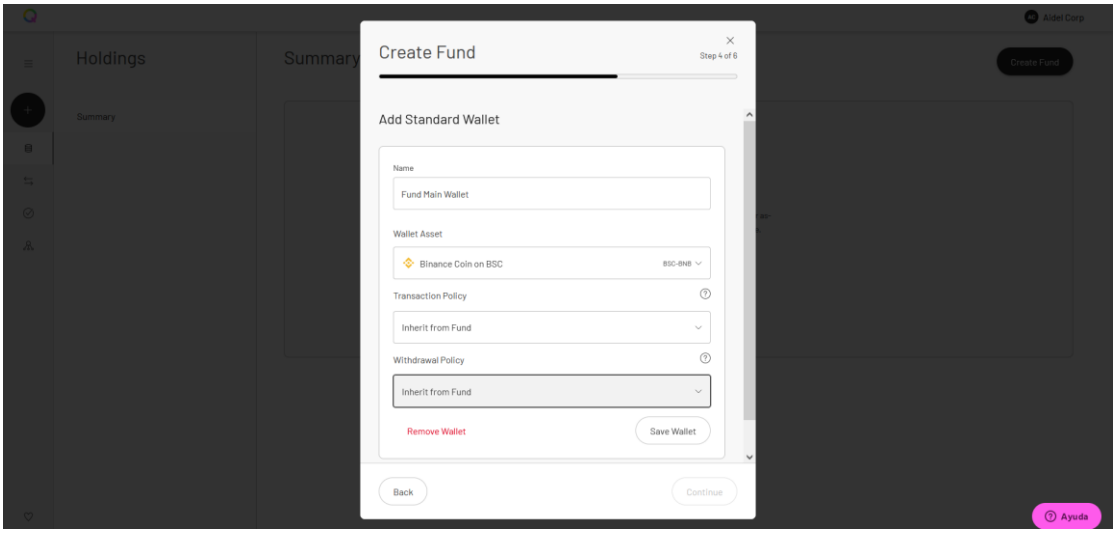
Ilustración 13 Cree una billetera dentro del fondo



(Fuente: Qredo (2022))

8. Ingrese los datos necesarios para la creación de la billetera, esta será el equivalente a una billetera de Metamask, independientemente del activo que se maneje en dicha billetera.

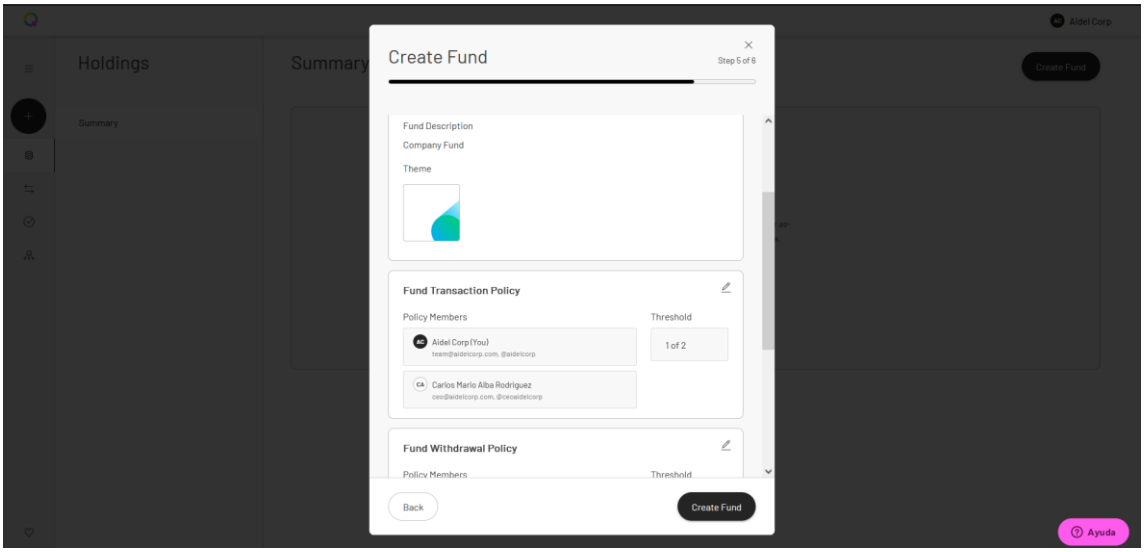
Ilustración 14 *Ingrese los datos para la creación de la billetera*



(Fuente: Qredo (2022))

9. Confirme los datos y proceda a crear el fondo si los datos son correctos

Ilustración 15 *Ingrese los datos para la creación del fondo final*

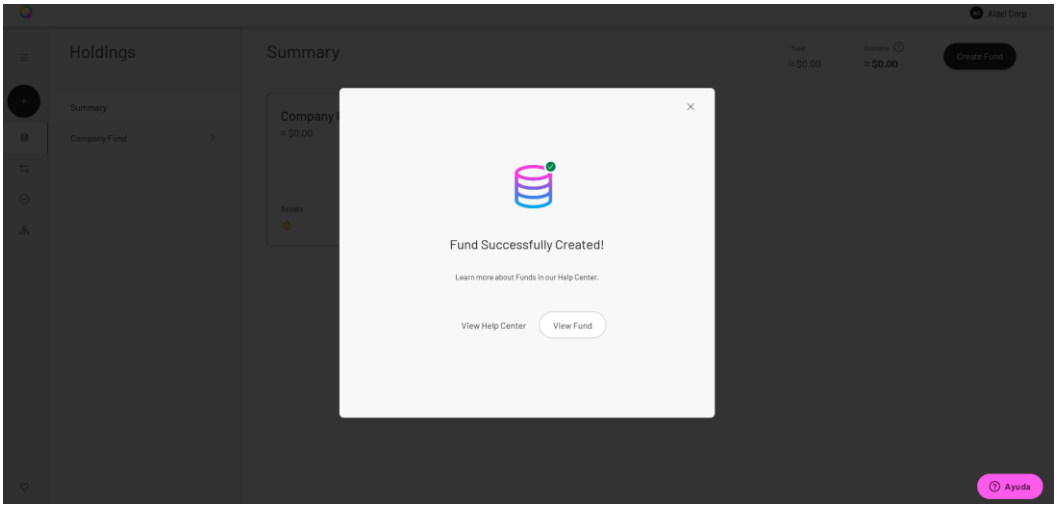


(Fuente: Qredo (2022))

10. Si los pasos fueron seguidos apropiadamente, actualmente cuenta con una billetera multifirma, la cual necesitará la aprobación de al menos una segunda cuenta para realizar transacciones con los fondos allí almacenados.

El método de Qredo añade seguridad al solicitar dicha confirmación a través del smartphone que se emparejó en el proceso de pre-implementación.

Ilustración 16 *Validación de la creación realizada*



(Fuente: Qredo (2022))

Medidas de seguridad adicionales

Como pasos de seguridad pos-implementación, se recomienda tomar las medidas 1, 2 y 3 del numeral 5.3, perteneciente al Capítulo 5: Implementación con Metamask.

