
	<b>BLOCKCHAIN TECHNOLOGY SAS</b>	Código :BT-A-002
	<b>TOKEN GRACO</b>	Fecha: 12 Dic de 2021
	<b>PROCESO: EVALUACIÓN Y CONTROL</b>	Versión: 02
	<b>FORMATO: INFORME DE AUDITORÍA INTERNA</b>	Número de Página 1 de 7

## INFORME DE AUDITORÍA INTERNA No. 2

<b>FECHA DE EMISIÓN DEL INFORME</b>	<b>Día:</b>	12	<b>Mes:</b>	12	<b>Año:</b>	2021
-------------------------------------	-------------	----	-------------	----	-------------	------

<b>1. PROCESO:</b>	Evaluación Técnica cambios del Código.
<b>2. LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):</b>	Juan Pablo Abadía Medina
<b>3. OBJETIVO DE LA AUDITORÍA:</b>	Definir parámetros de mercadeo, desarrollo y definir pautas para mejorar el proyecto Granacoin seguimiento de la Auditoría No.1 de Granacoin.
<b>4. ALCANCE DE LA AUDITORÍA:</b>	Describir los procesos técnicos del código actual de Granacoin y visibilidad de internet.
<b>5. CRITERIOS DE LA AUDITORÍA:</b>	Basados en el siguiente contrato 0x84aeA9789137bfEf54915d21DaD85ECbdcdF840b de la red BSC Maint, estudiaremos el proceso y llamaremos cada función. Basados en los nuevos links estudiaremos presencia en redes y comunidades.

	<b>BLOCKCHAIN TECHNOLOGY SAS</b>	Código :BT-A-002
	<b>TOKEN GRACO</b>	Fecha: 12 Dic de 2021
	<b>PROCESO: EVALUACIÓN Y CONTROL</b>	Versión: 02
	<b>FORMATO: INFORME DE AUDITORÍA INTERNA</b>	Número de Página 2 de 7

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día		Mes		Año		Desde:	12/12/21	Hasta:	13/1/21	Día	13	Mes	12	Año	21
							D / M / A		D / M / A						

## 6. HALLAZGOS DE LA AUDITORÍA

### 6.1 ASPECTOS FUERTES DEL PROCESO:


- Nombre Gracocoin
- Abreviatura GRACO
- Red: Binance Smart Chain (BSC)
- Network: Maint BSC
- Smart Contrac: 0x84aea9789137bfef54915d21dad85ecbdcdf840b
- Total coin supply: 15.000.000 coins
- Link: <https://bscscan.com/address/0x84aea9789137bfef54915d21dad85ecbdcdf840b#code>
- Fecha creacion: 9 diciembre 2021.

### 6.2 Bibliotecas e interfaces

- pragma solidity ^0.8.2;

Desplegado Granacoin token to mainnet with solidity ^0.8.2.

- import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
- bibliotecas seguras de OpenZeppelin. Esta es la implementación básica de ERC-20 en la que se basa GRACO.
- import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol";
- import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Snapshot.sol";
- import "@openzeppelin/contracts/access/AccessControl.sol";
- import "@openzeppelin/contracts/security/Pausable.sol";


	<b>BLOCKCHAIN TECHNOLOGY SAS</b>	Código :BT-A-002
	<b>TOKEN GRACO</b>	Fecha: 12 Dic de 2021
	<b>PROCESO: EVALUACIÓN Y CONTROL</b>	Versión: 02
	<b>FORMATO: INFORME DE AUDITORÍA INTERNA</b>	Número de Página 3 de 7

## 6.2 Bibliotecas e interfaces

- `import "@openzeppelin/contracts/token/ERC20/extensions/draft-ERC20Permit.sol";`
- archivo granacoin.sol

