INFORME DE AUDITORÍA INTERNA No.: 1

FECHA DE EMISIÓN DEL INFORME	**Día:**	1	**Mes:**	12	**Año:**	2021

1. PROCESO:	Investigación, Evaluación Técnica.
2. LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):	Juan Pablo Abadía Medina
3. OBJETIVO DE LA AUDITORÍA:	Definir parámetros de mercadeo, desarrollo y definir pautas para mejorar el proyecto Granacoin
4. ALCANCE DE LA AUDITORÍA:	Describir los problemas que en la actualidad tiene el código de Granacoin y visibilidad de internet.
5. CRITERIOS DE LA AUDITORÍA:	Nos basamos en búsquedas en google y en el código generado el Jan-25-2021 con el contrato 0x2b16d25b75aec74519c0a7487d3c509e74299a8f en la red de ethereum.

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día		**Mes**		**Año**		**Desde:**	1/12/21 D / M / A	**Hasta:**	15/1/21 D / M / A	Día	15	Mes	12	Año	21

6. HALLAZGOS DE LA AUDITORÍA

6.1 ASPECTOS FUERTES DEL PROCESO:

Informamos los siguientes errores: ABIDecodeTwoDimensionalArrayMemory, EmptyByteArrayCopy, DynamicArrayCleanup, ImplicitConstructorCallvalueCheck, TupleAssignmentMultiStackSlotComponents, MemoryArrayCreationOverflow, privateCanBeOverridden, SignedArrayStorageCopy, ABIEncoderV2StorageArrayWithMultiSlotElement, DynamicConstructorArgumentsClippedABIV2, UninitializedFunctionPointerInConstructor_0.4.x, IncorrectEventSignatureInLibraries_0.4.x, ABIEncoderV2PackedStorage_0.4.x, ExpExponentCleanup, EventStructWrongData, Solidity Compiler Bugs

Mercadeo: ¡No hay presencia oficial del proyecto, no se visualiza redes sociales o backlinks del tema!

6.2 OBSERVACIONES

1. Errores en el código de solidity
2. No hay una web oficial token.
3. No hay presencia de redes del token (médium, Reddit, youtube, Telegram, discord, bitcointalk, github, whitepaper, gitlab) desde google.
4. En el Codigo no hay funciones de control de usuario, no hay herramientas actuales.

Codigo:

https://etherscan.io/address/0x2b16d25b75aec74519c0a7487d3c509e74299a8f#code

en el informe técnico de auditoria se entrega los errores que pueden causar desconfianza en los inversionistas.

6.3 Informe Técnico Código Fuente Token viejo

DESCRIPCIÓN	Error
Esto podría llevar a que estos punteros apunten a áreas de la memoria fuera del área real que se va a decodificar. De esta manera, era posible que `` abi.decode '' devolviera valores diferentes para la misma matriz de bytes codificada.	ABIDecodeTwoDimensionalArrayMemory
Si la longitud de la matriz de almacenamiento se aumenta posteriormente mediante el uso de `` .push () '' o asignando a su atributo `` .length '' (solo antes de 0.6.0), los elementos de la matriz de bytes recién creados no serán cero. inicializado, pero contienen los datos no relacionados	EmptyByteArrayCopy
Considere una matriz de almacenamiento de tamaño dinámico cuyo tipo base sea lo suficientemente pequeño como para que se puedan empaquetar múltiples valores en una sola ranura, como `uint128 []`	DynamicArrayCleanup
A partir de Solidity 0.4.5, se supone que el código de creación de contratos sin constructor pagadero explícito contiene una verificación de valor de llamada que da como resultado la reversión de la creación del contrato, si se pasa un valor distinto de cero.	ImplicitConstructorCallvalueCheck
Esto puede suceder en presencia de tuplas anidadas o si el lado derecho contiene punteros de función externa o referencias a matrices de datos de llamada dinámicos, mientras que el lado izquierdo contiene una omisión.	TupleAssignmentMultiStackSlotComponents
En los casos en los que el tamaño de la memoria de una matriz en bytes, es decir, la longitud de la matriz multiplicada por 32, es mayor que 2 ^ 256-1, la asignación de memoria se desbordará, lo que potencialmente resultará en áreas de memoria superpuestas	MemoryArrayCreationOverflow
Si bien los métodos privados de los contratos base no son visibles y no se pueden llamar directamente desde el contrato derivado	privateCanBeOverridden
Cuando se realiza una conversión al mismo tiempo, los bits para poner a cero se determinaron incorrectamente a partir del origen y no del tipo de destino.	SignedArrayStorageCopy
el puntero del elemento no avanza correctamente entre lecturas.	ABIEncoderV2StorageArrayWithMultiSlotElement
La cantidad de bytes para copiar se calculó incorrectamente en caso de que todos los parámetros tengan un tamaño estático pero contengan matrices de tamaño dinámico como miembros de estructura o matrices internas.	DynamicConstructorArgumentsClippedABIV2
Las posiciones del objetivo de salto son diferentes durante la construcción y después del despliegue, pero el código para establecer este objetivo de salto especial solo consideró la situación después del despliegue	UninitializedFunctionPointerInConstructor_0.4.x
En lugar de usar el tipo "dirección" en la firma con hash, se usó el nombre real del contrato, lo que generó un hash incorrecto en los registros.	IncorrectEventSignatureInLibraries_0.4.x
Esto puede provocar daños en los valores mismos, pero también puede sobrescribir otras partes de los datos codificados.	ABIEncoderV2PackedStorage_0.4.x
Los bits de orden superior en el exponente no se limpian correctamente antes de que se aplique el código de operación EXP si el tipo de expresión del exponente es menor que 256 bits y no menor que el tipo de la base.	ExpExponentCleanup
Si se utiliza una estructura en un evento, se registra la dirección de la estructura en lugar de los datos reales	EventStructWrongData