7. Implementación con base en Ledger

7.1. Seguridad pre-implementación

Requerimientos:

- Computador
- Un dispositivo Ledger

Compre el dispositivo a un vendedor confiable

Debido a la naturaleza de almacenamiento de activos de alto valor en dichos dispositivos, existe una gran cantidad de atacantes que buscan suplantar, falsificar o alterar este tipo de elementos. Por esta razón es necesario comprar el dispositivo directamente desde la web oficial del sitio de la compañía o desde el perfil oficial del proveedor en tiendas globalmente reconocidas:

- https://shop.ledger.com/
- https://www.amazon.com/stores/Ledger/Ledger/page/D665D2FA-1FBB-4A5F-953C-15AC875BC674
- https://www.ledger.com/reseller

Valide el dispositivo una vez comprado

Una vez adquirido el dispositivo por parte de un vendedor confiable, tenga presente los siguientes puntos para validar si el dispositivo es seguro:

- Validaciones visuales:
  - Compruebe del estado de la caja, asegúrese de que no esté dañada ni abierta
  - Compruebe que el contenido de la caja está perfectamente en su lugar
  - Compruebe el estado de la hoja de Recuperación: debe estar vacía
- Validación técnica: Ataque pre-semilla.

  Cuando se configura el dispositivo Ledger, parte del proceso es generar una frase de recuperación de 24 palabras.

La frase de recuperación es fundamental para la seguridad del dispositivo. Si alguien más la supiera, podría robar todos los criptoactivos que se lleguen a almacenar en el dispositivo Ledger.

Solo usted está a cargo de generar la frase y escribirla en la hoja de frase de recuperación que viene con el dispositivo. Esta hoja es una parte del control de seguridad: si ya se han completado con palabras, significa que el dispositivo ha se ha manipulado y no es seguro de usar en lo absoluto. Esto se conoce como "ataque de pre-sembrado". La preconfiguración es cuando un atacante ingresa la frase inicial de su propia billetera en su hoja de frases de recuperación, con la esperanza de que una víctima la ingrese en su dispositivo. Hacer esto le da al atacante el control completo de lo que almacene en su dispositivo desde ese punto.

Uso de la aplicación genuina de Ledger

La aplicación Ledger Live es la plataforma donde se puede administrar y visualizar los cripto activos almacenados, así como acceder al amplio ecosistema de cripto a través de las aplicaciones nativas del proveedor. Es necesario validar que se usa la aplicación correcta al descargarla del sitio web oficial de la organización. [35]

- https://www.ledger.com/ledger-live/download

Medidas de seguridad adicionales

Como pasos de seguridad pre-implementación, se recomienda tomar las medidas 1, 2, 3, 4, 5, 6 y 7 del numeral 5.1 perteneciente al capítulo 5: Implementación con Metamask, sobre el computador a utilizar.

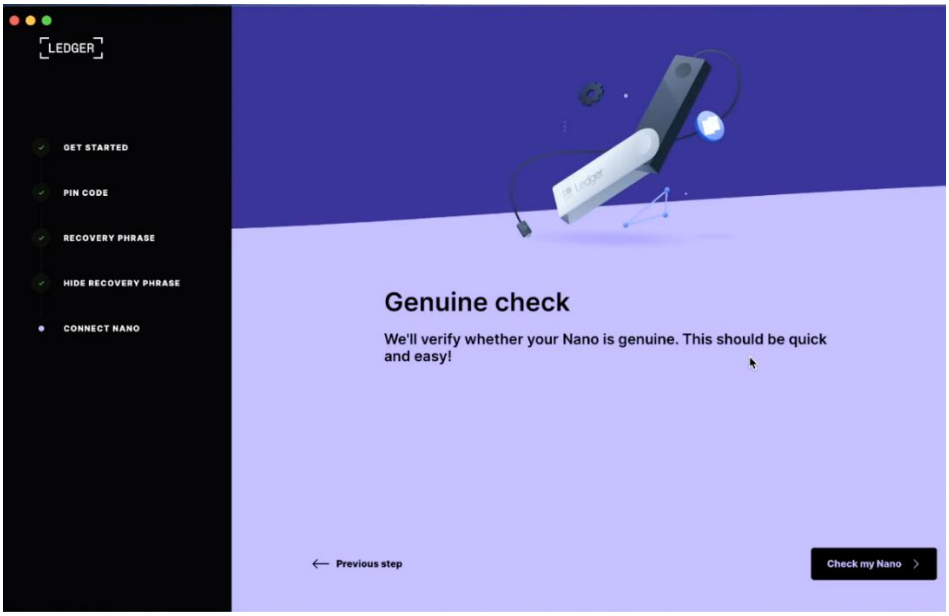
7.2. Seguridad implementación

Una vez se descargue la aplicación oficial mencionada en el punto anterior, tan solo es necesario seguir los pasos que la plataforma indica para lograr una implementación exitosa.

Dentro de los pasos a seguir (Ledger Support, 2022), se destacan los siguientes para validar que el método de implementación cumpla con todos los estándares de seguridad necesarios:

1. Realice una validación para comprobar que el dispositivo es genuino: Para este paso solo es necesario dar clic en el botón *Check my nano*.

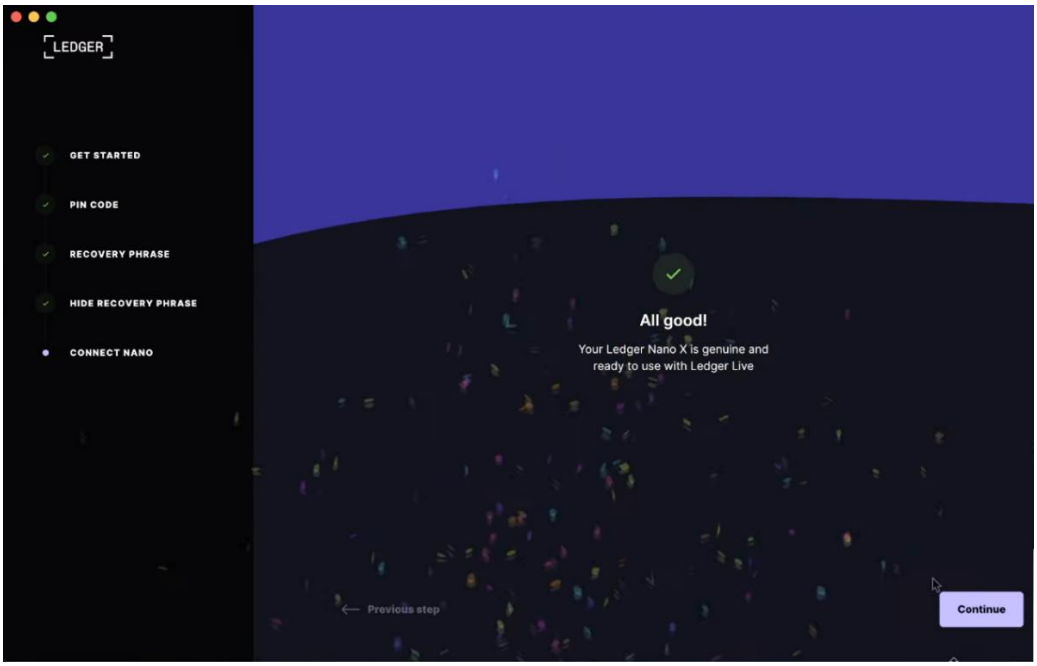
Ilustración 17 *Verificación genuina del dispositivo Ledger*



(Fuente: Ledger (2022))

2. Si el dispositivo es genuino aparecerá un mensaje similar al siguiente.

Ilustración 18 *Éxito en la validación del dispositivo*



(Fuente: Ledger (2022))

Para finalizar, siga los pasos indicados en la aplicación para terminar con el proceso de implementación con base en Ledger.

7.3. Seguridad pos-implementación

Una vez se finalice la implementación con base en los pasos indicados en la aplicación, es necesario tener presente los siguientes puntos para garantizar la seguridad de los cripto activos.