## 6.3 Informe Técnico Código Fuente Token GRACO

DESCRIPCIÓN	FUNCION
Puede realizar la función de Burning Token, realizar Recompras para poder Quemar Tokens. ** _burn(account, amount); **	ERC20Burnable
Con la función Snapshot nos permite obtener soporte del token en cualquier momento para tenerlo para consultas por temporadas definidas por una consecutiva, o tomar saldos de todos los titulares. ** _snapshot(); **  Escritura: <ul style="list-style-type: none"> <li>• &lt;Snapshot&gt; Write (crea una copia son consecutivo)</li> </ul> Lectura: <ul style="list-style-type: none"> <li>• &lt;TotalSupplyAt&gt; &lt;SnapshotId&gt;</li> <li>• &lt; BalanceOf &gt; ( Address ) and ( SnapshotId )</li> </ul>	ERC20Snapshot
El control de acceso, es decir, "a quién se le permite hacer esto", es increíblemente importante en el mundo de los contratos inteligentes. El control de acceso de su contrato puede regir quién puede acuñar tokens, congelar transferencias y muchas otras cosas. Por lo tanto, es fundamental comprender cómo lo implementa, no sea que alguien más robe todo su sistema.  Escritura: <ul style="list-style-type: none"> <li>• &lt; Grant Role &gt;</li> <li>• &lt; Renounce Role&gt;</li> <li>• &lt; Revoke Role &gt;</li> </ul> Lectura: <ul style="list-style-type: none"> <li>• &lt; Get Role Admin &gt;</li> <li>• &lt; Hash Role &gt;</li> </ul>	AccessControl

	<b>BLOCKCHAIN TECHNOLOGY SAS</b>	Código :BT-A-002
	<b>TOKEN GRACO</b>	Fecha: 12 Dic de 2021
	<b>PROCESO: EVALUACIÓN Y CONTROL</b>	Versión: 02
	<b>FORMATO: INFORME DE AUDITORÍA INTERNA</b>	Número de Página 4 de 7

### 6.3 Informe Técnico Código Fuente Token GRACO

DESCRIPCIÓN	FUNCION
la capacidad de realizar todas las operaciones del sistema con el administrador del sistema, esto permite evitar pérdidas.  Escritura: <ul style="list-style-type: none"> <li>&lt; Paused &gt; Activar o Desactivar</li> </ul> Lectura: <ul style="list-style-type: none"> <li>&lt; Paused &gt; Booleano (verdad y falso)</li> </ul>	Pausable
Muestra el total de token creados.	totalSupply
Devuelve la cantidad de tokens que posee una dirección ( account). Esta función es un captador y no modifica el estado del contrato.	balanceOf(address)
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.	allowance(address tokenOwner, address spender)
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.	transfer(address to, 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.	approve(address spender, 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.	transferFrom(address from, address to, uint tokens)

## 7. Compilación


### Compiler debug log:

Note: Contract was created during TxHash#  
0x02efe0ea7af149872c8e687999fea09657cb50879332dbaff371991012ee5953

Successfully generated ByteCode and ABI for Contract Address  
[0x84aea9789137bfef54915d21dad85ecbdcdf840b]

< Compiler Version: v0.8.10+commit.fc410830 > Optimization Enabled: 1

**Runs:** 200


	<b>BLOCKCHAIN TECHNOLOGY SAS</b>	Código :BT-A-002
	<b>TOKEN GRACO</b>	Fecha: 12 Dic de 2021
	<b>PROCESO: EVALUACIÓN Y CONTROL</b>	Versión: 02
	<b>FORMATO: INFORME DE AUDITORÍA INTERNA</b>	Número de Página 5 de 7

