

LOTERIA DE CUNDINAMARCA

860037234

ORDEN DE PAGO

Numero: 1329

ACREEDOR: TECH AND KNOWLEDGE S.A.S NIT: 900529191

Vir.Bruto: 22.645.700,00

FECHA: 23/12/2024 DOCUMENTO: PRESTACION DE SERVICIOS 107-2024

Descuentos: 4.951.485,00

Vir Neto: 17.694.215,00

CONCEPTO: Frs:107-2024/ Desarrollo de pruebas técnicas y tácticas que permitan determinar si existen vulnerabilidades que amenacen la información de la empresa y prestar servicios expertos para apoyar el procedimiento de innovación tecnológica

CUENTA	NOMBRE CUENTA	TERCERO	DEBITO	CREDITO
511179	Honorarios	900529191 TECH AND KNOWLEDGE S.A.S	22.645.700,00	
24362704	Renta 9.66	900529191 TECH AND KNOWLEDGE S.A.S		183.830,00
243803	Honorarios	900529191 TECH AND KNOWLEDGE S.A.S		2.093.300,00
243625	Impuesto a las ventas retenido	900529191 TECH AND KNOWLEDGE S.A.S		542.355,00
24072204	Procultura	900529191 TECH AND KNOWLEDGE S.A.S		190.000,00
24072207	Estamp prodesarrollo UDEC	900529191 TECH AND KNOWLEDGE S.A.S		285.000,00
24072210	Estampilla bienestar adulto mayor	900529191 TECH AND KNOWLEDGE S.A.S		381.000,00
24072205	Estampilla Pro-Hospitales U	900529191 TECH AND KNOWLEDGE S.A.S		381.000,00
24072202	Prodesarrollo departamental	900529191 TECH AND KNOWLEDGE S.A.S		381.000,00
2407900204	Tasa prodeporte y recreación	900529191 TECH AND KNOWLEDGE S.A.S		476.000,00
24072203	Pro-Electrificación	900529191 TECH AND KNOWLEDGE S.A.S		38.000,00
24010101	Lotería de Cundinamarca	900529191 TECH AND KNOWLEDGE S.A.S		17.694.215,00
			22.645.700,00	22.645.700,00

Rubro	Registro	Giro	Saldo
2.1.2.02.02.008.003DII Servicios	913 45.291.400	22.645.700	22.645.700
Total	45.291.400	22.645.700	

900529191 TECH AND KNOWLEDGE S.A.S

Login: cargar

Periodo: 12

Numero: 2206

Elaborado por	Contador	Secretario General	Tesorero
---------------	----------	--------------------	----------

Empresa Industrial y Comercial Lotería de Cundinamarca Los Lunes, Hágase Rico	Informe de Supervisión	Código: 130-GC-F015 Versión: 1 Fecha: 12/03/2018 Página: 1 de 4
--	-------------------------------	--

1. INTRODUCCIÓN
<p>El Informe de Supervisión contiene toda la información relacionada con la ejecución del contrato en el periodo correspondiente.</p> <p>Teniendo en cuenta la naturaleza y tipo de contrato, y de conformidad con lo establecido en las obligaciones específicas del contrato 107-2024</p>

2. DATOS DEL SUPERVISOR	
Nombre del Supervisor:	RUBIELA EDITH ROMERO PARDO
Dependencia:	Oficina Asesora de Planeación e Informática
Cargo:	Jefe Oficina Asesora de Planeación e Informática

3. DATOS BÁSICOS DEL CONTRATO SUPERVISADO			
Contrato No.	107 DE 2024	Tipo de Contrato	PRESTACIÓN DE SERVICIOS
Contratista:	TECH AND KNOWLEDGE SAS		
Nit / C.C. Contratista:	900529191-5		
Plazo:	DESDE LA FIRMA DEL ACTA DE INICIO HASTA EL 30/12/2024		
Valor del Contrato:	\$ 45.291.400	C.D.P. No. 903-2024	
Objeto del Contrato: Realizar la contratación para el desarrollo de pruebas técnicas y tácticas que permitan determinar si existen vulnerabilidades que amenacen la información de la empresa y contratar servicios expertos para apoyar el procedimiento de innovación tecnológica con el fin de mitigar los riesgos inherentes a las actividades que se están ejecutando.			
Fechas de Control del Contrato_____			
Fecha Acta de Inicio del Contrato:	dd/mm/aa <u>29/11/2024</u>	Fecha Proyectada de Terminación del Contrato:	dd/mm/aa 30/12/2024
Prórroga: __No __X__	N/A		
Adición en \$	N/A		
Justificación:	N/A		

