

Dossier de Verificación de Token

Raydium · Compromiso de autoridad admin

Documento de muestra. Reproduce la estructura y el formato exactos de un dossier entregable, construido sobre un caso real ya existente en el laboratorio de casos de norug.es. Sirve para calibrar el formato, revisión comercial y validación del pipeline. Los datos del caso son históricos y verificables.

IDENTIFICADOR DEL CASO SWAT-20261028-RAYDIUM-V1	ESTADO CANÓNICO SENSOR_BOUND_LIMITED
SUJETO Token: RAY / program authority	RED Solana mainnet
FECHA DE EMISIÓN 28 de octubre de 2026	MOTOR SWAT NeuralBus MCP v0.12.0
EVIDENCIAS EV-4D0F357CA65 · EV-6435F04B0C37 · EV-EA54F943D050	TRAZA OPERATIVA TRACE-7C41A9E2B8
VERSIÓN 1.0	CLASIFICACIÓN Uso interno · Composición con contraparte

DOCUMENTO CONFIDENTENCIAL. Su difusión, reproducción o uso fuera del ámbito autorizado requiere consentimiento expreso del propietario del caso. Este informe no ejecuta transacciones, no custodia fondos y no emite ratings regulados. El dictamen de la sección 10 es un análisis de riesgo con confianza y cobertura declaradas, no una recomendación de inversión.

01 Resumen ejecutivo	06 Superficie de riesgo del programa
02 Alcance, metodología y limitaciones	07 Timeline del incidente
03 Identidad del token y estructura de emisión	08 Actores y contraparties
04 Liquidity y estructura de holders	09 Score compuesto y cobertura de datos
05 Perfil del deployer y trazabilidad de fondos	10 Dictamen y condiciones
	11 Cadena de evidencia
	12 Expediente público y reutilización

01 RESUMEN EJECUTIVO

Se solicitó una verificación de token previa a admisión a mercado, con foco en la superficie de autoridad administrativa del programa. El encargo consiste en determinar si el token tiene un perfil de riesgo compatible con su listing y, en su caso, bajo qué condiciones.

El caso de referencia es el **compromiso de autoridad admin de Raydium (2022)**, uno de los incidentes más instructivos del ecosistema Solana: la pérdida de control sobre la autoridad administrativa permitió el drenaje de la pool de liquidez. El expediente se reconstruye con fuentes públicas y con el grafo de entidades de SWAT, y sirve como **caso de calibración** del motor: el resultado esperado de un token con autoridad admin concentrada y sin evidencia de mitigación verificable.

78/₁₀₀
RIESGO ALTO

Confianza del score	ALTA
Cobertura de datos SWAT	62%
Severidad máxima	CRITICAL
Severidad de atribución	UNKNOWN
Entidades analizadas	14
Hallazgos	3 CRITICAL · 2 HIGH · 1 MEDIUM

Advertencia de cobertura. «Live activity exists, but SWAT Core data coverage is below the declared threshold for full certainty. Treat the score as incomplete and rely on the declared coverage figure.» La cobertura del 62% no debe interpretarse como un resultado seguro ni como un resultado negativo: describe qué parte del análisis se apoya en cadena de evidencia sellada y qué parte en fuentes externas declaradas.

Qué se comprobó

- Identidad de la emisión: mint, decimals, metadata, mint authority, freeze authority, supply
- Estructura de liquidity: pools, TVL, locks, burning de LP tokens, concentración
- Perfil del deployer: historial de deploys, tokens previos, edad, wallet de funding
- Trazabilidad de fondos: ruta de funding, contrapartes, exposición a exploits conocidos
- Superficie de riesgo: permisos del programa, cuentas de programa, upgrade authority
- Scoring compuesto con cinco componentes ponderados

Qué queda fuera de alcance

- **Auditoría de smart contract.** No se revisa lógica de negocio, invariantes ni teoremas de solidez. Este dossier no sustituye a una auditoría de código.
- **Identificación de persona física.** Se modelan wallets, rutas y entidades. Una dirección no es una persona.
- **Asesoramiento legal, financiero o fiscal.** El dictamen no es una opinión jurídica ni una recomendación de inversión.
- **Verificación de equipo, roadmap o tokenomics fuera de la cadena.** No hay cobertura de fuentes fuera de la blockchain salvo las declaradas en §05.
- **Ejecución de transacciones o custodia de fondos.** SWAT no firma, no transfiere y no ejecuta.

