BUSINESS SHOP A&A, S.A. de C.V., SOFOM, E.N.R.

Informe de Auditoría Interna de Seguridad

Contrato inteligente EKOPresaleVestingCandidateV3
Venta, vesting y referidos del token EKOKIIN · Red TRON

DICTAMEN: NO APTO PARA MAINNET EN SU VERSIÓN ACTUAL

Apto condicionado tras aplicar la remediación V3.1 y completar las condiciones de la sección 7.

Proyecto	Eko K'iin — «Energía que da vida» (EKOKIIN)
Versión auditada	SHA-256 fuente a726af86c3f39f5c…93eede8d
Compilador declarado	solc 0.8.20 · optimizador 200 · EVM London
Fecha de emisión	28 de septiembre de 2026
Documento	BSAA-AUD-EKO-V3-001
Clasificación	Auditoría interna — parte relacionada con el emisor

Este informe es una revisión interna emitida por una parte relacionada con el emisor del token. No constituye certificación de un auditor externo independiente, opinión legal ni recomendación de inversión.

1. Resumen ejecutivo

BUSINESS SHOP A&A revisó el contrato **EKOPresaleVestingCandidateV3**, que administra la preventa y venta pública del token EKOKIIN a cambio de USDT TRC-20, la liberación lineal (vesting) de 365 días y las comisiones por referidos de tres niveles (5 % / 3 % / 2 %). La revisión partió del paquete de pre-auditoría interna preparado por el equipo técnico y verificó de forma independiente sus conclusiones.

El contrato está bien estructurado: control de acceso consistente, protección contra reentrancia, reservas contables de vesting y comisiones, y transferencia de propiedad en dos pasos. Sin embargo, se identificó **un hallazgo crítico no detectado por la pre-auditoría ni por las pruebas locales**: el USDT oficial de TRON retorna false en `transfer()` aun cuando la transferencia es exitosa. Con el código actual, **ningún USDT podría salir jamás del contrato**: ni las comisiones de referidos ni los ingresos de la venta. Los fondos de los compradores quedarían bloqueados de forma permanente.

Severidad	Cantidad	Estado
Crítica	1	Corrección de código entregada (V3.1)
Alta	0	—
Media	3	Controles operativos fuera de la cadena, pendientes
Baja	3	1 corregida en V3.1; 2 aceptadas con mitigación
Informativa	6	1 corregida en V3.1; resto para decisión del emisor

Dictamen. La versión auditada (SHA-256 de fuente `a726af86c3f39f5c6a728d2ddac083fe76b755800d4836dc498c90a593eede8d`) **no es apta para despliegue en TRON Mainnet**. La versión remediada V3.1 corrige el hallazgo crítico en el código, pero sólo podrá considerarse apta tras cumplir las condiciones de la sección 7, en particular su compilación, pruebas con un token que reproduzca el comportamiento real del USDT en TRON y pruebas en Nile con el bytecode exacto a desplegar.

2. Alcance, metodología y limitaciones

Archivos revisados

Archivo	SHA-256 / nota
EKOPresaleVestingCandidateV3.sol (204 líneas)	`a726af86c3f39f5c6a728d2ddac083fe76b755800d4836dc498c90a593eede8d` Coincide con el hash declarado en el paquete.
MockToken.sol	Token de pruebas; retorna true en todas las operaciones.
test_v3_local.js, test_security_v3.js	Pruebas locales en Ganache con MockToken como USDT.
PRE_AUDITORIA_INTERNA_V3.md, REMEDIACION.diff	Pre-auditoría previa y su corrección EKO-M01.

Metodología

Revisión manual línea por línea asistida por herramientas de inteligencia artificial, enfocada en: control de acceso y funciones privilegiadas; integración con activos externos (USDT TRC-20 y EKOKIIN); contabilidad de inventario, vesting y comisiones; reentrancia y orden de efectos; aritmética y redondeo; diferencias TVM frente a EVM; y riesgos operativos y de centralización. Se contrastó el comportamiento documentado del contrato USDT de TRON con fuentes técnicas públicas.

