

Libro 5: Topología de seguridad **y configuración de resiliencia del clearing**

Título	<u>Libro 5: Topología de seguridad y configuración de resiliencia del clearing</u>
Autor	Sr. Denis Bouzon
ORCID	0009-0007-8894-8902
Versión / fecha	2.1; 17 de octubre de 2026
Página de presentación	www.osnias-clearing.com/security
Licencia	© 2026 Denis Bouzon — All rights reserved
URL DOI	

Documentación previa de Osnias

<u>Libro 1</u>	Osnias ID	https://www.osnias-clearing.com/osniasid/
<u>Libro 2</u>	Arquitectura	https://www.osnias-clearing.com/architecture/
<u>Libro 3</u>	Reglas	https://www.osnias-clearing.com/rules/
<u>Libro 4</u>	Ciclos / Calendario	https://www.osnias-clearing.com/cycles/
<u>Libro 5</u>	Seguridad	https://www.osnias-clearing.com/security/
<u>Libro 6</u>	Incorporación	https://www.osnias-clearing.com/onboarding/
<u>Libro 7</u>	O-POP	https://www.osnias-clearing.com/pop/

Resumen

Este documento presenta la arquitectura de seguridad de los usuarios finales de Osnias Clearing a lo largo de todo el ciclo de vida de su identidad: incorporación, autorización en dos dominios independientes, liberación segura de fondos, renovación criptográfica y salida del sistema. También describe las funciones administrativas del gestor de nodo y del gestor Osnias, sus claves específicas y los controles de netting y de límites de fondos en garantía. Su objetivo es reducir el riesgo de que el compromiso de una única clave operativa ECDSA provoque el desvío de los fondos depositados en garantía.

La arquitectura utiliza las cadenas existentes sin modificarlas. Separa la dirección EVM de firma operativa, un dominio de autorización Sei independiente y una dirección EVM fría de recepción, generada a partir de una tercera semilla y registrada previamente en el contrato inteligente. Esta dirección no está destinada a firmar durante su fase de recepción: constituye un beneficiario predefinido, y no una clave de autorización operativa. Por tanto, el compromiso del firmante operativo no confiere, por sí solo, el control del destino de los fondos liberados.

El riesgo de un futuro ataque contra claves públicas ECDSA expuestas se trata como un riesgo criptográfico prospectivo, y no como una amenaza operativa actual demostrada. El enfoque responde a la seguridad a largo plazo: los mecanismos disponibles en las cadenas actuales reducen una categoría plausible de riesgos sin afirmar que ECDSA sea resistente a los ataques cuánticos. Estado del documento: evaluación técnica interna y preparación para la auditoría. Los controles se clasifican según las evidencias disponibles; este documento no constituye una auditoría independiente, una verificación formal, un informe de pruebas de penetración ni una certificación de seguridad en producción.

Palabras clave

Osnias-ID; incorporación; salida del sistema; ECDSA; secp256k1; depósito en garantía EVM; riesgo cuántico; dirección fría de recepción; autorización en dos dominios; defensa en profundidad; higiene criptográfica; ataque basado en el algoritmo de Shor.

Table des matières

1 Statut de l'évaluation et niveau documentaire.....	3
2 Périmètre, méthode et référentiels de l'évaluation.....	3
2.1 Référentiels méthodologiques.....	4
3 Matrice d'évaluation des contrôles.....	4
4 Objet, principes de sécurité et périmètre.....	5
4.1 Perspective de sécurité à long terme.....	5
4.2 Propriétés recherchées.....	5
4.3 Propriétés non revendiquées.....	6
5 Cycle de vie de la sécurité de l'utilisateur.....	6
6 Architecture de l'entrée sécurisée.....	6
6.1 Domaine A — Signataire EVM opérationnel.....	6
6.2 Domaine B — Autorisation Sei indépendante.....	6
6.3 Domaine C — Adresse froide de réception indépendante.....	6
6.4 Indépendance des graines et risque de cascade BIP-32.....	7
6.5 Condition composite de libération.....	8
6.6 Règle du bénéficiaire prédéfini.....	8
6.7 Ensemble minimal des données liées à l'autorisation.....	8
6.8 Autorisation à usage unique et protection contre le rejeu.....	8
6.9 Cycle de vie du portefeuille de réception.....	8
7 Modèle de menace à long terme : compromission d'une clé et risque lié à Shor.....	8
7.1 Scénario prospectif lié à Shor.....	8
7.2 Objectif de l'attaquant.....	9
7.3 Pourquoi la clé récupérée reste insuffisante.....	9
7.4 Surface d'attaque résiduelle.....	9
8 Osnias-ID, intégrité des registres et protection contre le rejeu.....	9
8.1 Cohérence des registres et risque TOCTOU.....	9
8.2 Séparation du plan de contrôle.....	9
9 WW=00 : mode de sécurité du séquestre autonome.....	9
10 Hygiène cryptographique, renouvellement de l'identité et sortie.....	10
10.1 Renouvellement complet.....	10
10.2 Sortie et révocation définitive.....	11
11 Exigences de renforcement institutionnel.....	11
12 Limites et travaux ouverts.....	12
13 Feuille de route de l'implémentation et de la validation de sécurité.....	12
14 Conclusion.....	13
15 Bibliographie.....	13

Estado de la evaluación y nivel documental

Este documento constituye una evaluación técnica interna y una preparación para la auditoría del sistema de seguridad previsto para los usuarios finales de Osnias Clearing. Examina la arquitectura, las fronteras de confianza, los objetivos de control, los riesgos abiertos y las evidencias necesarias para validar posteriormente la implementación. No constituye una auditoría independiente, una verificación formal, una prueba de penetración, una auditoría de custodia de activos, un dictamen jurídico, una certificación ni una autorización para operar en producción.

Elemento evaluado	Estado actual
Nivel documental	Evaluación técnica interna y preparación para la auditoría de seguridad
Base de la revisión	Arquitectura de seguridad de los usuarios finales de Osnias Clearing — Versión 4.3
Evaluador	Denis Bouzon / Osnias Clearing — evaluación interna
Evidencias de implementación	Pendientes para los controles identificados en el documento
Campaña adversarial en testnet	Pendiente
Auditoría independiente por terceros	No realizada
Certificación de seguridad en producción	No reivindicada
Estado general	Diseño evaluado; evidencias de implementación, pruebas adversariales y revisión independiente pendientes

Terminología relativa a las evidencias: REQUISITO DE DISEÑO — propiedad de seguridad buscada; ESPECIFICADO — semántica del control descrita; IMPLEMENTACIÓN PENDIENTE — evidencia a nivel de código no disponible; PRUEBAS PENDIENTES — evidencia de pruebas adversariales no disponible; ABIERTO — decisión importante de diseño o implementación sin resolver; REVISADO INDEPENDIENTEMENTE — reservado a los controles examinados posteriormente por un evaluador independiente identificado.