1. Recuerde que la frase de recuperación es una serie de 24 palabras, las cuales deben ser escritas en una hoja que debe ser almacenada de manera segura. Nunca deben ser compartidas, fotografiadas o transcritas a un medio digital como un archivo de notas o un documento Word.
2. Es indispensable usar siempre la aplicación legítima de Ledger Live, la cual está disponible en ledger.com
3. Durante el proceso de implementación fue necesario crear un PIN de seguridad el cual se digita directamente en el dispositivo. Recordar este PIN también es vital,

pero la frase de recuperación puede ayudarle a recuperar el acceso a los cripto activos si olvidó dicho PIN.

4. Si perdió la frase de recuperación, pero aún tiene acceso a su dispositivo y el PIN que creó, igualmente puede recuperar el acceso a los cripto activos.
5. Si ambos se pierden, todos los cripto activos se volverán inaccesibles
6. También es vital mantener la frase de recuperación segura, fuera de línea y fuera del alcance de cualquiera. (Moreland, 2022).

8. Implementación con base en plataforma de intercambio

La implementación con base en plataformas de intercambio es propia de cada plataforma y la serie de pasos para ejecutarla está detallada en su respectiva documentación. Se recomienda escribir a ceo@aidelcorp.com solicitando la lista actualizada de plataformas de intercambio consideradas seguras.

No obstante, existe una lista universal de recomendaciones a tener presente, las cuales se pueden llevar a cabo para realizar una implementación segura a través de una plataforma de intercambio. (Coinbase, 2022)

1. **Uso apropiado**

   El uso apropiado de las plataformas de intercambio es el de realizar la conversión de dinero local (pesos, dólares, euros, etc.) a cripto activos. No es recomendable utilizar dichas plataformas para intentar administrar grandes sumas de dinero o para almacenar los fondos por un largo periodo de tiempo.

2. **Validar el uso de un email seguro**

   Antes de registrarse en alguna plataforma de intercambio, se recomienda hacer uso del sitio https://haveibeenpwned.com/ para validar que el email que está intentando utilizar para crear la cuenta de la plataforma de intercambio, no se haya visto comprometida en ningún ataque o incidente de filtración de datos que posteriormente pueda afectar la seguridad de la implementación.

3. **Contraseña segura**

   Aun cuando la custodia de los activos esté a manos de un tercero es necesario contar con una contraseña segura, por lo tanto, se recomienda usar una creada a través de un administrador de contraseñas.

4. **Mecanismos de seguridad adicionales**

   Activar todos los mecanismos de seguridad adicionales como palabra de anti-phishing y autenticación de dos pasos. Dichos mecanismos dependen de la plataforma de intercambio y son establecidos desde sus propios portales.

5. **Envío de información en el mercado P2P**

Se recomienda abstenerse de enviar información personal o corporativa a terceros al momento de hacer compras P2P. La información compartida con terceras partes debe limitarse estrictamente a lo necesario para realizar y validar la transacción en proceso.

6. **Contacto a servicio al cliente**

   A diferencia de los métodos de implementación anteriormente mencionados, tan solo el método de plataforma de intercambio cuenta con servicio al cliente. Cada vez que se tenga una duda sobre seguridad o se presente una situación anómala, se recomienda contactar el servicio al cliente a través de los canales oficiales.

   Es necesario tener presente que los números y sitios web falsos de servicio al cliente son un peligro constante, por lo tanto, se requiere tener precaución con la información que se encuentra vía foros, redes sociales y anuncios de Google.

   Como regla general, el personal de una plataforma de intercambio nunca:

   - Preguntará por contraseñas, códigos de verificación de dos pasos
   - Pedirá instalar inicios de sesión o software de soporte técnico en su computador
   - Pedirá enviar dinero para resolver problemas con su cuenta
   - Le llamará directamente para manejar asuntos de soporte técnico o arreglar problemas (Coinbase, 2022)

9. MEDIDAS DE SEGURIDAD GENERALES

1. **Diversificación de riesgos**

   Debido a la naturaleza del tipo de activos a manejar se recomienda distribuir los fondos en al menos dos tipos diferentes de cripto billeteras y/o métodos de custodia. Esto con el fin de diversificar el riesgo de pérdida total de fondos debido a cualquier posible ataque o vulnerabilidad en la infraestructura que se pueda presentar en el futuro.

2. **Acuerdos de confidencialidad**

   Se recomienda hacer firmar al personal relacionado con la implementación, un acuerdo de confidencialidad el cual prohíba a los colaboradores divulgar información relacionada con la posesión de cripto activos por parte de la organización, cantidades y procesos relacionados.

   Dicha medida de seguridad es con el fin de evitar potenciales *5 USD wrench attack*, traducido como ataque de llave inglesa de 5 dólares. Este tipo de ataques tienen presente que el nivel de seguridad tecnológico es alto, por lo tanto, la opción más viable es atacar físicamente a la persona objetivo con tortura física, secuestros, extorsiones, etc. El objetivo es torturar a la víctima hasta que suministre información de como acceder a los activos de la organización. (Sun, 2022).

3. **Acceso a links y URLS**

   Nunca se debe acceder a un enlace o URL que le comparta un tercero que no conoce. Aunque conozca el sitio al cual se le solicita acceder, solo acceda al mismo a través de su propia búsqueda por internet del sitio oficial y añada dicho sitio a su lista de favoritos en su navegador.

4. **Limpieza de dispositivo**

   Desinstale todos los programas y piezas de software de su dispositivo que no utilice a menudo, especialmente herramientas que permitan acceso remoto.

5. **Bloqueador de anuncios**

   Instale un bloqueador de anuncios en su navegador para ayudarle a protegerse de anuncios maliciosos, los cuales continuamente aparecen cuando se navega a través de la web.

6. **Higiene de la navegación**

Practique hábitos de navegación web seguros y nunca haga clic en enlaces sospechosos ni descargue programas sospechosos.

7. ***Plug-ins* o *add-ons* inseguros**

   No instale ni utilice *plug-ins* ni *add-ons* de navegadores que hayan sido desarrollados por terceros desconocidos.

8. **Active el bloqueador de pantallas**

   Active el bloqueador de pantallas de la máquina sobre la cual se hará la implementación, esto con el fin de asegurar que solo el usuario legitimo tendrá acceso a la información que allí se almacena. Dicha medida realiza un bloqueo automático del dispositivo cada cierto periodo de tiempo después de detectar inactividad.

9. **Validación de fondos provenientes de billeteras en listas negras**

   Antes de recibir fondos de una billetera a través de una transacción entre pares, se recomienda validar con quién realizará el pago cual es la dirección desde la cual se enviarán los activos.

   El objetivo es validar si dicha dirección se encuentra registrada en listas negras, debido a que existe la posibilidad de que esta pueda haber incurrido en actividades criminales. Esta medida de seguridad permite evitar involucrarse en actividades de lavado de activos o financiación del terrorismo, y demostrar un sentido de responsabilidad si la organización se llega a ver comprometida con alguna investigación relacionada.

   Algunos de los exploradores pueden ser útiles para desarrollar este tipo de validaciones son:

   - https://www.enhancetoken.net/blacklist-wallets
   - https://info.etherscan.com/ethprotect/

10. **Asociación de nombres de dominio y direcciones de billeteras**

    Debido a que las direcciones de cripto billeteras suelen ser largas cadenas de texto de caracteres hexadecimales, estas tienden a ser complicadas de administrar y utilizar.

    Por tal motivo, se recomienda hacer uso de enlaces que permitan asociar la dirección de la cripto billetera con un dominio que sea posible recordar y administrar por humanos.