Limitaciones

• El entorno de revisión no contaba con compilador ni acceso a red: **no se compiló ni se ejecutó** la versión V3.1 ni se cotejó bytecode. Estas verificaciones quedan como condiciones obligatorias (sección 7).
• No se revisó el código del contrato del token EKOKIIN ya desplegado, ni la página web, backend, integración con Sumsub o SunSwap.
• Este informe es emitido por una parte relacionada con el emisor. No es una certificación independiente, opinión legal, fiscal o regulatoria, ni recomendación de inversión.

3. Hallazgos

ID	Severidad	Título	Estado
EKO-C01	**Crítica**	USDT de TRON retorna false en transfer(): bloqueo permanente de USDT	Corregido en V3.1
EKO-M01	**Media**	Aprobación KYC sin evidencia verificable en cadena	Pendiente (operativo)
EKO-M02	**Media**	Autorreferido mediante múltiples wallets (hasta 10 %)	Pendiente (operativo)
EKO-M03	**Media**	Llave única del owner con control total de fondos y parámetros	Pendiente (operativo)
EKO-L01	**Baja**	Cotización obliga a pausar la venta cada 24 h y no tiene límites	Corregido en V3.1
EKO-L02	**Baja**	Congelamiento del contrato por el emisor de USDT	Aceptado / mitigación
EKO-L03	**Baja**	Compilador EVM vs. compilador TRON y chain ID de Mainnet	Pendiente (verificación)
EKO-I01	**Informativa**	Vesting lineal sin cliff desde el momento de compra	Decisión del emisor
EKO-I02	**Informativa**	Una sola compra por wallet	Decisión del emisor
EKO-I03	**Informativa**	El owner cobra comisión de nivel 1 por compradores directos	Confirmar vs. esquema firmado
EKO-I04	**Informativa**	Mensajes de error y evento de cancelación ambiguos	Corregido en V3.1
EKO-I05	**Informativa**	Sin mecanismo de reembolso en cadena	Decisión del emisor
EKO-I06	**Informativa**	Razón social del emisor inconsistente entre documentos	Pendiente (documental)

EKO-C01	**Crítica**	**USDT de TRON retorna false en transfer(): bloqueo permanente de USDT**
Ubicación	`withdrawReferralCredit()`, `withdrawProceeds()`	
Descripción	El contrato exige `require(usdt.transfer(...))`. El contrato USDT oficial en TRON (TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t) mueve el saldo correctamente pero **retorna false en transfer()**, comportamiento documentado públicamente, entre otros, por OpenZeppelin Contracts for Tron, que adapta su librería precisamente por este caso. Las pruebas locales usaron MockToken, que retorna true, por lo que el defecto no podía detectarse. `transferFrom()` sí retorna true, por eso las compras funcionan y el problema permanece oculto hasta el primer retiro.	
Impacto	Todas las llamadas de retiro de USDT revierten siempre. Ni los referidos pueden cobrar sus comisiones ni el owner puede retirar los ingresos de la venta. Como el contrato no es actualizable, **el 100 % del USDT recaudado quedaría bloqueado de forma permanente**.	
Recomendación	Aplicado en V3.1: funciones privadas `_pushExact` y `_pullExact` que realizan una llamada de bajo nivel, ignoran el valor de retorno, exigen que la llamada no revierta y verifican que el saldo del contrato cambie exactamente por el monto. Se aplican también a EKOKIIN por robustez. Agregar a las pruebas el mock `MockUSDTTronLike.sol` (entregado) y probar todos los retiros con él.	

EKO-M01	**Media**	**Aprobación KYC sin evidencia verificable en cadena**
Ubicación	`configureBuyer()`, `buy()`	
Descripción	La lista de compradores aprobados depende exclusivamente de la decisión del owner. El contrato no puede verificar que exista un resultado de Sumsub vigente vinculado a la wallet. (Coincide con EKO-M02 de la pre-auditoría).	
Impacto	Una aprobación errónea o no documentada habilitaría compras sin KYC, con exposición regulatoria y de prevención de lavado.	
Recomendación	Procedimiento documentado: aprobar sólo wallets con verificación Sumsub vigente, conservar el vínculo identidad-wallet y el ID de verificación, y probar revocación. Considerar un rol de operador KYC separado del owner.	