Alcance, método y marcos de referencia de la evaluación

Alcance. La revisión abarca el firmante EVM operativo, la autorización Sei independiente, el beneficiario frío registrado previamente, la condición compuesta de liberación, la protección contra la reutilización, la coherencia de Osnias-ID y de los registros, las hipótesis de verificación entre cadenas, la renovación y la baja de la identidad, las facultades administrativas, las claves específicas del gestor de nodo y del gestor Osnias, los ajustes de netting y los límites de garantía por nodo, la custodia de claves por los participantes y la validación prevista.

Exclusiones. La revisión no certifica el código desplegado, la infraestructura de producción, los proveedores de monederos, los sistemas de custodia de los participantes, la corrección del consenso de la cadena de origen, el cumplimiento jurídico o normativo ni la eficacia de controles que no se hayan implementado y documentado. Aunque el consenso de la cadena de origen queda fuera del alcance, la liberación entre

cadenas depende de una hipótesis expresamente documentada sobre la finalidad y la autenticación del estado de origen.

Método. Los controles se valoran mediante revisión de arquitectura y análisis de fronteras de confianza, escenarios de compromiso, invariantes, ciclo de vida, facultades administrativas y fallos entre cadenas. El análisis también identifica los riesgos residuales y las evidencias de implementación y pruebas adversariales necesarias antes de cualquier cualificación para producción.

Marcos metodológicos de referencia

- ISO 19011:2026 — Directrices para la auditoría de los sistemas de gestión: principios de auditoría, organización del programa y enfoque basado en evidencias y riesgos.
- ISO/IEC 27001:2022 — Sistemas de gestión de la seguridad de la información: gobernanza de riesgos y contexto de gestión de la seguridad.
- ISO/IEC 27002:2022 — Controles de seguridad de la información: recomendaciones, en particular sobre control de acceso y criptografía.
- ISO/IEC 27005:2022 — Gestión de los riesgos de seguridad de la información: identificación, evaluación y tratamiento estructurados.
- ISO/IEC 27034-1:2011 — Seguridad de las aplicaciones: integración de los principios y procesos de seguridad en el ciclo de vida de las aplicaciones.
- NIST SP 800-218, SSDF v1.1 — Marco de desarrollo de software seguro: prácticas de desarrollo, reducción de vulnerabilidades y producción de evidencias durante todo el ciclo de vida del software.

Aclaración sobre los marcos de referencia. Estas normas y marcos se citan únicamente como referencias metodológicas y de diseño. Su mención no implica certificación ISO, evaluación de conformidad, aprobación del NIST, validación independiente ni la afirmación de que Osnias Clearing haya sido auditado conforme a todos los requisitos citados.

Matriz de evaluación de controles

La matriz distingue los requisitos de diseño de las evidencias de implementación. La criticidad describe las posibles consecuencias de la ausencia o elusión de un control; no significa que ya se haya observado una vulnerabilidad en código desplegado. La columna «Acción requerida» indica los trabajos y evidencias necesarios para avanzar hacia la verificación.

ID	Control / hallazgo	Criticidad	Estado actual de las evidencias	Acción requerida
SEC-001	El firmante operativo no debe elegir ni sustituir libremente al beneficiario de la liberación.	Crítica	REQUISITO DE DISEÑO	Implementar y probar la inmutabilidad o modificación controlada del beneficiario en el contrato; verificar el rechazo de destinos arbitrarios.
SEC-002	La autorización de liberación debe ser de un solo uso y vincularse al nonce, a la prueba y al beneficiario predefinido.	Alta	ESPECIFICADO	Consumir nonces y pruebas; probar reutilizaciones y sustituciones de contrato, cadena, importe o beneficiario.
SEC-003	La autenticación del estado Sei canónico, la finalidad y las reorganizaciones, el quórum y la rotación del verificador exigen evidencias de implementación.	Alta	ABIERTO	Definir estos mecanismos; probar fallos y estados obsoletos.

SEC-004	Ninguna autoridad única de actualización, registro, verificación o emergencia debe eludir la condición compuesta ni modificar por sí sola al beneficiario.	Crítica	REQUISITO DE DISEÑO	Definir la separación de funciones y los controles por umbral; probar abusos de las vías administrativas y de emergencia.
SEC-005	Las semillas A, B y C exigen raíces independientes y aislamiento de fallos comunes; las claves permanecen bajo la custodia del participante.	Alta	ESPECIFICADO / IMPLEMENTACIÓN PENDIENTE	Documentar la generación y custodia; demostrar la independencia de las raíces y probar configuraciones incorrectas durante la incorporación.
SEC-006	La migración de identidad y la vinculación con su sucesor exigen una máquina de estados y pruebas adversariales.	Alta	IMPLEMENTACIÓN PENDIENTE	Implementar estados, vinculaciones, condiciones de migración y revocación definitiva; probar ataques de migración.
SEC-007	El análisis estático, los escenarios de ataque en testnet, las correcciones y las nuevas pruebas siguen siendo necesarios antes de la revisión independiente.	Alta	PRUEBAS PENDIENTES	Ejecutar Slither y la campaña adversarial; corregir, repetir las pruebas y publicar el informe de validación.
SEC-008	La clave específica del gestor de nodo solo debe actuar en su nodo, dentro de la ventana autorizada y conforme a las posiciones netas definitivas.	Crítica	REQUISITO DE DISEÑO / IMPLEMENTACIÓN PENDIENTE	Probar operaciones fuera del nodo o de la ventana, importes injustificados, destinos no registrados y ejecuciones duplicadas; verificar el tratamiento de saldos deudores y acreedores.
SEC-009	La clave del gestor Osnias administra los números y parámetros de los nodos sin disponer de sus activos; los contratos deben aplicar los límites de garantía.	Alta	REQUISITO DE DISEÑO / IMPLEMENTACIÓN PENDIENTE	Especificar unidades y ámbito de los límites, su modificación y reducción; probar excesos y abusos de derechos administrativos.
SEC-010	Las semillas de los gestores deben ser independientes entre sí y de los dominios A, B y C; la rotación y revocación deben preservar las restricciones de cada función.	Alta	REQUISITO DE DISEÑO / PRUEBAS PENDIENTES	Documentar generación, custodia y recuperación; probar asignación, revocación, rotación y compromiso de cada clave de gestión.
SEC-011	El participante solo puede ajustar su depósito en garantía durante los días 2 a 4; toda retirada debe dirigirse a su dirección específica registrada; el depósito se bloquea al cierre del jueves.	Crítica	REQUISITO DE DISEÑO / IMPLEMENTACIÓN Y PRUEBAS PENDIENTES	Precisar el límite de cierre UTC; probar aportaciones y retiradas en los límites de la ventana, importes no liberables, sustitución de destino, superación del límite y mantenimiento de las operaciones de liquidación autorizadas.