    Un ejemplo de este servicio son los *Unstoppable domains*, los cuales permiten crear dominios de diversas extensiones. Ej., .crypto, .blockchain, .nft, .etc. y asociarlos con

una billetera. Una vez asociados, es posible realizar transferencias a dicho dominio en lugar de la dirección de la cripto billetera, es decir:

Normalmente una dirección de cripto billetera se ve de esta manera: b4b9301afddf380f6ec5026d6beb85d196f38e9f6d93d0c4515eadc159b6cf47

Con un *Unstoppable domain* es posible adquirir un cripto dominio, Ej. empresa.crypto, este dominio se puede asociar con la dirección de la billetera.

De este modo, el usuario que realizará el depósito en la próxima transferencia en lugar de ingresar toda la dirección de la cripto billetera, tan solo necesitará digitar el dominio empresa.crypto y el servicio de *Unstoppable domains* se encargará de hacer la dirección de los fondos hacia la cuenta que se haya configurado como objetivo. (Unstoppable domains, 2022)

11. Evite el uso de la misma contraseña en dos sitios diferentes

Este tipo de prácticas permite a los cibercriminales acceder a potenciales filtraciones de datos de plataformas vulneradas, y al obtener la contraseña del sitio vulnerado tendrán también acceso a los otros sitios en los cuales el usuario decidió reutilizar la contraseña.

12. Evite el uso de SMS como factor de autenticación de dos pasos

Esto con el fin de evitar ataques de *Smishing* y *Vishing*, los cuales se basan en suplantar la identidad del usuario o de personal del operador de su smartphone, con el fin de acceder a los códigos de doble factor de autenticación que llegan a su dispositivo a través de la línea telefónica.

Por otro lado, este tipo de autenticación suele tener inconvenientes cuando se cambia de país o región y el operador de telefonía deja de tener cobertura sobre el área a la cual se ha trasladado.

13. Ponga una contraseña segura a la máquina en la cual administra los cripto activos

Esto con el fin de evitar que los cibercriminales que lleguen a tener acceso físico a su dispositivo puedan realizar ataques de fuerza bruta y/o probar combinaciones fáciles de adivinar.

14. Documente el proceso de implementación

Debido al nivel de complejidad técnica que puede implicar este tipo de implementación, es recomendable documentar los pasos realizados y las decisiones tomadas en el proceso, teniendo presente que dicha implementación se trata de la adopción de un sistema que posteriormente requerirá ser actualizado, mejorado y mantenido.

10. Phishing y tipos de estafas a identificar

Del mismo modo que en el mundo de la banca tradicional existen diversos tipos de estafas de las que se puede ser víctima, también en el ecosistema de los cripto activos existen diversos tipos de engaños y vectores de ataque que los ciber criminales pueden llegar a intentar, entre ellos se encuentran:

10.1. Influencers y personajes famosos ofreciendo beneficios

En 2020 se dio lugar a un ataque involucrando las cuentas verificadas de personajes reconocidos como Elon Musk, Barack Obama, Joe Biden y Warren Buffet.

En este ataque el ciber criminal publicó un mensaje diciendo que estaría dando a la comunidad el doble de cripto activos que depositaran a una dirección de bitcoin determinada.

Aunque el atacante fue posteriormente arrestado, los reportes concluyen que logró estafar más de 100.000 dólares en bitcoin. (DanMangan, 2021)

Por otro lado, en la actualidad muchos atacantes clonan de manera precisa los perfiles de las redes sociales de personajes reconocidos en la industria, y utilizan dichos perfiles que suplantan a los personajes reales para contactar por mensaje privado a potenciales víctimas. Estos atacantes suelen ofrecer grandes oportunidades de rentabilidad asegurada a cambio de una pequeña inversión. (Kozhipatt, 2022).

Adicionalmente, con la llegada de la inteligencia artificial la capacidad de crear videos y notas de voz a través de *Deepfakes* es cada vez más factible para los cibercriminales, realizando así suplantaciones de identidad cada vez más realistas. (Hurst, 2022).

Se recomienda hacer caso omiso a todo tipo de consejos y sugerencias de inversión de cualquier tipo de personalidad que se contacte directa o indirectamente, a través de redes sociales.

10.2. Billeteras con fondos listos para ser retirados

Un tipo de estafa más compleja de identificar es aquella en la que un atacante envía por cualquier medio (correo electrónico, redes sociales, etc.) una billetera con fondos junto a la frase semilla o clave privada, lo cual permitiría al usuario retirar los fondos a su billetera propia.

El atacante suele usar cualquier tipo de pretexto para compartir esta información, el más popular es argumentar que es una persona con pocos conocimientos de cripto activos y que requiere ayuda técnica.

Esto genera que la víctima, dejándose llevar por la “oportunidad” de obtener dinero rápido, intente extraer los fondos de la billetera ofrecida por el atacante. Sin embargo, estas billeteras suelen tener los fondos en un token (como monedas estables) pero no cuentan con el token nativo de la red para pagar por la comisión de la transacción en la *blockchain*.

Es ahí cuando la víctima decide depositar fondos a la billetera cedida para poder pagar la comisión de transacción y posteriormente retirar los cripto activos con los que cuenta la billetera.

Sin embargo, el atacante tiene programado un robot que automáticamente extrae los fondos depositados por parte de la víctima, haciéndole perder su dinero en cuestión de milisegundos. (Hetler, 2022).

Se recomienda ignorar cualquier mensaje o comunicado que le haga entrega de billeteras con frases semillas o llaves privadas, aunque no lo parezca es una trampa en la que muchos usuarios suelen caer.

11. En caso de ser hackeado

11.1. Los activos son gestionados por un custodio o plataforma de intercambio

1. En este caso es recomendable contactar el soporte técnico de la plataforma de intercambio a través de los medios oficiales destinados para tal propósito. Debido a que es un tercero el que gestiona los activos, es posible que se pueda reversar la transacción o solicitar algún tipo de seguro ante ataques sobre los cuales se tenga evidencia de que no fueron causados intencionalmente.
2. En ningún caso se recomienda contactar de manera pública al personal de soporte técnico o servicio al cliente a través de redes sociales. La razón de esto es que existen numerosos robots que responden de manera automatizada cualquier mensaje, comentario o publicación que contenga palabras claves relacionadas con cripto activos. Estos robots buscan contactar potenciales víctimas con problemas con sus activos y se aprovechan de su desesperación para prometer la "recuperación de los activos", no sin antes pagar una "comisión" para poder dar solución al problema.
3. Adicionalmente, es necesario seguir las recomendaciones de los puntos 2,4,5 y 6 del numeral 11.2, las cuales se describen a continuación.

11.2. Los activos son gestionados por la organización directamente

1. Si los activos no son gestionados por un tercero custodio o plataforma de intercambio, entonces la probabilidad de reversar la transacción es cercana a cero. Por otro lado, no existe soporte técnico al que se pueda contactar. Al ser gestionados por la organización las tecnologías utilizadas son equivalentes a usar software de fuentes abiertas, el cual no cuenta con ningún tipo de servicio al cliente.

2. Sin embargo, se recomienda utilizar la funcionalidad de *blockchain* explorer para realizar trazabilidad de los activos una vez hayan sido expropiados, tan solo es necesario ingresar la dirección sobre la cual se quiere hacer el análisis, y la propiedad de acceso público de la *blockchain* permitirá identificar toda la información relacionada.