EKO-M02	**Media**	**Autorreferido mediante múltiples wallets**
Ubicación	`registerReferrer()`, bucle de referidos en `buy()`	
Descripción	El contrato impide referirse a uno mismo con la misma wallet y evita ciclos, pero una persona puede controlar varias wallets encadenadas y cobrar hasta 10 % de su propia compra. La cadena no puede probar identidad real. (Coincide con EKO-M03 de la pre-auditoría).	
Impacto	Descuento encubierto no previsto en el esquema comercial y pérdida de ingresos del emisor.	
Recomendación	Validar en el backend KYC que comprador y beneficiarios de niveles 1 a 3 sean personas distintas antes de aprobar la wallet; monitorear patrones de referidos y documentar la política en los términos de venta.	

EKO-M03	**Media**	**Llave única del owner con control total**
Ubicación	`onlyOwner`: fases, cotización, aprobaciones, retiros e inventario	
Descripción	Una sola llave controla la aprobación de compradores, la cotización, las fases, el retiro de USDT e inventario no vendido. No existe timelock ni firma múltiple.	
Impacto	El robo o pérdida de la llave del owner (TNCyBhtefa5kGDN1B6WyMpg4tHKRQP9LSE, propuesta) permitiría retirar todos los ingresos no reservados o paralizar la operación.	
Recomendación	Configurar la cuenta owner con permisos multifirma nativos de TRON (por ejemplo, 2 de 3 firmantes) antes de depositar inventario, resguardar llaves en hardware wallet y documentar un procedimiento de recuperación.	

EKO-L01	**Baja**	**Cotización con pausa obligatoria cada 24 horas y sin límites**
Ubicación	`configureQuote()`	
Descripción	La cotización vencía en máximo 24 horas y sólo podía renovarse con la venta pausada, lo que obligaba a interrumpir la venta diariamente. Además, el tipo de cambio no tenía límites, por lo que un error de captura podía fijar un precio absurdo.	
Impacto	Interrupciones diarias de la venta y riesgo operativo de error humano en una transacción firmada.	
Recomendación	Aplicado en V3.1: la cotización puede renovarse sin pausar (los compradores quedan protegidos por `expectedQuoteVersion` y `maxCost`), vigencia de hasta 30 días y tipo limitado entre 950,000 y 1,050,000 unidades por USD (valor de referencia 1,000,000).	

EKO-L02	**Baja**	**Congelamiento del contrato por el emisor de USDT**
Ubicación	Todas las funciones que mueven USDT	
Descripción	Tether puede incluir cualquier dirección en su lista negra. Si el contrato de venta fuera bloqueado, ningún USDT podría moverse.	
Impacto	Bloqueo de comisiones e ingresos por una decisión externa. No existe solución contractual unilateral.	
Recomendación	Aceptar el riesgo, retirar ingresos con periodicidad para limitar el saldo expuesto, y mantener cumplimiento KYC/AML que reduzca la probabilidad de una acción de bloqueo.	

EKO-L03	**Baja**	**Compilador y chain ID para TRON Mainnet**
Ubicación	Constructor, proceso de compilación y verificación	
Descripción	El paquete compila con solc de Ethereum 0.8.20 (EVM London). Para verificar el código en TRONSCAN se requiere el compilador y los ajustes exactos usados en el despliegue. El constructor exige `block.chainid` igual al valor recibido; las pruebas usan 3448148188 (Nile).	
Impacto	Imposibilidad de verificar el código públicamente o despliegue fallido con consumo de energía.	
Recomendación	Compilar y desplegar con la misma herramienta y versión que se usará en la verificación de TRONSCAN; obtener el chain ID de Mainnet con una llamada de lectura antes de firmar (valor esperado 728126428) y registrar ambos en la bitácora.	

EKO-I01	**Informativa**	**Vesting lineal sin cliff**
Ubicación	`claimable()`	
Descripción	La liberación comienza en el segundo de la compra y es lineal durante 365 días; no hay periodo inicial de bloqueo.	
Impacto	Compradores pueden reclamar tokens desde el primer día, con posible presión de venta temprana en SunSwap.	
Recomendación	Confirmar que coincide con el white paper y los términos de venta; si se requiere cliff, modificar antes de auditar externamente.	