## 7. Compilación

**Contract Name:** Granacoin

**ContractABI:**

```
[{"inputs":[],"stateMutability":"nonpayable","type":"constructor"},{"anonymous":false,"inputs":[{"indexed":true,"internalType":"address","name":"owner","type":"address"},{"indexed":true,"internalType":"address","name":"spender","type":"address"},{"indexed":false,"internalType":"uint256","name":"value","type":"uint256"}],"name":"Approve","type":"event"},{"anonymous":false,"inputs":[{"indexed":false,"internalType":"address","name":"account","type":"address"}],"name":"Paused","type":"event"},{"anonymous":false,"inputs":[{"indexed":true,"internalType":"bytes32","name":"role","type":"bytes32"},{"indexed":true,"internalType":"bytes32","name":"previousAdminRole","type":"bytes32"},{"indexed":true,"internalType":"bytes32","name":"newAdminRole","type":"bytes32"}],"name":"RoleAdminChanged","type":"event"},{"anonymous":false,"inputs":[{"indexed":true,"internalType":"bytes32","name":"role","type":"bytes32"},{"indexed":true,"internalType":"address","name":"account","type":"address"},{"indexed":true,"internalType":"address","name":"sender","type":"address"}],"name":"RoleGranted","type":"event"},{"anonymous":false,"inputs":[{"indexed":true,"internalType":"bytes32","name":"role","type":"bytes32"},{"indexed":true,"internalType":"address","name":"account","type":"address"},{"indexed":true,"internalType":"address","name":"sender","type":"address"}],"name":"RoleRevoked","type":"event"},{"anonymous":false,"inputs":[{"indexed":false,"internalType":"uint256","name":"id","type":"uint256"}],"name":"Snapshot","type":"event"},{"anonymous":false,"inputs":[{"indexed":true,"internalType":"address","name":"from","type":"address"},{"indexed":true,"internalType":"address","name":"to","type":"address"},{"indexed":false,"internalType":"uint256","name":"value","type":"uint256"}],"name":"Transfer","type":"event"},{"anonymous":false,"inputs":[{"indexed":false,"internalType":"address","name":"account","type":"address"}],"name":"Unpaused","type":"event"},{"inputs":[],"name":"DEFAULT_ADMIN_ROLE","outputs":[{"internalType":"bytes32","name":"","type":"bytes32"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"DOMAIN_SEPARATOR","outputs":[{"internalType":"bytes32","name":"","type":"bytes32"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"MINTER_ROLE","outputs":[{"internalType":"bytes32","name":"","type":"bytes32"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"PAUSER_ROLE","outputs":[{"internalType":"bytes32","name":"","type":"bytes32"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"SNAPSHOT_ROLE","outputs":[{"internalType":"bytes32","name":"","type":"bytes32"}],"stateMutability":"view","type":"function"},{"inputs":[{"internalType":"address","name":"owner","type":"address"},{"internalType":"address","name":"spender","type":"address"}],"name":"allowance","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[{"internalType":"address","name":"spender","type":"address"},{"internalType":"uint256","name":"amount","type":"uint256"}],"name":"approve","outputs":[{"internalType":"bool","name":"","type":"bool"}],"stateMutability":"nonpayable","type":"function"},{"inputs":[{"internalType":"address","name":"account","type":"address"}],"name":"balanceOf","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[{"internalType":"address","name":"account","type":"address"},{"internalType":"uint256","name":"snapshotId","type":"uint256"}],"name":"balanceOfAt","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[{"internalType":"uint256","name":"amount","type":"uint256"}],"name":"burn","outputs":[],"stateMutability":"nonpayable","type":"function"},{"inputs":[{"internalType":"address","name":"account","type":"address"},{"internalType":"uint256","name":"amount","type":"uint256"}],"name":"burnFrom","outputs":[],"stateMutability":"nonpayable","type":"function"},{"inputs":[],"name":"decimals","outputs":[{"internalType":"uint8","name":"","type":"uint8"}],"stateMutability":"view","type":"function"},{"inputs":[{"internalType":"address","name":"spender","type":"address"},{"internalType":"uint256","name":"subtractedValue","type":"uint256"}],"name":"decreaseAllowance","outputs":[{"internalType":"bool","name":"","type":"bool"}],"state
```

	<b>BLOCKCHAIN TECHNOLOGY SAS</b>	Código :BT-A-002
	<b>TOKEN GRACO</b>	Fecha: 12 Dic de 2021
	<b>PROCESO: EVALUACIÓN Y CONTROL</b>	Versión: 02
	<b>FORMATO: INFORME DE AUDITORÍA INTERNA</b>	Número de Página 6 de 7