Interpretación de la criticidad: Crítica — la ausencia del control podría permitir el desvío directo de fondos o eliminar la separación de autorizaciones; Alta — debilidad importante de un control o una frontera de

confianza; Media — debilidad que debe corregirse antes de producción; Baja — recomendación de refuerzo; Informativa — observación sin efecto directo demostrado sobre la seguridad.

Invariante administrativo buscado. Ninguna autoridad única encargada de actualizaciones, registros, verificadores o medidas de emergencia debe poder modificar por sí sola la condición de liberación, cambiar el beneficiario registrado o desactivar la autorización independiente del segundo dominio. Los umbrales, plazos de seguridad y reglas de separación de funciones siguen pendientes de implementación y documentación antes de cualquier verificación independiente.

Objeto, principios de seguridad y alcance

Osnias Clearing aborda la seguridad de los fondos de los usuarios como una propiedad del ciclo de vida, y no como un simple problema de firma. El protocolo separa la firma operativa, la autorización independiente, el destino de los fondos, el estado del registro y los controles del ciclo de vida de la identidad. Esta arquitectura se ha diseñado para las infraestructuras EVM y Sei actuales, reduciendo a la vez las consecuencias de un posible compromiso futuro de claves clásicas expuestas.

Principio de diseño: reducir los riesgos futuros con las cadenas disponibles hoy.

Perspectiva de seguridad a largo plazo

El algoritmo de Shor establece una vía teórica para resolver el problema del logaritmo discreto en curvas elípticas con un ordenador cuántico suficientemente potente. Este documento no afirma que esa capacidad exista actualmente contra cuentas secp256k1 en condiciones operativas. Por tanto, el escenario cuántico es prospectivo. La pregunta técnica es más concreta: si un atacante recupera mañana una clave de firma operativa expuesta, ¿debe esa única clave permitirle desviar fondos depositados en garantía?

La respuesta de Osnias se basa en la arquitectura. Sin modificar ECDSA, modifica las condiciones de liberación de fondos y su destino autorizado. Este enfoque constituye una defensa en profundidad, sin pretender una seguridad poscuántica completa.

Propiedades buscadas

- El compromiso de la clave de firma EVM operativa no debería, por sí solo, satisfacer todas las condiciones de liberación.
- Un segundo dominio de autorización, generado de forma independiente en Sei, puede añadir una condición criptográfica independiente.
- Una dirección EVM fría de recepción predefinida puede separar la facultad de firmar de la facultad de determinar el destino de los fondos.
- **La arquitectura puede implementarse con contratos EVM existentes, direcciones EOA, estado de registros, nonces y un estado autenticado entre cadenas.**

Propiedades no reivindicadas

- No se reivindica resistencia cuántica completa, demostración formal ni nivel cuantificado de seguridad poscuántica.
- La dirección fría de recepción no convierte ECDSA en poscuántico; reduce la utilidad del compromiso del firmante operativo para desviar fondos.
- **El verificador, la gobernanza de los registros, el consenso de la cadena de origen y la facultad de actualización siguen siendo fronteras de confianza explícitas.**

Ciclo de vida de la seguridad del usuario

El ciclo de vida comprende la incorporación, la operación activa, la liberación segura de fondos, la renovación opcional de la identidad y la salida del sistema. Osnias proporciona los mecanismos y transiciones de estado; el participante mantiene el control de su política de seguridad, incluida la decisión de renovar su identidad criptográfica y el momento de hacerlo.

- Durante la incorporación, se establece Osnias-ID y se vincula al firmante EVM operativo, al dominio Sei independiente y a la dirección fría de recepción.
- Durante la operación, el firmante operativo realiza las interacciones EVM habituales; el segundo dominio y el verificador limitan la facultad de liberación.
- Los fondos liberados se envían únicamente al beneficiario registrado previamente, nunca a un destino arbitrario indicado en el momento de la liberación.
- La renovación y la salida crean, si se desea, una nueva identidad, migran o liquidan las posiciones restantes y revocan después de forma irreversible la identidad anterior.

Arquitectura de incorporación segura

La incorporación crea la identidad de seguridad del protocolo. Osnias-ID vincula sus elementos; no constituye en sí mismo una clave criptográfica. La seguridad depende de la separación de las funciones técnicas asociadas a ese identificador.

Dominio A — Firmante EVM operativo

El dominio A comprende la clave y la dirección EVM de firma operativa del participante. Perfil recomendado: generar y conservar esta clave en un monedero físico que permita las firmas EVM habituales sin exponer la clave privada al ordenador de uso general. Esta clave operativa, potencialmente expuesta por la actividad habitual de firma, no debe poder determinar por sí sola el destino final de los fondos liberados del depósito en garantía.

Dominio B — Autorización Sei independiente

El dominio B procede de una semilla independiente y participa en el proceso canónico de autorización o transición de estado en Sei. El participante puede utilizar un monedero operativo compatible con Sei, como MetaMask si el entorno elegido lo permite. No debe compartirse ninguna semilla, raíz de derivación ni dato de recuperación entre los dominios A y B. La separación de redes no basta si se comparte la semilla subyacente.