La funcionalidad varía con base en la red o *blockchain* en la que se hayan robado los fondos, por ejemplo, la siguiente lista hace referencia a los exploradores más populares en la actualidad:

- Bitcoin https://www.blockchain.com/explorer
- Ethereum https://etherscan.io/
- Polygon https://polygonscan.com/
- Solana https://solscan.io/

3. En caso de que se sospeche que la billetera pudo haber sido comprometida o vulnerada, se recomienda mover los activos a una billetera completamente nueva en un dispositivo diferente al usualmente utilizado, siguiendo todas las normas anteriormente mencionadas para garantizar una implementación segura.
4. Por otro lado, se recomienda registrar pantallazos de toda la información relacionada con el incidente junto con la fecha y hora de registro. Esto con el fin de utilizarlo como evidencia en caso de poder realizar una investigación a profundidad posteriormente o llevar el caso ante autoridades competentes.
5. Adicionalmente, una vez superado el incidente, se recomienda informar a la comunidad relacionada de manera interna y privada para evitar inconvenientes reputacionales, y evitar atraer la atención de otros cibercriminales interesados en sacar provecho de personal desesperado por recuperar los activos.
6. Finalmente, realizar el reporte ante las autoridades competentes puede ser una medida apropiada para tener registro legal del incidente que permita obtener de vuelta los activos, o en el peor de los casos, tener un justificante válido de pérdida de activos al momento de realizar la tributación correspondiente a las actividades del año.

12. Lista de verificación de auditoría de seguridad

La siguiente lista de verificación, se crea con el fin de realizar una auditoría a la implementación realizada. Esto con el fin de contar con un resumen conciso que destaque los puntos a tener presentes en la larga lista de controles y medidas necesarias, para garantizar una implementación segura de tesorería de criptomonedas en las organizaciones.

12.1. Auditoría general

Esta auditoría es independiente a cualquier tipo de implementación realizada, contiene la lista de validación general que cualquier empresa que cuente con tesorería de criptomonedas debería cumplir para garantizar la seguridad de su cripto activos.

Tabla 6 *Auditoría general*

Control	Si	No	Comentarios
Cuenta con al menos 2 mecanismos diferentes de custodia para diversificar riesgos			
Cuenta con acuerdos de confidencialidad firmados por el personal relacionado con la implementación			
El acceso a los portales y sitios web relacionados con los cripto activos es realizado a través de los favoritos del navegador			
El computador utilizado para administrar los activos no cuenta			

con programas/software que no usa hace más de 90 días			
El computador utilizado para administrar los activos no suele ser usado para navegar por la web de manera ordinaria			
El computador utilizado para administrar los activos no cuenta con plug-ins, add-ons, o extensiones desarrolladas por terceros no oficiales			
El computador utilizado para administrar los activos no cuenta con programas crackeados o software pirateado			
El computador utilizado para administrar los activos cuenta con bloqueador de pantalla, el cual se activa 20 minutos o menos después de inactividad			
Antes de recibir fondos de terceros, se valida que su dirección no haga parte de una lista negra de direcciones			
Las contraseñas utilizadas para la administración de los activos nunca han sido utilizadas en ningún otro sitio web o plataforma			

Todas las contraseñas utilizadas son gestionadas por un administrador de contraseñas			
La contraseña maestra del administrador de contraseñas es una frase larga, compleja y fácil de recordar			

(Fuente: Elaborado por el autor)

12.2. Auditoría con base en Metamask

Tabla 7 *Auditoría con base en Metamask*

Control	Si	No	Comentarios
El computador utilizado para administrar los activos nunca ha sido usado para descargar archivos potencialmente peligrosos, y si lo ha sido, se ha formateado previo a la implementación de cripto activos.			
El sistema operativo se encuentra actualizado a la versión más reciente			
El antivirus se encuentra activo y actualizado a la versión más reciente			

Las navegaciones por internet nunca son realizadas a través de redes WiFi públicas			
El computador utilizado para administrar los activos hace uso de un DNS seguro			
Cada vez que se realizan transacciones por internet, estas hacen uso de una VPN			
Las conexiones a internet se dan exclusivamente a través de cable LAN			

(Fuente: Elaborado por el autor)

12.3. Auditoría con base en Qredo

Tabla 8 *Auditoría con base en Qredo*

Control	Si	No	Comentarios
El computador utilizado para administrar los activos nunca ha sido usado para descargar archivos potencialmente peligrosos, y si lo ha sido, se ha formateado previo a la implementación de cripto activos.			

El sistema operativo se encuentra actualizado a la versión más reciente			
El antivirus se encuentra activo y actualizado a la versión más reciente			
Las navegaciones por internet nunca son realizadas a través de redes WiFi públicas			
El computador utilizado para administrar los activos hace uso de un DNS seguro			
Cada vez que se realizan transacciones por internet, estas hacen uso de una VPN			
Las conexiones a internet se dan exclusivamente a través de cable LAN			
Los smartphones utilizados no han pasado por un proceso de *rooting* o *jailbreaking*			
Ninguno de los correos electrónicos a utilizar se ha visto comprometido en un incidente de filtración de datos			
Se configuró una política de aprobación de transacciones sobre			

los cripto activos que requiere al menos 2 firmas			
Se configuró una política de aprobación de retiros sobre los cripto activos que requiere al menos 2 firmas			

(Fuente: Elaborado por el autor)

12.4. Auditoría con base en Ledger

Tabla *9 Auditoría con base en Ledger*

Control	Si	No	Comentarios
El dispositivo fue comprado directamente del sitio oficial o por parte de un proveedor confiable autorizado			
La caja en la cual llegó el dispositivo no se encontraba dañada ni abierta y el contenido de la misma estaba en su lugar			
La hoja de recuperación se encuentra vacía			
La aplicación de Ledger utilizada para administrar los cripto activos fue descargada a través del sitio web oficial de la organización			

El computador utilizado para administrar los activos nunca ha sido usado para descargar archivos potencialmente peligrosos, y si lo ha sido, se ha formateado previo a la implementación de cripto activos.			
El sistema operativo se encuentra actualizado a la versión más reciente			
El antivirus se encuentra activo y actualizado a la versión más reciente			
Las navegaciones por internet nunca son realizadas a través de redes WiFi públicas			
El computador utilizado para administrar los activos hace uso de un DNS seguro			
Cada vez que se realizan transacciones por internet, estas hacen uso de una VPN			
Las conexiones a internet se dan exclusivamente a través de cable LAN			

El dispositivo a utilizar es genuino fue validado con la funcionalidad "Check my nano"			
El PIN de seguridad implementado para desbloquear el dispositivo no está escrito sobre ningún papel ni ha sido digitalizado			
La frase de recuperación se ha almacenado de manera segura, fuera de línea y fuera del alcance de cualquiera			

(Fuente: Elaborado por el autor)

12.5. Auditoría con base en plataforma de intercambio

Tabla *10 Auditoría con base en plataforma de intercambio*

Control	Si	No	Comentarios
La plataforma de intercambios no es utilizada para almacenar grandes cantidades de cripto activos, ni para almacenarlos a largo plazo			
El correo electrónico con el que se asoció la cuenta de la plataforma de intercambios nunca se ha visto comprometido en un incidente de filtración de datos			

La cuenta de la plataforma de intercambios tiene activado al menos un mecanismo de seguridad adicional			
En ningún momento se envía información personal o corporativa al realizar compras P2P			
El computador utilizado para administrar los activos nunca ha sido usado para descargar archivos potencialmente peligrosos, y si lo ha sido, se ha formateado previo a la implementación de cripto activos.			
El sistema operativo se encuentra actualizado a la versión más reciente			
El antivirus se encuentra activo y actualizado a la versión más reciente			
Las navegaciones por internet nunca son realizadas a través de redes WiFi públicas			
El computador utilizado para administrar los activos hace uso de un DNS seguro			

Cada vez que se realizan transacciones por internet, estas hacen uso de una VPN			
Las conexiones a internet se dan exclusivamente a través de cable LAN			
El contacto con el servicio al cliente o soporte técnico es realizado exclusivamente a través del portal oficial de la plataforma de intercambio			

(Fuente: Elaborado por el autor)

13. Evaluación y resultados con base en la auditoría sobre Aidel Corp

Para finalizar, con base en los controles de las auditorías creados, se realiza una auditoría para evaluar el resultado de implementación por parte de Aidel Corp.