Empresa Industrial y Comercial Lotería de Cundinamarca Los Lunes, Hágase Rico	Informe de Supervisión	Código: 130-GC-F015 Versión: 1 Fecha: 12/03/2018 Página: 2 de 4
--	-------------------------------	--

4.DATOS DE LA CUENTA A CANCELAR		
Período a cancelar	Diciembre de 2024	
Saldo que viene	\$ 45.291.400	
Valor de la Factura Pago 1	\$ 22.645.700	Factura: 626
Saldo del Contrato a la Fecha	\$ 22.645.700	

5. SEGUIMIENTO CONTRACTUAL																												
GRADO DE CUMPLIMIENTO DEL OBJETO DEL CONTRATO EN EL PERÍODO A SUPERVISAR																												
Relación Actividades Realizadas:																												
<ul style="list-style-type: none"> El informe presentado por el contratista describe las vulnerabilidades tecnológicas encontradas en la infraestructura tecnológica de Lotería de Cundinamarca con corte el día 16 de diciembre del 2024. El contratista realizó las pruebas de intrusión las cuales se realizaron sobre el activo de la página Web de la Lotería de Cundinamarca, estas pruebas fueron realizadas del 13 de diciembre al 16 de diciembre del 2024 (3 días). El contratista muestra el detalle de los hallazgos obtenidos durante las pruebas de intrusión, como se evidencia en el siguiente cuadro, así como sus gráficos correspondientes. 																												
<table border="1"> <thead> <tr> <th rowspan="2">ID</th><th colspan="4">Hallazgos Identificados</th></tr> <tr> <th>CVSS v3.1</th><th>Impacto</th><th>Complejidad</th><th>Descripción</th></tr> </thead> <tbody> <tr> <td>2024_LOT_CUNDINAMAR CA_AVPT_001</td><td>4.6</td><td>Medio</td><td>Medio</td><td>Enumeración de Direcciones Email</td></tr> <tr> <td>2024_LOT_CUNDINAMAR CA_AVPT_002</td><td>4.0</td><td>Medio</td><td>Alta</td><td>Divulgación de Información</td></tr> <tr> <td>2024_LOT_CUNDINAMAR CA_AVPT_003</td><td>2.2</td><td>Bajo</td><td>Alta</td><td>Exposición de Portales Administrativos</td></tr> </tbody> </table>					ID	Hallazgos Identificados				CVSS v3.1	Impacto	Complejidad	Descripción	2024_LOT_CUNDINAMAR CA_AVPT_001	4.6	Medio	Medio	Enumeración de Direcciones Email	2024_LOT_CUNDINAMAR CA_AVPT_002	4.0	Medio	Alta	Divulgación de Información	2024_LOT_CUNDINAMAR CA_AVPT_003	2.2	Bajo	Alta	Exposición de Portales Administrativos
ID	Hallazgos Identificados																											
	CVSS v3.1	Impacto	Complejidad	Descripción																								
2024_LOT_CUNDINAMAR CA_AVPT_001	4.6	Medio	Medio	Enumeración de Direcciones Email																								
2024_LOT_CUNDINAMAR CA_AVPT_002	4.0	Medio	Alta	Divulgación de Información																								
2024_LOT_CUNDINAMAR CA_AVPT_003	2.2	Bajo	Alta	Exposición de Portales Administrativos																								
<ul style="list-style-type: none"> Por otra parte, el contratista realiza descripción de los hallazgos más relevantes identificados durante las pruebas realizadas, así como sus posibles implicaciones. De acuerdo con la forma de pago establecida queda el 50% del pago en cuentas por pagar, una vez culminadas las pruebas tácticas 																												

Empresa Industrial y Comercial Lotería de Cundinamarca Los Lunes, Hágase Rico	Informe de Supervisión	Código: 130-GC-F015 Versión: 1 Fecha: 12/03/2018 Página: 3 de 4
--	-------------------------------	--