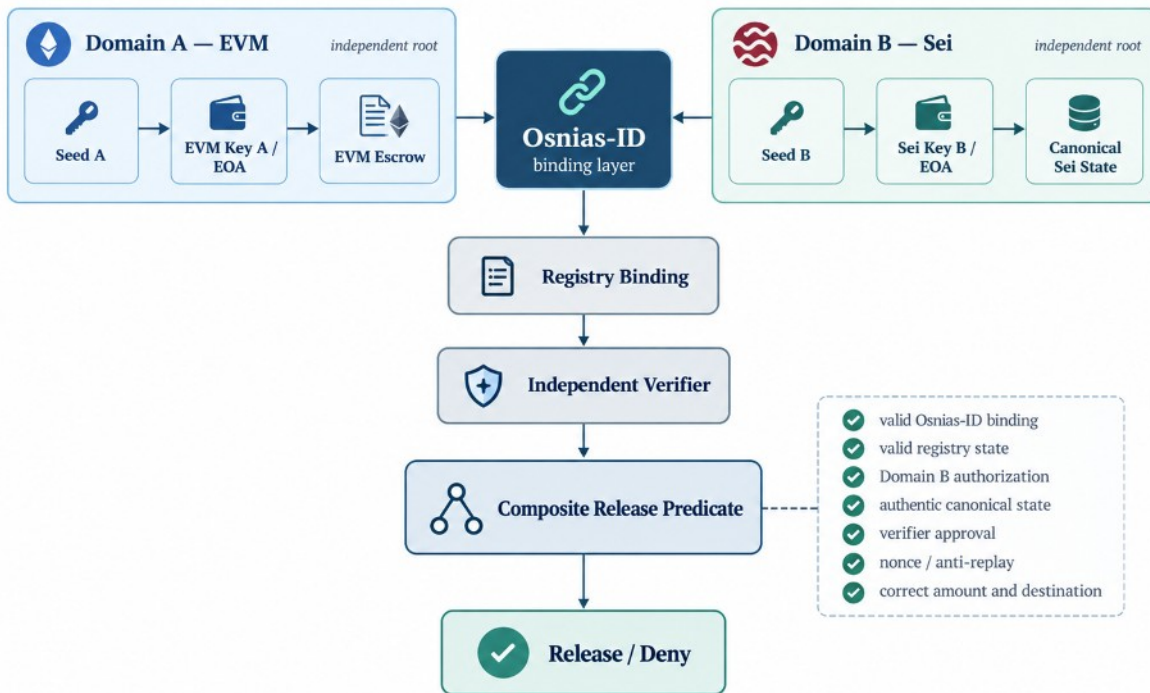
Dominio C — Dirección fría de recepción independiente

Durante la incorporación también se registra un beneficiario EVM específico a partir de una tercera semilla independiente. Perfil recomendado: la semilla C permanece fuera de línea en un monedero frío, normalmente sin utilizar para firmar operaciones habituales. Su dirección se registra como beneficiario de la liberación. Durante la fase prevista para recibir fondos, esta dirección no necesita firmar; por tanto, la mera recepción no revela su clave pública mediante una firma ECDSA saliente.

El beneficiario se fija antes de la liberación. El firmante operativo no debe poder sustituirlo por un destino arbitrario en ese momento. Cualquier modificación debería someterse a un procedimiento separado de renovación o nueva incorporación, con controles adecuados, en lugar de depender de una decisión unilateral del firmante.

Osnias Dual-Domain Authorization Architecture

One Osnias-ID · Two Independent Authorization Domains · One Composite Release Predicate



Security objective: compromise of one ECDSA key alone should remain insufficient for escrow release.

Figura 1 — Arquitectura de autorización en dos dominios

Independencia de las semillas y riesgo de cascada BIP-32

Las semillas A, B y C deben generarse de forma independiente: una raíz común comprometería la separación buscada. Varias direcciones derivadas de una misma semilla no constituyen dominios de seguridad independientes. En la medida de lo posible, la generación también debe evitar un mismo entorno comprometido.

Responsabilidad de custodia del participante. Las semillas A, B y C, las claves privadas, frases de recuperación, dispositivos físicos y copias de seguridad permanecen bajo la custodia y responsabilidad operativa del participante. Osnias Clearing no mantiene, deposita en garantía, respalda, recupera ni controla ninguna clave privada ni frase de recuperación de los participantes. Estos siguen siendo responsables de la generación, almacenamiento, recuperación, accesos y política de custodia.

Aislamiento de fallos comunes. Semillas distintas creadas en un mismo dispositivo comprometido, en una misma sesión o entorno de recuperación, o bajo un control administrativo común, no garantizan un aislamiento completo. Los despliegues institucionales deberían demostrar la separación mediante ceremonias de generación de claves, dominios HSM o de custodia separados, o procedimientos equivalentes aprobados.

Riesgo de firma en el dominio B. Una autorización independiente no protege contra una firma conjunta maliciosa o una firma a ciegas. El control buscado consiste en vincular la autorización Sei a una intención legible por una persona, a Osnias-ID, al beneficiario, al activo, al importe, al nonce y a la expiración, para que el participante pueda verificar la operación antes de aprobarla. 7. Autorización compuesta y liberación segura de fondos

La función de liberación se basa en una condición compuesta. La firma válida del firmante EVM operativo solo es necesaria si la acción correspondiente la exige; no basta para redirigir los fondos depositados en garantía.

Condición compuesta de liberación

Objetivo de auditoría — condición compuesta. El diseño exige una vinculación Osnias-ID válida, un estado aceptable del registro, una autorización autenticada del segundo dominio o un estado canónico de la cadena de origen, la aprobación del verificador, garantías de vigencia y protección contra la reutilización, y una

coincidencia exacta con el beneficiario registrado previamente. La aplicación efectiva por el contrato sigue pendiente de demostración mediante implementación y pruebas.

Si se cumple la condición compuesta, los fondos se envían al beneficiario frío registrado, nunca a una dirección indicada a última hora por el firmante operativo.

Regla del beneficiario predefinido

Requisito de diseño — beneficiario predefinido. El beneficiario debe registrarse durante la incorporación o mediante un procedimiento que ofrezca protección equivalente. La vía normal de liberación no debe permitir al firmante operativo indicar un destino arbitrario. Se necesita evidencia de aplicación en el contrato antes de considerar verificado este control.

Conjunto mínimo de datos vinculados a la autorización

Una autorización en producción debería vincular, como mínimo: versión del protocolo y separador de dominio; Osnias-ID; identificadores de las cadenas de origen y destino; contrato de garantía verificador; identificador preciso del activo; código de divisa ISO 4217, cuando corresponda; ciclo o modo; importe; nonce único; referencia del estado canónico de origen; identificador de la autorización de liberación; compromiso del beneficiario; marca temporal; condición de expiración o vigencia.