EKO-I02	**Informativa**	**Una sola compra por wallet**
Ubicación	`buy()` — ONE_PURCHASE_PER_WALLET	
Descripción	Cada wallet sólo puede comprar una vez; una segunda compra requiere otra wallet con KYC.	
Impacto	Fricción comercial y posible incentivo a múltiples wallets (relacionado con EKO-M02).	
Recomendación	Confirmar que es la política deseada y comunicarla claramente en la página del token.	

EKO-I03	**Informativa**	**Comisión de nivel 1 al owner**
Ubicación	`registerReferrer()`, `buy()`	
Descripción	El owner es la raíz del árbol de referidos: por cada comprador directo acumula 5 % como crédito de referido, reservado separadamente de los ingresos.	
Impacto	Contabilidad de ingresos dividida entre dos rubros.	
Recomendación	Confirmar que es consistente con el esquema de comisiones firmado y reflejarlo en la contabilidad.	

EKO-I04	**Informativa**	**Mensajes de error y eventos ambiguos**
Ubicación	`registerReferrer()`, `cancelOwnershipTransfer()`	
Descripción	El owner recibía ALREADY_REGISTERED al intentar registrarse, y la cancelación de transferencia reutilizaba el evento de inicio.	
Impacto	Diagnóstico confuso en soporte y monitoreo.	
Recomendación	Aplicado en V3.1: error OWNER_IS_ROOT y evento OwnershipTransferCancelled.	

EKO-I05	**Informativa**	**Sin mecanismo de reembolso en cadena**
Ubicación	Diseño general	
Descripción	Si la venta se cancela, el contrato no permite devolver USDT a compradores; el owner puede retirar ingresos en cualquier momento.	
Impacto	La devolución dependería de un proceso manual fuera de la cadena.	
Recomendación	Definir en los términos de venta la política de cancelación y reembolso.	

EKO-I06	**Informativa**	**Razón social inconsistente**
Ubicación	Documentación del paquete	
Descripción	La pre-auditoría identifica al emisor como BUSINESS STORE, S.A. de C.V.; el acta constitutiva revisada corresponde a BUSINESS SHOP A&A, S.A. de C.V., SOFOM, E.N.R.	
Impacto	Confusión sobre la entidad responsable ante compradores, auditores y autoridades.	
Recomendación	Unificar la razón social del emisor en white paper, página del token, términos de venta y documentación técnica.	

4. Controles verificados satisfactoriamente

Área	Resultado
Control de acceso	Funciones privilegiadas protegidas por onlyOwner; transferencia de propiedad en dos pasos con aceptación explícita. claim, withdrawReferralCredit y registerReferrer operan sólo sobre msg.sender.
Reentrancia	Modificador lock en todas las funciones que mueven activos; el estado se actualiza antes de las llamadas externas.
Vesting	claimable() descuenta lo ya reclamado; un segundo claim sin tiempo transcurrido revierte. Inventario adeudado protegido frente a withdrawUnsoldInventory.
Referidos	Registro secuencial que impide ciclos y autorreferido directo. Suma máxima 10 % con división hacia abajo; créditos reservados frente a withdrawProceeds.
Límites de venta	1 a 100,000 tokens por compra; preventa hasta 100,000; pública hasta 900,000; total hasta 1,000,000; verificación de inventario libre antes de vender.
Pagos	Verificación de saldo exacto en cada ingreso de USDT (rechaza pagos incompletos o con comisión). Protección de precio con maxCost y quoteVersion.
Aritmética	Solidity 0.8.20 con verificación nativa de desbordamiento. Precio: 1 token = 3,800,000 (preventa) y 5,240,000 (pública) unidades mínimas de USDT con tipo 1,000,000.
Salida de usuarios	claim y withdrawReferralCredit no dependen de la pausa: los usuarios pueden retirar aun con la venta detenida (una vez aplicada EKO-C01).