NÚMERO DE CONTRATO	OBJETO DEL CONTRATO	DEFICIENTE	A MEJORAR	SATISFACTORIO	SOBRESALIENTE	NO APLICA	OBSERVACIONES
107	Realizar la contratación para el desarrollo de pruebas técnicas y tácticas que permitan determinar si existen vulnerabilidades que amenacen la información de la empresa y contratar servicios expertos para apoyar el procedimiento de innovación tecnológica con el fin de mitigar los riesgos inherentes a las actividades que se están ejecutando.			X			Queda pendiente por pagar el 50% del valor total del contrato
Concepto general del cumplimiento de las obligaciones derivadas del contrato.				X			NA

6. PLAN DE MEJORAMIENTO DEL CONTRATISTA ANTE UN DESEMPEÑO DEFICIENTE O A MEJORAR					
	Acción	Fecha Inicio dd/mm/aa	Fecha Final dd/mm/aa	Cumplió	
				Si	No
N/A		N/A	N/A		

7. RELACIÓN DE PAGOS A LA SEGURIDAD SOCIAL Y APORTES PARAFISCALES				
ITEM	PERIODO DE PAGO AÑO - MES	FECHA DE PAGO AÑO - MES - DÍA	VALOR	
Pensión	-	-	-	
Salud	-	-	-	
Riesgos Profesionales	-	-	-	
Certificado de revisor Fiscal - persona jurídica	anexa certificación de Revisor Fiscal	02/12/2024	-	

Empresa Industrial y Comercial Lotería de Cundinamarca Los Lunes, Hágase Rico	Informe de Supervisión	Código: 130-GC-F015 Versión: 1 Fecha: 12/03/2018 Página: 4 de 4
--	-------------------------------	--

8. DESCRIPCIÓN DE LOS RIESGOS QUE PUEDEN MATERIALIZARSE EN EL DESARROLLO DEL OBJETO DEL CONTRATO

Riesgo	Efecto	SI	NO
Variación de Precios			X
Incumplimiento de los plazos establecidos por parte del contratista	No se materializó	X	
Deficiente Calidad de los Materiales			X
No entrega a tiempo de los elementos contratados			X
Incumplimiento de las pólizas			X
Caso fortuito o fuerza mayor	No se materializó	X	
Incumplimiento de los términos de referencia	No se materializó	X	
Otro (Relacionar)			X

9. RESULTADO ESPERADO AL MOMENTO DE FINALIZAR EL CONTRATO

N/A

10. VERIFICACIÓN DE SOPORTES DEL CONTRATISTA

(Relacionar todos los soportes de la cuenta de cobro)

1. Presenta Informe de con la descripción de las vulnerabilidades tecnológicas encontradas en la infraestructura tecnológica de Lotería de Cundinamarca con corte el día 16 de diciembre del 2024.
2. Certificación de cumplimiento de pago de parafiscales y aportes al SGSSS, emitida por revisor fiscal y soportes que lo acreditan durante el periodo correspondiente a diciembre de 2024.
3. Presenta comprobante de pago planilla de seguridad social
4. Presenta Factura electrónica de venta N. 623

11. CERTIFICACIÓN DE PAGO

¿Procede el pago para este periodo?

SI ☒

NO ☐

12. OTRAS OBSERVACIONES RELEVANTES POR PARTE DEL SUPERVISOR

Sin observaciones adicionales.

FIRMA DEL SUPERVISOR:



Empresa Industrial y Comercial Lotería de Cundinamarca Los Lunes, Hágase Rico	Informe de Supervisión	Código: 130-GC-F015 Versión: 1 Fecha: 12/03/2018 Página: 5 de 4
--	-------------------------------	--

Fecha de Elaboración del Informe: 20 diciembre de 2024

CONTROL DE CAMBIOS		
No. Versión	Fecha	Descripción del Cambio
1	12/03/2018	Se modificó la codificación del Formato, para adaptarlo a los códigos de las Tablas de Retención Documental y se incluyó la modificación en el Listado Maestro de Registros.