Autorización de un solo uso y protección contra la reutilización

La prueba debe poder utilizarse una sola vez. El contrato de garantía debe registrar el consumo del nonce o del identificador de prueba y rechazar las reutilizaciones y sustituciones de contrato, cadena, importe y beneficiario.

Ciclo de vida del monedero de recepción

La dirección fría de recepción no firma durante su fase prevista de recepción; sirve como beneficiario predefinido y no como clave de autorización operativa. Si el participante mueve posteriormente esos fondos, la dirección pasa a una fase activa de firma. De forma opcional, puede designar una nueva dirección fría para futuras liberaciones. Esta elección responde a su política de seguridad y no constituye un intervalo obligatorio del protocolo.

Modelo de amenaza a largo plazo: compromiso de una clave y riesgo asociado a Shor

Objetivo de seguridad SG-1 — Insuficiencia de una sola clave: la recuperación de una clave privada ECDSA del participante, en particular la clave EVM operativa, no debe bastar para satisfacer toda la condición que autoriza la transferencia de fondos en garantía a una dirección controlada por el atacante. Se trata de una propiedad buscada por el diseño, no de un hallazgo de implementación ni de un resultado verificado independientemente.

Escenario prospectivo asociado a Shor

El algoritmo de Shor y sus adaptaciones a curvas elípticas permiten resolver el logaritmo discreto en tiempo polinómico en un ordenador cuántico ideal suficientemente potente. El protocolo no modifica este hecho. Considera que un futuro atacante podría recuperar la clave privada operativa correspondiente a una clave pública expuesta por la actividad normal de firma y examina qué podría hacer realmente con ella.

Objetivo del atacante

El objetivo económico relevante del atacante no se limita a suplantar la firma: consiste en provocar la transferencia de fondos legítimos del participante a una dirección bajo su control. La versión 4.3 separa estas dos capacidades.

El compromiso de 0xSIGNER no da el control de 0xRELEASE.

Por qué la clave recuperada sigue siendo insuficiente

La recuperación de la clave EVM operativa no proporciona acceso conocido a la clave Sei generada independientemente, no crea un estado canónico Sei auténtico, no satisface al verificador independiente y no revela ni controla la clave privada de la dirección fría independiente. Si el beneficiario es inmutable o está sujeto a un compromiso firme, el atacante no puede sustituir simplemente el destino por 0xATTACKER.

Superficie de ataque residual

El atacante debe entonces comprometer o eludir otras fronteras de confianza: segundo dominio de autorización, integridad del registro, verificación del estado canónico, control del verificador, gobernanza de actualizaciones o vinculación con el beneficiario. Estos riesgos residuales siguen siendo explícitos.

Osnias-ID, integridad de los registros y protección contra la reutilización

Osnias-ID vincula los dominios de seguridad del participante con el estado de su ciclo de vida. No aporta por sí mismo resistencia criptográfica. Por tanto, la integridad de los registros constituye una frontera de seguridad: las vinculaciones deben ser auténticas, coherentes en cuanto a su versión y bloquear la operación si divergen.

Coherencia de los registros y riesgo TOCTOU

Si una vinculación Osnias-ID cambia entre la creación de la autorización y la liberación en EVM, existe un riesgo de divergencia entre el momento de la comprobación y el del uso (TOCTOU). La lógica de producción debería vincular la autorización a una versión del registro, a un compromiso inmutable del beneficiario o a un estado de resolución específico del depósito en garantía. Cualquier divergencia entre las vistas de los registros debe bloquear la operación.

Separación del plano de control

La gestión de actualizaciones, emergencias y registros no debe restablecer una facultad de liberación basada en una sola clave. En particular, el firmante operativo no debe poder modificar por sí solo la dirección fría ni desactivar el requisito del segundo dominio.

Frontera de confianza del verificador. El verificador entre cadenas constituye una frontera de seguridad explícita. La implementación debe definir la autenticación del estado canónico Sei, la política de finalidad y reorganizaciones aceptada, el mecanismo de rotación o sustitución del verificador y el quórum o condición de prueba exigidos antes de cualquier liberación EVM. Mientras estos elementos no se demuestren en el código y las pruebas, SEC-003 permanece ABIERTO.

WW=00: modo de seguridad del depósito en garantía autónomo

La misma arquitectura puede funcionar sin compensación. WW=00 puede reservarse a un modo explícito limitado al depósito en garantía: sin cámara, sin ciclo de 7, 28 o 91 días, sin compensación multilateral y sin transición de estado propia del clearing. Osnias-ID vincula entonces el depósito en garantía EVM, el dominio de autorización independiente y la dirección de recepción predefinida.

WW=00 significa «sin ciclo de clearing / modo exclusivamente de garantía». Nunca debe interpretarse como un ciclo de clearing de cero semanas.

En este modo, el evento del segundo dominio puede adoptar la forma de una autorización de liberación, una transición de estado reflejada, una aprobación de política u otro evento vinculado de forma única y aceptado por el verificador. Se mantiene el objetivo de insuficiencia de una sola clave.

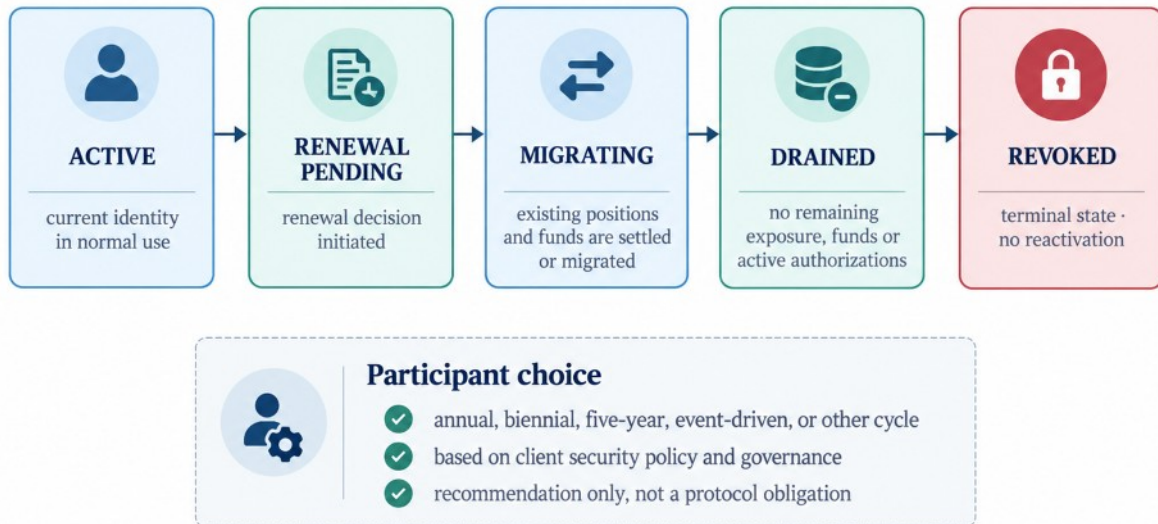
Higiene criptográfica, renovación de la identidad y salida