Separación de fuentes

Este dossier distingue explícitamente dos planos, y ambos son verificables por separado:

PLANO	QUÉ INCLUYE	ESTADO	USO PERMITIDO
SWAT CORE	Datos leídos de la cadena, relaciones del grafo, cálculos derivados de ellos	Sellado	Sustenta el score, las relaciones y el dictamen
EXTERNO	Reportes públicos de terceros, preparación, comunicados, listas de exploit	Declarado, no sellado	Corrobora el contexto. No sostiene el score por sí solo
DESCONOCIDO	Atribución civil, intención, collusion, control efectivo	No determinable	Se declara como no determinable. Nunca se estima

Esta separación es deliberada. Ningún dato externo se presenta como si fuera evidencia canónica, y ningún dato no determinable se rellena con una estimación.

03 IDENTIDAD DEL TOKEN Y ESTRUCTURA DE EMISIÓN

CAMPO	VALOR	PLANO	LECTURA
Mint	4kzw3wG6mT1r2L9pQ8vX3nB7cD5eF4hJ6kL8mN9pQ2r	SWAT CORE	Identificador único de la emisión
Decimales	9	SWAT CORE	Convención de Solana
Supply total	1.000.000.000	SWAT CORE	Verificado contra el supply de mint
Mint authority	activa · 4kzw3wG6...	SWAT CORE	Hallazgo CRITICAL. Permite expandir supply
Freeze authority	activa · 4kzw3wG6...	SWAT CORE	Hallazgo CRITICAL. Permite bloquear cuentas
Update authority	activa · programa Raydium	SWAT CORE	Superficie de admin mutable
Metadata URI	arweave.net/.../metadata.json	SWAT CORE	Metadata inmutable. Correcto
Program owner	4kzw3wG6mT1...	SWAT CORE	Coincide con la autoridad de mint. Concentración
Identidad del emisor	no determinable	DESCONOCIDO	No se afirma equipo, identidad ni_control efectivo

Lectura. Mint authority, freeze authority y update authority activas y concentradas en la misma wallet son la configuración de mayor riesgo posible en un token SPL. No es un defecto exótico: es exactamente el vector que permitió el incidente de referencia de 2022. Ningún score de screening de una sola llamada capture esto con esta claridad.

04 LIQUIDITY Y ESTRUCTURA DE HOLDERS

MÉTRICA	VALOR	PLANO	LECTURA
TVL total	\$2.410.000	SWAT CORE	Concentrado en una pool principal
Volumen 24h	\$184.000	SWAT CORE	Cobertura de salida insuficiente para posiciones grandes
Pool principal	89% del TVL	SWAT CORE	Sin diversificación de venues
LP lock	ninguno detectado	SWAT CORE	Hallazgo CRITICAL. Retirada de liquidez sin fricción
Top 10 holders	41,3%	SWAT CORE	Excluyendo pools
Deployer wallet	6,2%	SWAT CORE	Hallazgo HIGH. Posición sin lock
Clusters relacionados	3 wallets · 0,7%	SWAT CORE	Relación detectada en grafo
Bundles de lanzamiento	4 wallets · mismo slot	SWAT CORE	Hallazgo HIGH. Señal de coordinación en el lanzamiento
Edad del token	8 días	SWAT CORE	Sin historial para evaluar comportamiento

05 PERFIL DEL DEPLOYER Y TRAZABILIDAD DE FONDOS

El deployer es una wallet con 3 deploys previos en la misma red, ninguno con retención de liquidity. El funding inicial procede de una wallet de funding que seintersecta con un cluster de wallets ya marcadas en la base de exploits de SWAT. La intersección es de un solo nodo y de baja confianza, y se declara como tal.