Auditoría General

Tabla 11 *Auditoría general Aidel Corp*

Control	Si	No	Comentarios
Cuenta con al menos 2 mecanismos diferentes de custodia para diversificar riesgos	X		Los mecanismos de custodia implementados son Metamask y Qredo
Cuenta con acuerdos de confidencialidad firmados por el		X	En este caso, debido a la naturaleza de la implementación enfocada a

personal relacionado con la implementación			convertirse en un servicio ofrecido por la organización, no se considera adecuado crear un acuerdo de confidencialidad al respecto.
El acceso a los portales y sitios web relacionados con los cripto activos es realizado a través de los favoritos del navegador	X		Los sitios relacionados se han guardado en una carpeta dedicada en los favoritos del navegador.
El computador utilizado para administrar los activos no cuenta con programas/software que no usa hace más de 90 días	X		Se han eliminado los programas que no se han usado hace más de 90 días.
El computador utilizado para administrar los activos no suele ser usado para navegar por la web de manera ordinaria		X	El computador también se utiliza para realizar actividades relacionadas con las operaciones de la organización
El computador utilizado para administrar los activos no cuenta con plug-ins, add-ons, o extensiones desarrolladas por terceros no oficiales	X		No existe este tipo de software instalado que haya sido creado por terceros
El computador utilizado para administrar los activos no cuenta con programas crackeados o software pirateado	X		El dispositivo no cuenta con este tipo de software
El computador utilizado para administrar los activos cuenta con bloqueador de pantalla, el cual se	X		Se ha activado esta funcionalidad sobre el computador

activa 20 minutos o menos después de inactividad			
Antes de recibir fondos de terceros, se valida que su dirección no haga parte de una lista negra de direcciones	X		Aún no se han recibido fondos de terceros, pero se tiene presente dicha validación cuando suceda
Las contraseñas utilizadas para la administración de los activos nunca han sido utilizadas en ningún otro sitio web o plataforma	X		Las contraseñas son creadas de manera automatizada y aleatoria por un administrador de contraseñas
Todas las contraseñas utilizadas son gestionadas por un administrador de contraseñas	X		Se utiliza un administrador de manera general para este propósito
La contraseña maestra del administrador de contraseñas es una frase larga, compleja y fácil de recordar	X		La contraseña fue creada con estos principios en mente

(Fuente: Elaborado por el autor)

Auditoría Metamask

Tabla 12 *Auditoría MetaMask sobre Aidel Corp*

Control	Si	No	Comentarios
El computador utilizado para administrar los activos nunca ha sido usado para descargar archivos	X		Uno de los computadores utilizados para hacer este tipo de actividades, pero actualmente se encuentra limpio

potencialmente peligrosos, y si lo ha sido, se ha formateado previo a la implementación de cripto activos.			
El sistema operativo se encuentra actualizado a la versión más reciente	X		Actualizado a la versión más reciente
El antivirus se encuentra activo y actualizado a la versión más reciente	X		Antivirus activo y actualizado
Las navegaciones por internet nunca son realizadas a través de redes WiFi públicas	X		Nunca se hace uso de redes WiFi públicas
El computador utilizado para administrar los activos hace uso de un DNS seguro	X		Se ha configurado un DNS seguro para navegar de manera segura
Cada vez que se realizan transacciones por internet, estas hacen uso de una VPN		X	Debido al monto de las transacciones aún no se ha considerado el uso de una VPN
Las conexiones a internet se dan exclusivamente a través de cable LAN	X		Las conexiones relacionadas con la administración de cripto activos se dan a través de cable LAN

(Fuente: Elaborado por el autor)

Auditoría Qredo

Tabla 13 *Auditoría Qredo sobre Aidel Corp*

Control	Si	No	Comentarios
El computador utilizado para administrar los activos nunca ha sido usado para descargar archivos potencialmente peligrosos, y si lo ha sido, se ha formateado previo a la implementación de cripto activos.	X		Uno de los computadores fue utilizado para hacer este tipo de actividades, pero actualmente se encuentra limpio
El sistema operativo se encuentra actualizado a la versión más reciente	X		Actualizado a la versión más reciente
El antivirus se encuentra activo y actualizado a la versión más reciente	X		Antivirus activo y actualizado
Las navegaciones por internet nunca son realizadas a través de redes WiFi públicas	X		Nunca se hace uso de redes WiFi públicas
El computador utilizado para administrar los activos hace uso de un DNS seguro	X		Se ha configurado un DNS seguro para navegar de manera segura
Cada vez que se realizan transacciones por internet, estas hacen uso de una VPN		X	Debido al monto de las transacciones aún no se ha considerado el uso de una VPN

Las conexiones a internet se dan exclusivamente a través de cable LAN	X		Las conexiones relacionadas con la administración de cripto activos se dan a través de cable LAN
Los smartphones utilizados no han pasado por un proceso de *rooting* o *jailbreaking*	X		Ninguno de los smartphones utilizados ha pasado por este tipo de procesos
Ninguno de los correos electrónicos a utilizar se ha visto comprometido en un incidente de filtración de datos	X		Ninguno
Se configuró una política de aprobación de transacciones sobre los cripto activos que requiere al menos 2 firmas	X		Se requiere aprobación de al menos 2 firmas para poder realizar una transacción
Se configuró una política de aprobación de retiros sobre los cripto activos que requiere al menos 2 firmas	X		Se requiere aprobación de al menos 2 firmas para poder realizar un retiro

(Fuente: Elaborado por el autor)

14. CONCLUSIONES DE LA PRUEBA PILOTO

La prueba piloto realizada se considera un éxito. Dentro de la prueba se realizó la implementación de dos métodos de custodia y al finalizar se realizó la auditoría de la seguridad de dichas implementaciones. El detalle de las auditorías fue el siguiente:

Auditoría general

- Cumplimiento del 83.33%
- 10/12 controles se satisfacen exitosamente
- Oportunidades de mejora:
    - Se identifica como oportunidad de mejora la necesidad de una vez se empiecen a administrar grandes cantidades de cripto activos, dedicar un computador, servidor o máquina virtual exclusivamente para tal propósito, con el fin de mitigar cualquier potencial amenaza que se pueda presentar

Auditoría implementación Metamask

- Cumplimiento del 85%
- 6/7 controles se satisfacen exitosamente
- Oportunidades de mejora:
    - Se identifica como oportunidad de mejora el uso continuo de una VPN para mejorar la seguridad de las transacciones. Este control no se ha implementado debido a que aún no se manejan cripto activos de gran valor y porque la regulación del territorio no persigue de manera judicial el uso de tal tipo de activos.

Auditoría implementación Qredo

- Cumplimiento del 90%
- 10/11 controles se satisfacen exitosamente
- Oportunidades de mejora:
    - Al igual que en el caso de la implementación de Metamask, la oportunidad de mejora identificada está relacionada con el uso de VPN, la cual se implementará cuando se dé una condición necesaria.

En total se identificaron 30 controles que buscan garantizar la implementación de tesorería de criptomonedas en las organizaciones, de esta cantidad se evidenció que se dio satisfacción a 26 de ellos. Logrando así un cumplimiento del 86% del total de los controles definidos.

Esta lista de controles será continuamente actualizada, de modo que se convierta en un estándar que permita a la organización contar con una tesorería de cripto activos digitalmente segura.