Osnias permite la renovación completa y voluntaria de la identidad criptográfica del participante como medida de seguridad operativa e higiene criptográfica. El protocolo no impone ningún intervalo de renovación. El participante decide de acuerdo con su política de seguridad, gobernanza, sistemas de custodia y análisis de riesgos.

El participante puede elegir una renovación anual, bienal, quinquenal, activada por un evento o con otra periodicidad. Estas elecciones no definen una duración de validez impuesta por el protocolo a las claves ECDSA o secp256k1.

Voluntary Cryptographic Identity Renewal Lifecycle

Osnias proposes the mechanism · The participant chooses whether and when to use it



The protocol supports renewal; the participant decides the timing.

Figura 2 — Ciclo de renovación voluntaria de la identidad

10

Renovación completa

Una renovación completa crea una identidad de seguridad realmente nueva, en lugar de modificar una vinculación de claves existente. Puede incluir un nuevo Osnias-ID, nuevas semillas independientes para el firmante EVM, Sei y la dirección fría, nuevas direcciones en cadena, nuevas vinculaciones en los registros y una migración o liquidación controlada de las posiciones y fondos existentes.

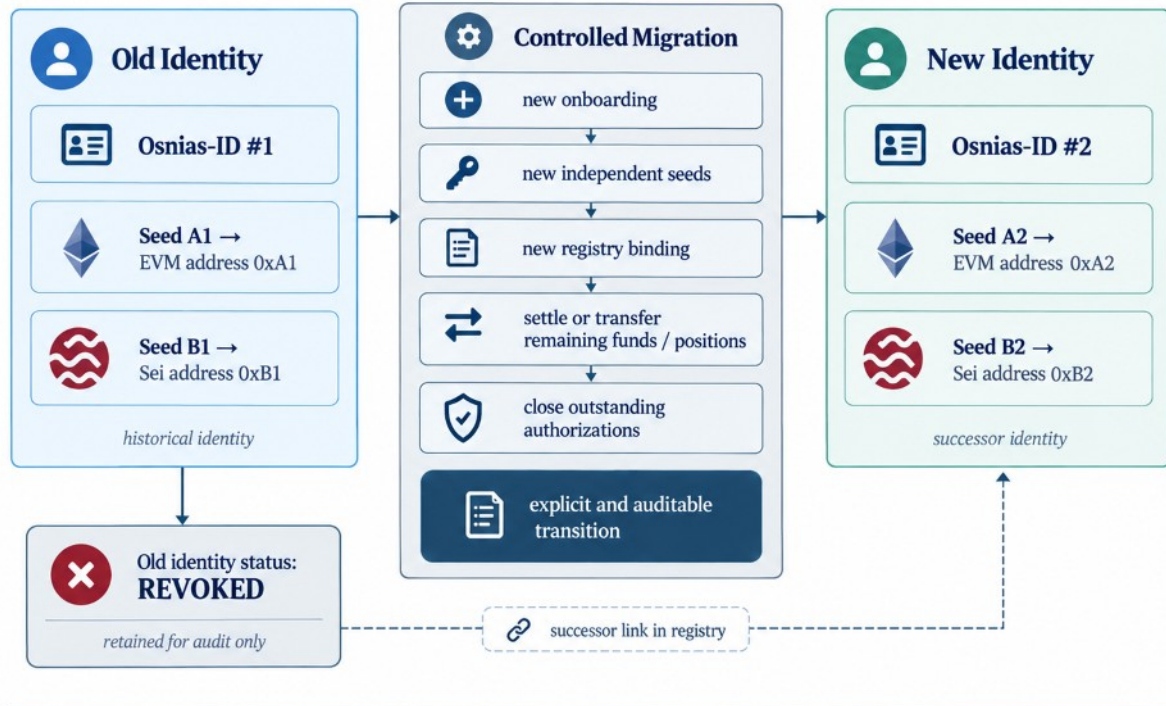
Frontera de riesgo de la migración. La migración es un estado del ciclo de vida que presenta un riesgo elevado. La vinculación con el sucesor solo debería hacerse efectiva después de verificar la autorización de migración, la versión del registro, los compromisos de destino y las posiciones restantes. Al finalizar la transición controlada, la identidad anterior no debe poder asumir nuevas exposiciones.

Salida y revocación definitiva

La identidad anterior sigue siendo consultable a efectos de verificación histórica y auditoría, pero pierde toda capacidad de crear nuevas autorizaciones tras su revocación final. Un ciclo posible es ACTIVO → RENOVACIÓN PENDIENTE → MIGRACIÓN → LIQUIDADO → REVOCADO. El estado REVOCADO es definitivo e irreversible.

Full Identity Renewal Procedure

New Osnias-ID · New independent seeds · New on-chain addresses



No in-place key rotation. Renewal creates a genuinely new security identity.

Figura 3 — Procedimiento de renovación completa de la identidad 11

El registro puede conservar, si es necesario, una referencia permanente entre el Osnias-ID revocado y su sucesor, sin modificar las vinculaciones históricas de las claves de la identidad anterior.

Ajuste del depósito en garantía por el participante

Tras la liquidación del lunes, día 1 del ciclo, el participante dispone de una ventana de ajuste de su depósito en garantía el martes, miércoles y jueves, días 2, 3 y 4. Durante esta ventana puede añadir fondos o solicitar la retirada del importe liberable de su depósito, sujeto a los controles de seguridad, las posiciones pendientes de liquidación y el límite aplicable al nodo. Esta facultad corresponde al participante y se distingue de las facultades del gestor de nodo durante la liquidación del lunes.