ELEMENTO	DETALLE	CONFIANZA	PLANO
Wallet deployer	8wrZotRfmsBAf6gVEaREoNAmRHD4jSSU9bp5DdUAaWwX	ALTA	SWAT CORE
Deploys previos	3 tokens · 2 sin holders Liquidity · 1 con mint authority revocada	ALTA	SWAT CORE
Edad de la wallet	3 días al momento del deploy	ALTA	SWAT CORE
Funding source	7yKq...9pQ (cluster C-118)	MEDIA	SWAT CORE
Intersección con base de exploits	1 nodo · peso 0,18 · sin coincidencia de victimario	MEDIA	SWAT CORE
Coincidencia con Slope breach	no detectada	ALTA	SWAT CORE
Coincidencia con Mango exploit	no detectada	ALTA	SWAT CORE
Identidad del emisor	no determinable	—	DESCONOCIDO

Sobre el caso de referencia: el incidente de Raydium de 2022 se produjo por compromiso de la autoridad admin del programa deAMM, con drenaje de pools. Fuentes públicas: Immunefi, CertiK y el post-mortem de Raydium.

El informe *no* usa ese caso para atribuir identidad al emisor actual: lo usa para calibrar qué configuración de autoridad debe disparar un hallazgo CRITICAL.

06 SUPERFICIE DE RIESGO DEL PROGRAMA

PERMISO	ESTADO	SEVERIDAD	EXPLOTABILIDAD	PLANO
Update authority del programa	activa	CRITICAL	Permite modificar el código del AMM en caliente	SWAT CORE
Withdraw authority	activa	CRITICAL	Permite drenar liquidity sin fricción	SWAT CORE
Admin multisig	1 de 3 firmas	HIGH	Umbral de firma demasiado bajo	SWAT CORE
Timelock	ausente	HIGH	Cambios de admin aplicables de inmediato	SWAT CORE
Account data size	8.192 bytes	MEDIUM	Dentro de rango normal	SWAT CORE
Upgradeable program	sí	INFO	Esperable en AMMs. Se documenta, no se penaliza	SWAT CORE

07 TIMELINE DEL INCIDENTE

T-3 días

Wallet del deployer creada y financiada desde el cluster C-118.

SWAT CORE · EV-4D0F357CA65

T-2 días

Mint authority, freeze authority y update authority se mantienen activas en la wallet del deployer. Sin revocación.

SWAT CORE · EV-6435F04B0C37

T0 · mismo slot

Cuatro wallets despliegan yIMAL en el mismo slot. Señal de coordinación.

SWAT CORE · EV-EA54F943D050

T0 + 4 min

Se crea la pool inicial con 89% del TVL y sin lock de LP tokens.

SWAT CORE · EV-8318101CBC63

T0 + 22 min

Primeras compras desde wallets bundled. Concentración de tenencia.

SWAT CORE

T+2 días

Empieza **میزة** la extracción de liquidity por la vía de la autoridad admin.

SWAT CORE · cobertura parcial

T+4 días

Retirada de la mayor parte de la liquidity. TVL residual por debajo del 5%.

SWAT CORE

T+5 días

Solicitud de verificación a SWAT. Emisión de este dossier.

TRAZA OPERATIVA

08 ACTORES Y CONTRAPARTIES

EMISOR / DEPLOYER

Wallet deployer

8wrZotRfmsBAf6gVEaREoNAmRHD4jSSU9bp5DdUAaWwX

3 días de antigüedad al desplegar. 3 deploys previos sin retención de liquidity.

MEDIUM Identidad no determinable

FUNDING

Wallet de funding · cluster C-118

7yKq3nF8bW2mL5xR9pQ4tV6hJ1kD8sA3fG7nZ2cE5r

Un nodo de intersección con la base de exploits. Peso 0,18. Sin coincidencia de victimario.

MEDIUM Relación, no atribución

PROGRAMA

AMM program

675kPX9MHTjS2zt1qfr1NYHuzeLXfQM9H24wFSUt1Mp8

Update authority y withdraw authority activas.
Timelock ausente.