Factura Electrónica De Venta

FE No. de Factura 626

Documento Oficial de Autorización de Numeración Facturación Electrónica No. 18764067194041 que habilita desde FE 501 hasta FE 3000. Vence 2025-03-12

Somos responsables del impuesto a las ventas - regimen comun
somos Agentes de retención de renta, art 437-2

Somos Responsables de Iva
no somos grandes contribuyentes

no somos agentes retenedores del impuesto sobre las ventas
no somos autorretenedores

Actividad económica 6201/6202/6209/6311
Actividad Económica 9,86 xml

TECH AND KNOWLEDGE S.A.S

Nit 900529191 5

Av. Cra 15 No. 119-43 Oficina 204

Teléfonos: 8053945

Bogotá D.C. Colombia

Fecha de Emisión: 20-dic-24

Fecha de Vencimiento: 19-ene-25

Código de Moneda:

Plazo (Días): 30

FACTURAS

CLIENTE EMPRESA INDUSTRIAL Y COMERCIAL LOTERIA DE CUNDINAMARCA
NIT 860037234 7
DIRECCIÓN CR 30 49 A 10
TELÉFONO 4802020
CIUDAD Bogotá D.C.

Item	Descripción	ValorUnitario	Cantidad	IVA	Total
1	SERVICIOS INFORMATICOS Contrato: 107-2024 Fecha contrato 25-11-2024 DETALLE: SERVICIOS DE CONSULTORIA TAK para la IMPLEMENTACIÓN DE PRUEBAS TECNICAS Y TACTICAS DE VULNERABILIDADES *Factura 1/2 con el 50% del contrato N. 107-2024	19.030.000,00	1	19%	19.030.000,00

Valor en Letras

VEINTIDOS MILLONES SEISCIENTOS CUARENTA Y CINCO MIL SETECIENTOS PESOS M/CTE

Favor precificar retención en la fuente del 3.5% según Decreto 2490 del 06 de diciembre de 2012 emitido por el Ministerio de Hacienda y Crédito Público.

FORMA DE PAGO

Consignación o transferencia en la Cuenta de Ahorro Banco Davivienda N. 006301200967 a nombre de TECH AND KNOWLEDGE S.A.S.

SUBTOTAL 19.030.000,00

IVA 3.615.700,00

TOTAL FACTURA 22.645.700,00

Total líneas o items: 1



Representación Gráfica de la Factura de Venta Electrónica

Fecha y Hora de Generación: 20/12/2024 11:44:41

Calle 127 # 70 G - 68 OF 315 Teléfono 6017704865

Correo Electrónico: facturación@takcolombia.com



Ciberseguridad Lotería de Cundinamarca Reporte Ejecutivo de Pruebas de Intrusión

Tabla de Contenido

Introducción	3
Objetivo	5
Metodología	6
Clasificación de las Vulnerabilidades	7
Alcance	8
Informe Técnico de Hallazgos	9
Resumen de Hallazgos	9
Referencias	11

CONFIDENCIAL



Empresa: EMPRESA INDUSTRIAL Y COMERCIAL LOTERIA DECUNDINAMARCA.

Ciudad: Bogotá

Dirección: Carrera 30 #49a-10

Contacto: Juan José Cristancho

INFORME GERENCIAL DE PRUEBAS DE INTRUSIÓN

Dirigida a	Rubiela Romero		
Palabras Claves	Pruebas de intrusión, evaluación, seguridad de la información y ciberseguridad.		
Formato	PDF	Reunión Inicial Requerimientos	03/12/2024
Código	EK – EHPT	Versión:	1.0
Autor y consultor	Ing. Miguel Javier Felizzola Figueredo - Pentester		
Revisó	Victoria Alzate – Product Manager		

APROBÓ	CARGO	FECHA DE APROBACIÓN
		16/12/2024:

	
Realizó: Ing. Miguel Javier Felizzola Figueredo	Aprobó: Victoria Alzate

Introducción

Las pruebas de intrusión constituyen un elemento fundamental para la gestión de riesgos tecnológicos, ya que permite la **identificación de vulnerabilidades y brechas de seguridad**, lo que ayuda a diseñar con exactitud e implementar un plan de acciones preventivas y correctivas para mejorar los controles técnicos de seguridad.

Lotería de Cundinamarca preocupado por garantizar la eficiencia en la prestación de servicios, poniendo especial énfasis en la seguridad de la información, ha decidido realizar pruebas de intrusión sobre **su aplicativo web expuesto en la red externa**, dicha aplicación a evaluar es empleada para la prestación de diversas tareas y servicios de la organización.

Enterkey realizó pruebas de penetración en la modalidad de Caja Negra que permiten identificar las vulnerabilidades existentes en los activos tecnológicos e identificar el riesgo derivado del aprovechamiento exitoso de estos. Las pruebas de caja negra son aquellas que se realizan sin el conocimiento de los activos que están bajo evaluación y sin ningún tipo de credenciales válidas.