Las retiradas se ejecutan exclusivamente hacia la dirección específica de retirada, registrada previamente y distinta de la dirección del depósito en garantía. Este destino corresponde a la dirección fría de recepción del dominio C descrita en este Libro. Una solicitud de retirada no debe permitir elegir otro destino; sigue sujeta a la condición compuesta de liberación, a la verificación del importe liberable y a la protección contra la reutilización.

El jueves, día 4, el depósito en garantía se bloquea al cerrarse la ventana de ajuste. El importe retenido queda inmovilizado para la fase activa del ciclo; las aportaciones y retiradas a iniciativa del participante permanecen cerradas hasta la siguiente ventana autorizada. Esta inmovilización se distingue de la congelación de posiciones de clearing al final del ciclo. El bloqueo no debe impedir las operaciones de liquidación autorizadas al gestor de nodo.

Referencia de calendario: Libro 4 — Ciclos / Calendario. La secuencia de liquidación del lunes, ajuste del martes al jueves y bloqueo al cierre del jueves debe reflejarse en el estado canónico del ciclo y aplicarse mediante los contratos. La hora exacta de cierre UTC del jueves y su tratamiento en los límites siguen pendientes de especificación en el calendario de referencia; aquí no se presupone ninguna hora. El calendario testnet 1W debe armonizarse expresamente antes de aplicarle esta misma secuencia.

Claves de gestión y separación de facultades

Dos funciones de gestión complementan los tres dominios de seguridad A, B y C de los participantes. Cada gestor dispone de una clave específica derivada de una semilla independiente: una semilla propia del gestor de cada nodo y otra distinta para el gestor Osnias. No se trata de dos claves adicionales que deba aportar cada participante. No debe compartirse ninguna raíz de derivación ni dato de recuperación con los dominios A, B y C ni entre las funciones de gestión.

Gestor de nodo y ventana de netting

La clave del gestor de nodo autoriza operaciones de gestión únicamente en el nodo al que está asignada. Durante la ventana de netting del primer lunes del ciclo, este gestor tiene la facultad de ejecutar en los contratos inteligentes los ajustes de las cuentas de sus miembros conforme a las posiciones netas definitivas del ciclo cerrado. Ese lunes es el primer día del ciclo siguiente; los ajustes afectan a las obligaciones del ciclo anterior.

El gestor realiza los ajustes internos de las cuentas de sus miembros y procesa el saldo neto del nodo. Si su nodo adeuda un importe neto a la red, organiza la transferencia del excedente debido desde los depósitos en garantía correspondientes a la cuenta del nodo y, después, su liquidación conforme al circuito previsto. Si el nodo es acreedor, espera a recibir el saldo neto acreedor en la cuenta del nodo antes de finalizar los ajustes correspondientes en los contratos de los miembros.

Requisitos de diseño. Los contratos deben limitar estas operaciones al nodo, a los miembros, al ciclo y a los importes resultantes del netting. La cuenta del nodo y los destinos de liquidación deben identificarse en los registros; la clave de gestión no debe permitir designar libremente un beneficiario, modificar posiciones definitivas ni utilizar fondos de otro nodo. Las operaciones deben ser trazables y estar protegidas contra ejecuciones duplicadas. La ventana autorizada debe controlarse mediante el estado canónico del ciclo, y no únicamente mediante el reloj de la interfaz.

Gestor Osnias y parámetros de los nodos

La clave del gestor Osnias es distinta de las claves de los gestores de nodo. Autoriza la administración de los parámetros de los nodos, en particular la asignación de sus números y la configuración de un límite máximo de fondos en garantía por nodo conforme a las solicitudes del regulador aplicables al nodo correspondiente. Esta función, por sí sola, no confiere la facultad de ejecutar el netting de los miembros en sustitución del gestor de nodo ni de disponer de los activos depositados en garantía.

El límite de garantía constituye un requisito de control que debe implementarse en los contratos. Su definición debe precisar el activo o la unidad de cuenta, el ámbito de agregación de los depósitos en garantía del nodo y las operaciones que puedan superar el límite. Toda modificación debe fecharse, versionarse y registrarse con la referencia de la decisión correspondiente. Las modalidades de reducción del límite cuando ya existen fondos depositados siguen pendientes de especificación: una reducción no debe liberar fondos automáticamente ni impedir la liquidación de obligaciones existentes.

Custodia de claves y evidencias de control

Cada gestor conserva su propia semilla, clave privada y datos de recuperación bajo su responsabilidad. La documentación debe precisar, para ambas funciones, las direcciones autorizadas, la cadena y los contratos correspondientes, el procedimiento de asignación, rotación y revocación, las medidas en caso de compromiso y los posibles controles por umbral. Las funciones de gestión siguen sujetas al invariante administrativo: ninguna clave por sí sola debe eludir la condición compuesta de liberación de fondos de un participante ni modificar unilateralmente su beneficiario frío.

Las operaciones de liquidación del netting y las liberaciones al beneficiario frío constituyen dos circuitos distintos que deben documentarse y probarse. Las transferencias de netting deben justificarse por las

posiciones definitivas y limitarse a destinos de liquidación registrados. La descripción de una función y su semilla no demuestra la implementación de estas restricciones. Los controles anteriores tienen el estado REQUISITO DE DISEÑO / IMPLEMENTACIÓN Y PRUEBAS PENDIENTES.

Requisitos de refuerzo institucional

Los controles operativos en producción deben preservar la separación prevista por la arquitectura. Para un despliegue institucional, los siguientes controles forman parte del modelo de seguridad:

- dominios de generación de claves independientes y ceremonias verificables, preferiblemente con dominios HSM o de custodia separados;
- funciones de operadores, copias de seguridad y vías de recuperación separadas, con análisis explícito de fallos comunes;
- control por umbral o multipartito de los registros, la administración del verificador y las medidas de emergencia;
- procedimientos definidos de rotación de claves, revocación, respuesta a incidentes y bloqueo en caso de incertidumbre;
- actualizaciones inmutables o estrictamente controladas, con separación explícita de funciones;
- ninguna autoridad única de actualización debe poder modificar por sí sola la condición de liberación ni su beneficiario;
- registro y supervisión continuos de los estados de registros, oráculos, verificadores y depósitos en garantía;
- agilidad criptográfica que permita a claves, registros y verificadores migrar a firmas poscuánticas normalizadas o híbridas sin cambiar la función de Osnias-ID.