7. Otros Auditoria Tecnica

VULNERABILIDADES EN EL CÓDIGO

Gasto: (Requisito de gas de la función**)**

- **gracoToken.symbol**
- **gracoToken.name**
- **gracoToken.transferFrom**
- **gracoToken.approveAndCall**

Es infinito: si el requisito de gas de una función es superior al límite de gas de bloqueo, no se puede ejecutar. Evite bucles en sus funciones o acciones que modifiquen grandes áreas de almacenamiento (esto incluye borrar o copiar matrices en el almacenamiento)

GracoToken.() : Potencialmente debería ser constante pero no es.

variable **names**: gracoToken.balanceOf(address) : Las variables tienen nombres muy similares "saldos" y "saldos".

Condiciones: Utilice "assert (x)" si nunca quiere que x sea falso, no en ninguna circunstancia (aparte de un error en su código). Utilice "require (x)" si x puede ser falso, debido,

Datos Truncados: la division de valores enteros produce de nuevo un valor entero. eso significa, por ejemplo, 10/100=0 en lugar de 0.1, ya que el resultado es un numero entero de nuevo.

FUNCIONES

- **Función totalSupply():** genera el total de token creados.
- **Función balanceOf(address tokenOwner):** Devuelve la cantidad de tokens que posee una dirección (account). Esta función es un captador y no modifica el estado del contrato.
- **Función allowance(address tokenOwner, address spender):** El estándar ERC-20 permite que una dirección dé una asignación a otra dirección para poder recuperar tokens de ella. Este captador devuelve el número restante de tokens que spenderse le permitirá gastar en nombre de owner. Esta función es un captador y no modifica el estado del contrato y debería devolver 0 por defecto.
- **Función transfer(address to, uint tokens):** Mueve el número tokens de la dirección de la persona que llama a la función (msg.sender) a la dirección del destinatario. Esta función emite el Transferir. Devuelve verdadero si la transferencia fue posible.
- **Función approve(address spender, uint tokens)** Establecer la cantidad de token que permite la transferencia de la función de llamada (msg.sender) equilibrio. Esta función emite el evento de aprobación. La función devuelve si la asignación se estableció correctamente.
- **Función transferFrom(address from, address to, uint tokens)** Mueve la cantidad tokens de direccion recipiente mediante el mecanismo de asignación. la cantidad se deduce luego de la asignación de la persona que llama. Esta función emite el Transfer event.

7. Otros Auditoria Tecnica

EVENTOS

- **Event Transfer(address indexed from, address indexed to, uint tokens);** Este evento se emite cuando la cantidad de tokens (valor) se envía de la dirección from a la dirección to.
- **Event Approval(address indexed tokenOwner, address indexed spender, uint tokens);** Este evento se emite cuando la cantidad de tokens (value) es aprobada por el dueño para ser utilizados por spender(Usuario final).

CONCLUSIONES:

Es un código compilado sin optimización “200”, en una versión pragma solidity ^0.4.24; esto ya es obsoleto librerías comparado con la actual pragma solidity ^0.8.2; no tiene control de acceso para realizar labores de BURN o quemado de token, Crear nuevos Token MINT, Agregar Administradores y roles.

8. RESPONSABLES INFORME DE AUDITORÍA

Nombre Completo	Responsabilidad	Firma
Juan Pablo Abadia Medina	Gerente	

9. OBSERVACIONES

Usencia de documentos:

- Whitepaper.
- Roadmap.
- Website del token.
- Plan Comercial.
- Diseño de Moneda en 3D.
- Desarrolladores (Mayerly, Carlos Albeiro) y existencia del token no tiene logo en el explorador.

Nota: en documento suministrado encontramos perfiles de comunidades con poca comunidad https://twitter.com/Gracocolombia https://www.facebook.com/profile.php?id=100073689724379