CRITICAL Superficie de admin activa

POOL PRINCIPAL

Pool RAY/SOL

9WzDXwBbmkg8ZTbNMqUxvQRAyrZzDsGYdLVL9zYtAWMM

89% del TVL. Sin lock. Salida concentrada en una sola venue.

HIGH Liquidity withdrawable

09 SCORE COMPUESTO Y COBERTURA DE DATOS

COMPONENTE	PESO	RESULTADO	CONTRIBUCIÓN	BASE DEL CÁLCULO
Autoridad y control	30%	92 / 100	27,6	Mint, freeze, update y withdraw authority activas
Liquidity y estructura	25%	84 / 100	21,0	TVL, lock de LP, concentración, bundles
Perfil del deployer	20%	58 / 100	11,6	Edad, historial, funding, clusters
Token y holders	15%	48 / 100	7,2	Distribución, freeze, freeze de cuentas
Antigüedad y estabilidad	10%	100 / 100	10,0	8 días de existencia, sin historial
Score bruto	100%	—	77,4 → 78	Rescalado y capado a 100

Cobertura de datos

PLANO	VOLUMEN DE DATOS	CONTRIBUCIÓN AL SCORE	ESTADO
SWAT CORE cadena de evidencia sellada	14 entidades · 6 relaciones	42 pts	Sellado
EXTERNO fuentes públicas de terceros	4 referencias	18 pts	Declarado
DESCONOCIDO atribución e intención	—	18 pts	No determinable
Cobertura total	—	62%	Por encima del umbral mínimo

Los 18 puntos de atribución no determinable están en el score y no se rellenan con estimaciones. Un dossier con 30% de atribución y 70% de evidencia sellada es un dossier distinto de uno con 70% de atribución sin sellar, aunque el score bruto coincida. La cobertura es lo que los distingue.

Dictamen: No apto para admisión en condiciones actuales

La configuración de autoridad detectada en el programa (update authority y withdraw authority activas, multisig 1 de 3 firmas, sin timelock) reproduce el vector del incidente de referencia de 2022. Sumado a la ausencia de lock de LP tokens, a un deployer de 3 días con launches previos sin retención y a la concentración de bundles en el slot de creación, **la combinación de vectores es la que se cita en el caso histórico.**

El dictamen no es irreversible. Cambia con hechos verificables, no con negotiation.

CONDICIONES PARA REVERTIR EL DICTAMEN – CADA UNA VERIFICABLE ON-CHAIN

1. **Revocar mint authority y freeze authority** de la wallet del deployer, y verificarla. Evidencia: consulta de la cuenta del mint posterior a la revocación.
2. **Revocar o delegar la update authority** a un multisig con umbral mínimo 2 de 3 y timelock de al menos 48 horas. Evidencia: estado del programa y configuración del multisig.
3. **Revocar o restringir la withdraw authority.** Evidencia: estado del programa.
4. **Lock de LP tokens** por un mínimo de 6 meses o burn definitivo del 80% del supply en circulación. Evidencia: posición de lock verificable.
5. **Desbloquear o distribuir la posición del deployer** (6,2%) o transferirla a un multisig con timelock. Evidencia: distribución de tenencia posterior.
6. **Revisión de prohibición de lock** en la revisión de la que disponga la plataforma. Evidencia: distribución final de tenencia.

Condición de plazo: si las seis condiciones se cumplen y verifican dentro de los 30 días naturales siguientes a la emisión de este dossier, se emite una re-verificación sin coste adicional. Transcurridos 30 días sin cumplimiento, el dictamen se reevalúa desde cero con la nueva configuración y puede requerir un dossier nuevo.

Lo que este dictamen no dice. No afirma que el equipo detrás del token sea fraudulento. No afirma intención de fraude. No identifica a ninguna persona. Lo que afirma es que la configuración técnica observada en la cadena expone a los tenedores a un vector de pérdida total que ya se materializó en un caso público y verificable del mismo protocolo. La distinción entre «configuración de riesgo» y «comportamiento fraudulento» es sustantiva, y este dossier sólo mide lo primero.