15. Conclusiones y futuras líneas de desarrollo

15.1. Conclusiones

El objetivo general de este trabajo se considera cumplido satisfactoriamente, ya que ofrece la metodología para la implementación segura de tesorería de criptomonedas en las organizaciones. Guiando a cualquier organización que decida enfrentarse a este reto, hacia el método de implementación que mejor se ajuste a sus objetivos empresariales, necesidades y recursos.

Por otro lado, existen conclusiones detalladas sobre cada uno de los objetivos:

- Estudiar las tecnologías que pueden hacer posible la custodia segura de cripto activos en las organizaciones: Este objetivo se cumplió en el apartado 2.3. Tecnologías base, en el cual se detallaron las diversas tecnologías existentes relacionadas.
- Analizar los métodos que pueden hacer posible la custodia segura de cripto activos en las organizaciones: Este objetivo fue cumplido en el apartado 2.4. Investigaciones relacionadas, en donde se detalla históricamente cuales han sido los métodos más comunes y seguros de implementación.
- Facilitar el proceso de identificación de la categoría a la que una organización pertenece, respecto a sus capacidades y requerimientos de implementación: Este objetivo fue cumplido en el apartado 4.1. Identificación del contexto de la organización y 4.2. Identificación del método de implementación más adecuado. Allí se detalla los factores que las organizaciones deben tener presente para elegir sus métodos de implementación.
- Diseñar una serie de pasos y uso de tecnologías, que permitan a las organizaciones contar con custodia segura de cripto activos con base en sus necesidades y capacidades: Este objetivo fue cumplido satisfactoriamente en los apartados 5, 6, 7 y 8. Los cuales detallan las medidas y controles antes, durante y después de la implementación.
- Ejecutar una prueba piloto de la implementación sobre una organización real: Este objetivo fue cumplido al implementar dos de los principales métodos en la organización Aidel Corp SAS, Bogotá, Colombia. De la cual el autor es socio cofundador.

- Evaluar el nivel de la ciberseguridad de la implementación a través de una auditoría de controles y medidas ejecutadas: Este objetivo fue satisfecho al desarrollar una lista de controles para auditoría en el apartado 12. Lista de verificación de auditoría de seguridad y validarla sobre la organización de la prueba piloto en la sección 13. Evaluación y resultaos con base en la auditoría sobre Aidel Corp.

Finalmente, se concluye que este trabajo excedió los objetivos propuestos, al añadir los apartados 10. Phishing y tipos de estafas a identificar y 11. En caso de ser hackeado, de modo que las empresas puedan tomar acción efectiva, ya sea proactiva o reactiva sobre la seguridad de su tesorería de cripto activos.

15.2. Futuras líneas de desarrollo y trabajos futuros

Se identifica la potencial necesidad a futuro de definir controles y medidas de seguridad alrededor del proceso de transferencia de cripto activos, ya que se plantea que en el futuro estos serán ampliamente usados como medio de transferencia de valor del mismo modo que actualmente se usan monedas locales para tal propósito.

Por otro lado, se considera apropiado mantener una lista actualizada de potenciales estafas y vectores de ataque implementados por los cibercriminales, esto con el fin evitar caer en ellos y que se reconoce que en la mayoría de las veces son las personas el eslabón más débil en la cadena de ciberseguridad en las organizaciones.

Finalmente, para complementar dicho trabajo y estar al tanto con las medias de cripto ciberseguridad y seguridad en Web3 más recientes, se puede consultar el sitio web del autor www.aidelcorp.com o escribir a su correo electrónico ceo@aidelcorp.com.

16. REFERENCIAS BIBLIOGRÁFICAS

Binance Academy. (2022a). Custodial vs. Non-Custodial Wallets: What's the difference? Binance Academy. Recuperado el 26 de octubre de 2022, de https://academy.binance.com/en/articles/custodial-vs-non-custodial-wallets-what-s-the-difference

Binance Academy. (2022b). What is a crypto wallet? Binance Academy. Recuperado el 25 de septiembre de 2022, de https://academy.binance.com/en/articles/crypto-wallet-types-explained

Binance. (2021). How to store bitcoin: A complete guide for beginners. Binance Blog. Recuperado el 23 de septiembre de 2022, de https://www.binance.com/en-IN/blog/ecosystem/how-to-store-bitcoin-a-complete-guide-for-beginners-421499824684901935

Binance. (2022). Where to safely keep Bitcoin? Blog Ng Binance. Binance Blog. Recuperado el 23 de septiembre de 2022, de https://www.binance.com/ph/blog/all/where-to-safely-keep-bicoin-421499824684901861

BitGo. (2022). Wallet platform. BitGo. Recuperado el 23 de octubre de 2022, de https://www.bitgo.com/services/custody/wallet-platform

Bitwarden. (2022). Install and sync all of your devices. Bitwarden: Administrador de contraseñas. Recuperado el 1 de noviembre de 2022, de https://bitwarden.com/download/

Butterfill, J. (2022). Digital Asset Bi-Monthly Fund Manager Survey. Recuperado el 14 de septiembre de 2022, de https://a.storyblok.com/f/155294/x/085c7c03d8/digital_asset_investor_survey_july_2022_.pdf

Chainalysis. (2022). Global crypto adoption up 880% in 2021. Chainalysis. Recuperado el 28 de septiembre de 2022, de https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/

Coinbase Help. (2022). Coinbase Help Center. How can I make my account more secure? Recuperado el 7 de noviembre de 2022, de https://help.coinbase.com/en/coinbase/privacy-and-security/data-privacy/how-can-i-make-my-account-more-secure

CoinGecko. (2022). Public companies with Bitcoin Holdings. CoinGecko. Recuperado el 17 de septiembre de 2022, de https://www.coingecko.com/en/public-companies-bitcoin

Cointelegraph. (2022). What is the bitcoin blockchain? A guide to the technology behind BTC. Cointelegraph. Recuperado el 23 de octubre de 2022, de

https://cointelegraph.com/bitcoin-for-beginners/how-does-blockchain-work-a-beginners-guide-to-blockchain-technology

DanMangan. (2021). Man busted in 2020 Twitter Hack, bitcoin scam of Biden, Obama, Musk, Buffett accounts. CNBC. Recuperado el 17 de noviembre de 2022, de https://www.cnbc.com/2021/07/21/man-busted-for-twitter-hack-of-biden-obama-musk-in-bitcoin-scam.html

de Orbe Catalán, M. (2019). IMPACTO DEL BLOCKCHAIN Y LAS CRIPTOMONEDAS EN LAS ENTIDADES FINANCIERAS. 2019; Madrid.

Gartner. (2021). Newsroom, announcements and media contacts. Gartner Survey Suggests Most Finance Executives Not Planning to Hold Bitcoin as a Corporate Asset. Recuperado el 30 de septiembre de 2022, de https://www.gartner.com/en/newsroom/press-releases/2020-02-16-gartner-survey-suggests-most-finance-executives-not-planning-to-hold-bitcoin-as-a-corporate-asset

GeeksforGeeks. (2022). Types of blockchain. Recuperado el 23 de octubre de 2022, de https://www.geeksforgeeks.org/types-of-blockchain/

Guardeño, D., Vico J., & Encinas L. (2019). What is Ethereum?. Amazon. Recuperado el 23 de octubre de 2022, de https://aws.amazon.com/blockchain/what-is-ethereum/

Hayes, A. (2022). Blockchain facts: What is it, how it works, and how it can be used. Investopedia. Recuperado el 23 de octubre de 2022, de https://www.investopedia.com/terms/b/blockchain.asp

Hayes, A. (2022). Blockchain facts: What is it, how it works, and how it can be used. Investopedia. Recuperado el 28 de septiembre de 2022, de https://www.investopedia.com/terms/b/blockchain.asp

Helena. (2020). Las DNS Cloudflare: 1.1.1.1 y todas sus variantes: Ayuda ley Datos. Ayuda Ley Protección Datos. Recuperado el 5 de noviembre de 2022, de https://ayudaleyprotecciondatos.es/dns/cloudflare/

HERMOSILLA , P. (2019). Criptomonedas y libertad de empresa. Recuperado el 27 de noviembre de 2022, de https://repositorio.uchile.cl/bitstream/handle/2250/168552/Criptomonedas-y-libertad-de-empresa.pdf?