El presente informe describe las vulnerabilidades tecnológicas encontradas en la infraestructura tecnológica de **Lotería de Cundinamarca** con corte el día 16 de diciembre del 2024.

Como parte del constante esfuerzo de **Lotería de Cundinamarca** en el fortalecimiento de su postura de seguridad, solicitó a **ENTERKEY** la ejecución de pruebas de intrusión a su aplicativo web, permitiendo identificar el estado actual de la seguridad que guardan sus activos. A continuación, se presentan los objetivos particulares del ejercicio:

- Identificación de vulnerabilidades tecnológicas en los activos bajo evaluación a través del **análisis automatizado y manual**.
- **Informar de manera técnica y ejecutiva** sobre los hallazgos realizados durante las pruebas realizadas, clasificándolos por su impacto.
- Aportación de recomendaciones que permitan la mitigación de las vulnerabilidades identificadas dentro del contexto de la organización, con el fin de **eleva la postura de seguridad**.

Para la ejecución de pruebas técnicas sobre **Lotería de Cundinamarca**, se utilizó una metodología que contempla un set robusto de pruebas técnicas automatizadas y manuales basadas en los estándares y normas alineadas al framework de pruebas del **Open Web Application Security Project** (OWASP, por sus siglas en inglés) y **The Penetration Testing Execution Standard** (PTES, por sus siglas en inglés). A continuación, se muestran las actividades que el framework contempla como parte de la metodología de las pruebas técnicas.

Reconocimiento

El reconocimiento es la parte de enumerar y obtener toda la información posible del organismo, ya sea mediante fuentes públicas o privadas (técnicas sigilosas) para así poder dibujar un diagrama de cómo está construida la empresa y analizar cuáles podrían ser unas posibles entradas y/o identificar sus puntos más débiles.

Modelo de Amenazas

El análisis de modelo de amenaza (TMA) es un análisis que ayuda a determinar los riesgos de seguridad que supone para un producto, aplicación, red o entorno, y cómo se pueden ver los ataques. El objetivo es determinar qué amenazas requieren mitigación y cómo mitigarlas.

Escaneos – Análisis de vulnerabilidades

En esta fase se realizan escaneos a todo lo identificado anteriormente para analizar y detectar vulnerabilidades, las cuales pueden ser aprovechadas en las siguientes fases.

Explotación

Esta fase consiste en aprovechar alguna vulnerabilidad identificada en las fases anteriores para obtener acceso a cierto lugar (sistema, aplicativo, servidor, etc) para forzar cambios en el flujo de ejecución con posibilidad de ser controlados a voluntad. Se valorarán las posibles vulnerabilidades a explotar con el líder de proyecto asignado por la organización y, una vez que se obtenga la aprobación de este, se utilizarán exploits previamente probados en el laboratorio de **ENTERKEY**, para corroborar las vulnerabilidades críticas identificadas en un intento de obtener acceso a la aplicación y/o infraestructura de soporte.

Post-explotación

Esta fase consta de mantener el acceso al equipo comprometido y hacer reconocimiento del sistema y poder elevar privilegios explotando alguna otra vulnerabilidad, poder meter persistencia, poder realizar movimientos laterales, hacer volcado de la memoria RAM, entre

otras actividades.

Generación de recomendaciones y reportes

Se realizará la documentación de los resultados del diagnóstico y se revisarán con el líder del proyecto. Una vez validado se generarán los escenarios de riesgo y la recomendación para la solución de las vulnerabilidades.

Clasificación de la información: 02-35

La ponderación de la severidad de las vulnerabilidades se realiza de acuerdo con la NVD (National Vulnerability Database) Vulnerability Severity Ratings (CVSS v3.1), el cual establece que de 0 a 3.9 la vulnerabilidad es de **severidad baja**, de 4.0 a 6.9 es de **severidad media**, de 7.0 a 8.9 es de **severidad alta** y de 9.0 a 10 es **Crítica**.