## 7. Compilación


```

Mutability:"nonpayable", "type": "function", {"inputs": [{"internalType": "bytes32", "name": "role", "type": "bytes32"}],
"name": "getRoleAdmin", "outputs": [{"internalType": "bytes32", "name": "", "type": "bytes32"}], "stateMutability": "view",
"type": "function", {"inputs": [{"internalType": "bytes32", "name": "role", "type": "bytes32"}, {"internalType": "address",
"name": "account", "type": "address"}], "name": "grantRole", "outputs": [], "stateMutability": "nonpayable", "type":
"function", {"inputs": [{"internalType": "bytes32", "name": "role", "type": "bytes32"}, {"internalType": "address", "name":
"account", "type": "address"}], "name": "hasRole", "outputs": [{"internalType": "bool", "name": "", "type": "bool"}], "stateMutability": "view",
"type": "function", {"inputs": [{"internalType": "address", "name": "spender", "type": "address"}, {"internalType": "uint256", "name": "addedValue", "type": "uint256"}], "name": "increaseAllowance", "outputs": [{"internalType": "bool", "name": "", "type": "bool"}], "stateMutability": "nonpayable", "type": "function", {"inputs": [{"internalType": "address", "name": "to", "type": "address"}, {"internalType": "uint256", "name": "amount", "type": "uint256"}], "name": "mint", "outputs": [], "stateMutability": "nonpayable", "type": "function", {"inputs": [], "name": "name", "outputs": [{"internalType": "string", "name": "", "type": "string"}], "stateMutability": "view", "type": "function", {"inputs": [{"internalType": "address", "name": "owner", "type": "address"}], "name": "nonces", "outputs": [{"internalType": "uint256", "name": "", "type": "uint256"}], "stateMutability": "view", "type": "function", {"inputs": [], "name": "pause", "outputs": [], "stateMutability": "nonpayable", "type": "function", {"inputs": [], "name": "paused", "outputs": [{"internalType": "bool", "name": "", "type": "bool"}], "stateMutability": "view", "type": "function", {"inputs": [{"internalType": "address", "name": "owner", "type": "address"}, {"internalType": "address", "name": "spender", "type": "address"}, {"internalType": "uint256", "name": "value", "type": "uint256"}, {"internalType": "uint256", "name": "deadline", "type": "uint256"}, {"internalType": "uint8", "name": "v", "type": "uint8"}, {"internalType": "bytes32", "name": "r", "type": "bytes32"}, {"internalType": "bytes32", "name": "s", "type": "bytes32"}], "name": "permit", "outputs": [], "stateMutability": "nonpayable", "type": "function", {"inputs": [{"internalType": "bytes32", "name": "role", "type": "bytes32"}, {"internalType": "address", "name": "account", "type": "address"}], "name": "renounceRole", "outputs": [], "stateMutability": "nonpayable", "type": "function", {"inputs": [{"internalType": "bytes32", "name": "role", "type": "bytes32"}, {"internalType": "address", "name": "account", "type": "address"}], "name": "revokeRole", "outputs": [], "stateMutability": "nonpayable", "type": "function", {"inputs": [], "name": "snapshot", "outputs": [], "stateMutability": "nonpayable", "type": "function", {"inputs": [{"internalType": "bytes4", "name": "interfaceId", "type": "bytes4"}], "name": "supportsInterface", "outputs": [{"internalType": "bool", "name": "", "type": "bool"}], "stateMutability": "view", "type": "function", {"inputs": [], "name": "symbol", "outputs": [{"internalType": "string", "name": "", "type": "string"}], "stateMutability": "view", "type": "function", {"inputs": [], "name": "totalSupply", "outputs": [{"internalType": "uint256", "name": "", "type": "uint256"}], "stateMutability": "view", "type": "function", {"inputs": [{"internalType": "uint256", "name": "snapshotId", "type": "uint256"}], "name": "totalSupplyAt", "outputs": [{"internalType": "uint256", "name": "", "type": "uint256"}], "stateMutability": "view", "type": "function", {"inputs": [{"internalType": "address", "name": "recipient", "type": "address"}, {"internalType": "uint256", "name": "amount", "type": "uint256"}], "name": "transfer", "outputs": [{"internalType": "bool", "name": "", "type": "bool"}], "stateMutability": "nonpayable", "type": "function", {"inputs": [{"internalType": "address", "name": "sender", "type": "address"}, {"internalType": "address", "name": "recipient", "type": "address"}, {"internalType": "uint256", "name": "amount", "type": "uint256"}], "name": "transferFrom", "outputs": [{"internalType": "bool", "name": "", "type": "bool"}], "stateMutability": "nonpayable", "type": "function", {"inputs": [], "name": "unpause", "outputs": [], "stateMutability": "nonpayable", "type": "function"}

```

## 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.

	<b>BLOCKCHAIN TECHNOLOGY SAS</b>	Código :BT-A-002
	<b>TOKEN GRACO</b>	Fecha: 12 Dic de 2021
	<b>PROCESO: EVALUACIÓN Y CONTROL</b>	Versión: 02
	<b>FORMATO: INFORME DE AUDITORÍA INTERNA</b>	Número de Página 7 de 7


## 7. Compilación

- **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

### Documentos:

- Whitepaper.
  - Roadmap.
- Link: <https://github.com/granacoin/granacoin/blob/main/doc/whitepaper-es.md>
- Website del token. Link: <https://granacoin.com.co>

### Repositorio:

- <https://bitbucket.org/granacoin/graco/>
- <https://gitlab.com/granacoin/granacoin>
- <https://github.com/granacoin/granacoin>

## 10. CONCLUSIONES

- El Desarrollo del Token tiene la función de Mint que solo los administradores con el Rol de creación podrán usar a futuro para crear o Burn que pueden solo los Admin con Roles. Tiene librerías seguras y modernas @openzeppelin ofrece códigos seguros que se pueden emplear en token donde se le dé respaldo a los usuarios de la comunidad.