Hetler, A. (2022). 9 common cryptocurrency scams in 2023. WhatIs.com. Recuperado el 19 de noviembre de 2022, de https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams

Huillet, M. (2018). Payments company square open-sources its Bitcoin Cold Storage Tool. Cointelegraph. Recuperado el 8 de septiembre de 2022, de

https://cointelegraph.com/news/payments-company-square-open-sources-its-bitcoin-cold-storage-tool

Hurst, L. (2022). Crypto scam: Binance Exec claims hackers used 'deepfake' of him. euronews. Recuperado el 18 de noviembre de 2022, de https://www.euronews.com/next/2022/08/24/binance-executive-says-scammers-created-deepfake-hologram-of-him-to-trick-crypto-developer

Kozhipatt, J. (2022). 5 social media crypto scams to avoid. CoinDesk Latest Headlines RSS. Recuperado el 20 de noviembre de 2022, de https://www.coindesk.com/learn/5-social-media-crypto-scams-to-avoid/

Kraken. (2021). What is Polygon? (MATIC). Recuperado el 23 de octubre de 2022, de https://www.kraken.com/learn/what-is-polygon-matic

Ledger Support. (2022). How to get started with Ledger. YouTube. Recuperado el 21 de noviembre de 2022, de https://www.youtube.com/watch?v=ZphG5NpNzB4&t=1s.

Marquit, M. (2022). Is Coinbase Vault Safe? [here's what you need to know]. FinanceBuzz. Recuperado el 23 de octubre de 2022, de https://financebuzz.com/is-coinbase-vault-safe

Matt Hussey, D. P. (2022). What is Metamask? how to use the top Ethereum Wallet. Decrypt. Recuperado el 29 de octubre de 2022, de https://decrypt.co/resources/metamask

Metamask. (2022). Metamask: Blockchain Wallet app and browser extension. Download MetaMask | Blockchain wallet app and browser extension. Recuperado el 1 de noviembre de 2022, de https://metamask.io/download/

Mg. (2021). Protecting yourself from $5 wrench attacks. CryptoSec. Recuperado el 14 de septiembre de 2022, de https://cryptosec.info/wrench-attack/

Ministerio de comercio, industria y turismo. (2019). ¿Por qué son importantes las MIPYME dentro de la agenda estatal? Guía de Contratación Pública para micro, Pequeñas y Medianas empresas - MIPYME-. Recuperado el 29 de septiembre de 2022, de http://www.aplicaciones-mcit.gov.co/guiapymes/c1i3.html#:~:text=Peque%C3%B1a%20Empresa%3A%20Personal%20entre%2011,entre%2051%20y%20200%20trabajadores

Moreland, K. (2022). Keep my crypto safe: 6 essential rules. Ledger. Recuperado el 21 de noviembre de 2022, de https://www.ledger.com/academy/how-to-make-sure-that-my-crypto-stays-safe-with-ledger

Moreland, K. (2022). Not your keys, not your coins. it's that simple. Ledger. Recuperado el 19 de septiembre de 2022, de https://www.ledger.com/academy/not-your-keys-not-your-

Natalie. (2020). Leading US-based crypto custodian providers for institutional clients. Medium. Recuperado el 4 de septiembre de 2022, de https://natalie-d.medium.com/leading-us-based-crypto-custodian-providers-for-institutional-clients-3ba9b8683c6d

Norge, S. (2022). Satoshi nakamoto's Bitcoin State of Mind. Bitcoin Magazine - Bitcoin News, Articles and Expert Insights. Recuperado el 18 de septiembre de 2022, de https://bitcoinmagazine.com/culture/satoshi-nakamotos-bitcoin-state-of-mind

Orenes-Lerma, L. (2022). Buy a ledger on Amazon: How to know it's safe. Ledger. Recuperado el 20 de noviembre de 2022, de https://www.ledger.com/academy/buying-a-ledger-from-a-third-party

Orji, C. (2022). The countries where Bitcoin and crypto are banned or restricted. euronews. Recuperado el 28 de septiembre de 2022, de https://www.euronews.com/next/2022/08/25/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2

Picardo, E. (2022). What is Solana (sol) and how does sol crypto work? Investopedia. Recuperado el 23 de octubre de 2022, de https://www.investopedia.com/solana-5210472

Qredo Team. (2022). What is Qredo built on? Qredo. Recuperado el 29 de octubre de 2022, de https://www.qredo.com/blog/what-is-qredo-built-on

Qredo. (2021). Crypto Treasury Management Solutions. Recuperado el 14 de septiembre de 2022, de https://www.qredo.com/blog/what-to-look-for-in-a-crypto-treasury-management-solution

RFC 4949 - internet security glossary, version 2. Document search and retrieval page. (2022). Recuperado el 15 de septiembre de 2022, de https://datatracker.ietf.org/doc/html/rfc4949

Rosenberg, E. (2022). What happens when a crypto exchange goes bankrupt? Investopedia. Recuperado el 28 de septiembre de 2022, de https://www.investopedia.com/crypto-bankruptcy-affecting-investors-6274367

Scorechain. (2021). What is BNB Smart Chain (BSC)?. Recuperado el 23 de octubre de 2022, de https://www.scorechain.com/resources/crypto-glossary/bnb-smart-chain-bsc

Sharma, R. (2022). What is a ledger wallet? Investopedia. Recuperado el 29 de octubre de 2022, de https://www.investopedia.com/terms/l/ledger-wallet.asp

Sophos. (2022). Sophos Home: Ciberseguridad sin complicaciones. Sophos Home | Ciberseguridad sin complicaciones. Recuperado el 1 de noviembre de 2022, de https://my.sophos.com/es-es/download/

Square, Inc. (2020). Bitcoin Investment Whitepaper. Recuperado el 13 de septiembre de 2022, de https://images.ctfassets.net/2d5q1td6cyxq/5sXNrlEh2mEnTvvhgtYOm2/737bcfdc15e2a1c3cbd9b9451710ce54/Square_Inc._Bitcoin_Investment_Whitepaper.pdf

Sun, Z. (2022). $5 wrench attacks appear to be on the rise in the Crypto Community. Cointelegraph. Recuperado el 7 de noviembre de 2022, de https://cointelegraph.com/news/5-wrench-attacks-appear-to-be-on-the-rise-in-the-crypto-community

Team, T. B. P. (2022). Custodial vs non-custodial wallet - what's the difference?: BitPay. The BitPay Blog. Recuperado el 8 de octubre de 2022, de https://bitpay.com/blog/non-custodial-wallets-vs-custodial-wallets/

Unstoppable domains. (2022). Domina tu identidad en el mundo digital. Domina tu identidad en el mundo digital. Recuperado el 10 de noviembre de 2022, de https://unstoppabledomains.com/es-es

Wikimedia Foundation. (2022). Cryptocurrency exchange. Wikipedia. Recuperado el 17 de septiembre de 2022, de https://en.wikipedia.org/wiki/Cryptocurrency_exchange

Wikiwand. (2022). Cryptocurrency wallet. Wikiwand. Recuperado el 21 de septiembre de 2022, de https://www.wikiwand.com/en/Cryptocurrency_wallet