5. Remediación entregada (V3.1)

Se entrega `EKOPresaleVestingCandidateV3_1.sol` con los cambios mínimos necesarios, el diff `REMEDIACION_V31.diff` y el mock `MockUSDTTronLike.sol`. SHA-256 de la fuente V3.1:
`78bb26f580d83b54a93176871bbbebf37ab0716fc394d183c12821c0e6a8f102`

Hallazgo	Cambio en código
EKO-C01	Nuevas funciones _pushExact / _pullExact con llamada de bajo nivel y verificación exacta de saldo; reemplazan todas las transferencias de USDT y EKOKIIN.
EKO-L01	configureQuote sin pausa obligatoria; límites MIN/MAX_MICRO_USDT_PER_USD (950,000 a 1,050,000) y vigencia máxima de 30 días.
EKO-I04	Error OWNER_IS_ROOT separado de ALREADY_REGISTERED; nuevo evento OwnershipTransferCancelled.

La versión V3.1 no ha sido compilada ni probada en este entorno. Cualquier cambio posterior, incluso en comentarios, altera el hash y el bytecode.

6. Pruebas mínimas requeridas

1. Compilar V3.1 con el compilador definitivo y registrar hash de fuente y de bytecode.
2. Ejecutar la batería existente sustituyendo el USDT de pruebas por MockUSDTTronLike.
3. Nuevas pruebas: withdrawProceeds y withdrawReferralCredit exitosos con token que retorna false; renovación de cotización durante la venta invalida compras con versión anterior; rechazo de tipos fuera de rango; claim parcial y total.
4. Desplegar V3.1 en Nile y repetir: compra con tres niveles, claim, pausa, depósito y retiro de inventario, retiro de comisiones y de ingresos.

7. Condiciones para declarar apto el despliegue en Mainnet

#	Condición	Responsable
1	Aplicar V3.1 y cumplir las pruebas de la sección 6 con resultado satisfactorio.	Equipo técnico
2	Cotejo del bytecode probado en Nile contra el bytecode a firmar en Mainnet: IGUAL.	Equipo técnico
3	Owner con multifirma TRON y prueba de control de cada firmante (EKO-M03).	Dirección
4	Procedimiento KYC y política antiautorreferido documentados (EKO-M01, EKO-M02).	Cumplimiento
5	Decisiones del emisor sobre EKO-I01, I02, I03, I05 y unificación de razón social (I06).	Dirección / Legal
6	Revisión por un auditor externo independiente de la versión final — recomendada firmemente antes de recibir fondos de terceros.	Dirección

8. Declaración y firma

Declaración de relación con el emisor. El firmante es socio fundador de BUSINESS SHOP A&A, S.A. de C.V., SOFOM, E.N.R., entidad vinculada al proyecto Eko K'iin. En consecuencia, este documento constituye una **auditoría interna realizada por una parte relacionada** y no una auditoría externa independiente. Se emite de buena fe con base en el código y la documentación descritos en la sección 2, y sus conclusiones se limitan a dicha versión.

Dato	Detalle
Firmante	Aldo Ahuja Montiel
Formación	Máster en Blockchain — ESDEN Business School en colaboración con Binance, Madrid, diciembre de 2023. Firma legitimada ante el Notario Juan José de Palacio Rodríguez y apostillada por el Colegio Notarial de Madrid el 09/02/2024 (No. N7201/2024/008691).
Entidad	BUSINESS SHOP A&A, S.A. de C.V., SOFOM, E.N.R. — Escritura No. 11,125, Libro 139, del 3 de noviembre de 2022, otorgada ante la Lic. Justina Reducindo Candanedo, Notaría Pública No. 1 de Zongolica, Veracruz.
Cargo	_____
Documento	BSAA-AUD-EKO-V3-001 · 28 de septiembre de 2026



_____

Aldo Ahuja Montiel

Máster en Blockchain · BUSINESS SHOP A&A

Firma autógrafa o firma electrónica avanzada (e.firma SAT)

Nota: la validez de este documento depende de la firma del emisor. Este informe no certifica la seguridad del contrato frente a terceros ni sustituye la opinión de un auditor externo independiente, de un abogado o de las autoridades competentes.