Los HSM separados o los procedimientos aprobados de generación aleatoria constituyen indicios operativos de separación de dominios de claves; no demuestran matemáticamente la independencia de todo el sistema. Administradores, copias de seguridad, datos de recuperación o planos de control de proveedores compartidos pueden seguir generando fallos comunes.

Limitaciones y trabajos abiertos

Este documento no pretende aportar una demostración formal de la composición de los controles. Antes de cualquier afirmación de seguridad en producción, la implementación debe precisar el modelo de adversario y corrupción, la verificación del estado canónico, la coherencia de los registros, el cuórum del verificador y las facultades de actualización, la modificación del beneficiario, la rotación de claves, los procedimientos de emergencia, los permisos y circuitos de liquidación del gestor de nodo, los parámetros y límites administrados por el gestor Osnias y una estrategia de migración poscuántica.

El resultado debe entenderse como una defensa en profundidad: puede aumentar el coste y los requisitos previos de un ataque, pero no transforma ECDSA clásico en una firma poscuántica. Las firmas poscuánticas normalizadas responden al problema criptográfico de base; Osnias aborda si el compromiso de una sola clave operativa debería bastar para liberar o desviar fondos.

Hoja de ruta de implementación y validación de seguridad

Esta evaluación describe la arquitectura de seguridad prevista para los usuarios finales de Osnias Clearing, su modelo de amenaza, fronteras de confianza, objetivos de auditoría y propiedades de seguridad buscadas. Separa los controles de diseño de las evidencias que deben producir la implementación y la validación.

No afirma que estas propiedades ya se hayan demostrado mediante código de producción desplegado, infraestructura auditada independientemente o un entorno operativo certificado.

La siguiente etapa es implementar esta arquitectura en el testnet público de Osnias, incluida la condición compuesta de liberación, las vinculaciones de los registros, los dominios de autorización independientes, la

dirección fría predefinida, la protección contra la reutilización, los controles del ciclo de vida y el bloqueo en caso de incertidumbre.

Una vez implementado el sistema, una campaña específica de seguridad adversarial combinará análisis estático, pruebas de integración y escenarios de ataque controlados contra el sistema real.

La validación debería incluir, según proceda: análisis estático de los contratos desplegados, en particular con Slither; pruebas adversariales del circuito de liberación y de su vinculación con el beneficiario; ensayos de reutilización, sustitución y estado obsoleto; pruebas de coherencia de registros y estados del ciclo de vida; escenarios de fallo del verificador y de los dominios de autorización; abusos de actualizaciones y del plano de control; ensayos de bloqueo ante estados incoherentes o no disponibles; pruebas de derechos de los gestores, restricciones de netting y límites de garantía por nodo; y, finalmente, corrección de hallazgos y nuevas pruebas.

El método de ataque detallado se definirá a partir del sistema efectivamente implementado, y no exclusivamente en la fase de diseño.

Al finalizar la campaña, Osnias prevé publicar un informe separado de validación de seguridad e implementación.

Ese informe debería precisar la implementación realmente probada: versiones de contratos, referencias de despliegue, condiciones de ensayo, escenarios de ataque ejecutados, resultados del análisis estático, fallos observados, correcciones, resultados de las nuevas pruebas y riesgos residuales.

Esta evaluación de preparación para la auditoría y el futuro informe de validación e implementación responden a objetivos diferentes: el presente texto define el diseño, los objetivos de control, los puntos abiertos y las evidencias requeridas; el futuro informe describirá el comportamiento observado tras el análisis estático, las pruebas adversariales, las correcciones y las nuevas pruebas.

En esta fase no se presupone ningún éxito de implementación ni resultado favorable de seguridad.

Conclusión

Conclusión de la evaluación. La arquitectura examinada define una separación real entre el firmante EVM operativo, el dominio de autorización Sei independiente y el beneficiario frío predefinido. El objetivo principal es preciso y comprobable: el compromiso de una clave ECDSA operativa no debería, por sí solo, satisfacer todas las condiciones de liberación ni redirigir los fondos en garantía a una dirección controlada por el atacante.

En la fase actual del documento, se trata de una propiedad de seguridad buscada y de un objetivo de diseño, no de un resultado observado en la implementación ni verificado independientemente. La implementación de contratos, la autenticación del estado canónico, la gobernanza del verificador, los controles administrativos, las pruebas adversariales, las correcciones y las nuevas pruebas siguen siendo necesarias antes de considerar verificados los controles.

Este documento sirve para preparar la auditoría y la revisión técnica. No constituye una auditoría independiente, una verificación formal, un informe de pruebas de penetración ni una certificación o cualificación de seguridad en producción.

Diseñado para las cadenas actuales. La seguridad anticipa el siguiente riesgo.

Bibliografía

- [1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, vol. 26, no. 5, 1997.
- [2] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," Quantum Information & Computation, vol. 3, no. 4, 2003. arXiv: quant-ph/0301141.
- [3] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum resource estimates for computing elliptic curve discrete logarithms," ASIACRYPT 2017, LNCS 10625.
- [4] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," International Journal of Information Security, 2001.
- [5] SECG, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010.
- [6] NIST, Module-Lattice-Based Digital Signature Standard, FIPS 204, 2024.

- [7] NIST, Stateless Hash-Based Digital Signature Standard, FIPS 205, 2024.
- [8] NIST SP 800-90A Rev. 1 and SP 800-90B, random bit generation and entropy-source recommendations.
- [9] P. Wuille, BIP-32: Hierarchical Deterministic Wallets, 2012.
- [10] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger (Ethereum Yellow Paper).
- [11] Sei Labs, Sei technical documentation, consensus and EVM documentation.
- [12] D. Bouzon, "Osnias-ID: An internal interchain identifier for multi-chain clearing," Osnias Clearing Technical Report, Release 2.0, 2026.
- [13] ISO 19011:2026, Guidelines for auditing management systems, Edition 4, May 2026.
- [14] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- [15] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls.
- [16] ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
- [17] ISO/IEC 27034-1:2011, Information technology — Security techniques — Application security — Part 1: Overview and concepts (confirmed current by ISO review).
- [18] NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, 2022.

Aclaración sobre las normas: las referencias [13] a [18] se citan como guías metodológicas y de diseño. No implican certificación, evaluación de conformidad, aprobación ni validación independiente de Osnias Clearing.