11 CADENA DE EVIDENCIA

EV-4D0F357CA65

TIPO	Lectura de cuenta SPL · mint authority y freeze authority
CADENA	Solana mainnet · RPC público
ESTADO	Sellado en cadena de evidencia SWAT
VERIFICABILIDAD	Reconsultable por el titular del caso en cualquier momento

EV-6435F04B0C37

TIPO	Estado de permisos del programa · update y withdraw authority
CADENA	Solana mainnet · programa AMM
ESTADO	Sellado en cadena de evidencia SWAT
VERIFICABILIDAD	Reconsultable por el titular del caso

EV-EA54F943D050

TIPO	Bundles de lanzamiento · misma signature block
CADENA	Solana mainnet · 4 wallets
ESTADO	Sellado en cadena de evidencia SWAT
VERIFICABILIDAD	Reconsultable por el titular del caso

EV-8318101CBC63

TIPO	Estructura de la pool · TVL, lock de LP, concentración de holders
CADENA	Solana mainnet · pool principal
ESTADO	Sellado en cadena de evidencia SWAT
VERIFICABILIDAD	Reconsultable por el titular del caso

CAMPO	VALOR
Identificador del caso	SWAT-20261028-RAYDIUM-V1
Traza operativa	TRACE-7C41A9E2B8
Motor	SWAT NeuralBus MCP v0.12.0
Estado canónico	SENSOR_BOUND_LIMITED
Scope del cálculo de score	El token y su configuración. No reutilizable como rating de otro activo
Limitaciones registradas	Cobertura de sensores de Solana en expansión. Atribución no determinable. Sin auditoría de código

12 EXPEDIENTE PÚBLICO Y REUTILIZACIÓN

Con autorización del proyecto, este caso puede publicarse en forma de expediente forense en el laboratorio de casos de norug.es, en el formato JSON que el Globe carga natively («Cargar JSON propio»). La publicación

se genera **desde el caso sellado**, no desde una versión editada: el veredicto publicado es el mismo que el emitido.

ARTEFACTO	ESTADO	USO PREVISTO
Dossier sellado (PDF, 12 secciones)	PRIVADO	Expediente de admisión y de compliance. Contiene la cadena de evidencia completa
JSON del caso	COMPARTIDO CON AUTORIZACIÓN	Replay en el Globe. Verificable de forma independiente
Informe ejecutivo (1 página)	COMPARTIDO	Decisión de admisión de PM y CTO. Sin detalle de cadena de evidencia
Expediente público	CON AUTORIZACIÓN	Laboratorio de casos de norug.es. Versión sin datos sensibles
Re-verificación	SIN COSTE	Si las seis condiciones de la sección 10 se cumplen dentro de los 30 días

Regla de separación. El expediente público y la comunicación de marca se derivan del caso sellado. El dictamen no se edita para la publicación. Un expediente público con un veredicto más suave que el emitido invalidaría la cadena de evidencia y la confianza del sistema entero — y es la razón por la que el motor registra sus propios tickets de capacidad cuando un comprobador devuelve un falso positivo.

Acerca de esta muestra. Este documento es una **plantilla de formato con datos de demostración**. Reproduce la estructura, el tono y los mecanismos de evidencia de un dossier entregable, usando el incidente público de Raydium de 2022 como caso de calibración y un token ficticio como sujeto. Las direcciones, el score, la cobertura y el dictamen no corresponden a un token real y no deben citarse como findings de ningún activo. Antes de usarse con un cliente hay que sustituir el bloque de datos por el caso real emitido por el motor, y verificar que el JSON que sale tiene el mismo esquema que el que carga el Globe.

Fuentes del caso de referencia: Immunefi, CertiK y el post-mortem de Raydium sobre el compromiso de autoridad admin de 2022. Formato de expediente y capacidad de carga JSON verificados en norug.es/globe el 28 Oct 2026. Estructura de dossier derivada del informe SWAT-20261027-119319FE (27 Oct 2026).