Impacto	Rango del CVSS V3.1	Definición
Crítico	9.0-10.0	La explotación es sencilla y generalmente da como resultado un compromiso total o parcial a nivel del sistema. Se aconseja formar un plan de acción y mitigar inmediatamente.
Alto	7.0-8.9	La explotación es complicada, pero podría causar potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda formar un plan de acción y mitigar tan pronto como sea posible.
Medio	4.0-6.9	Las vulnerabilidades existen, pero no tienen un impacto elevado sobre la seguridad de la información. Se recomienda formar un plan de acción y mitigar después de que se hayan resuelto los problemas de alta prioridad.
Bajo	0.1-3.9	Las vulnerabilidades existen, pero es difícil poder explotarlas, aunque reducen la superficie de ataque de la organización. Se recomienda formar un plan de acción y mitigar durante la próxima ventana de mantenimiento.
Informativo	N/A	No existe ninguna vulnerabilidad. Sino que proporciona información adicional sobre elementos observados durante las pruebas, controles estrictos y documentación adicional.

Las pruebas de intrusión se realizaron sobre diversos activos. A continuación, se detalla la información.

Ámbito	Detalle			
Activos	Las pruebas de intrusión se centraron en los siguientes activos de información:			
	<table> <tr> <th data-bbox="522 583 1133 625">URL</th><th data-bbox="1133 583 1383 625">IP</th></tr> <tr> <td data-bbox="522 625 1133 667">https://www.loteriadecundinamarca.com.co</td><td data-bbox="1133 625 1383 667">104.21.80.26</td></tr> </table>	URL	IP	https://www.loteriadecundinamarca.com.co
URL	IP			
https://www.loteriadecundinamarca.com.co	104.21.80.26			
Periodo de ejecución	Las pruebas de intrusión fueron realizadas del 13 de diciembre al 16 de diciembre del 2024 (3 días).			
Tipo de análisis	Desde el punto de vista del conocimiento previo: Caja Negra			
Equipamiento y herramientas utilizadas durante las pruebas	<p>Las pruebas de intrusión se realizaron utilizando los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> - Kali Penetration Testing and Ethical Hacking Linux Distribution - Windows 10 <p>Durante el análisis se utilizaron varias aplicaciones de auditoría de seguridad, entre las cuales se destacan:</p> <ul style="list-style-type: none"> - Burp Suite Professional - Nuclei - Netsparker - Metasploit - Nessus Tenable 			

Al realizar la prueba de penetración, se sigue la metodología establecida por **ENTERKEY** que está alineada con las recomendaciones de frameworks como OWASP, PTES y el NIST. Para el proyecto, se realizaron todas las pruebas descritas en la Guía de pruebas de OWASP (Versión 4), incluidas, entre otras, las siguientes:

- Pruebas de gestión de configuración e implementación
- Pruebas de gestión de identidad
- Pruebas de autenticación y autorización
- Pruebas de la Gestión de la Sesión
- Pruebas de validación de entrada
- Pruebas de manejo de errores
- Pruebas de criptografía débil

- Pruebas de lógica de negocios y pruebas del lado del cliente

Informe Técnico de Hallazgos

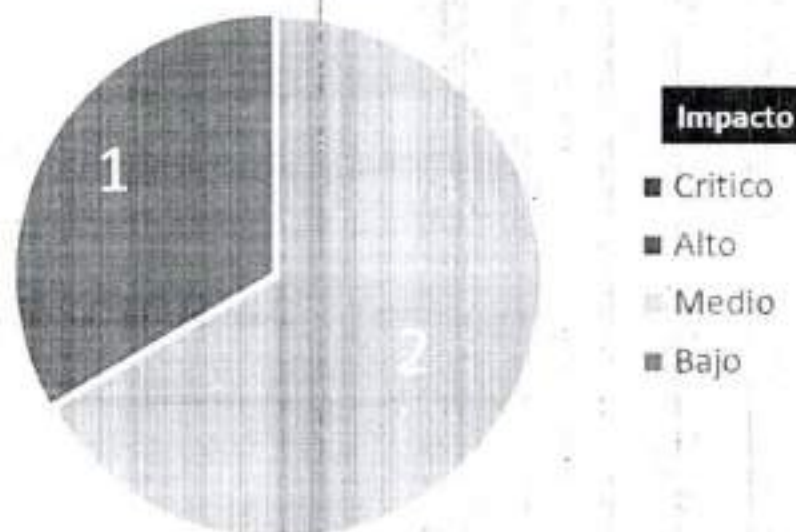
Resumen de Hallazgos

En la siguiente tabla se muestran los detalles de los hallazgos obtenidos durante las pruebas de intrusión:

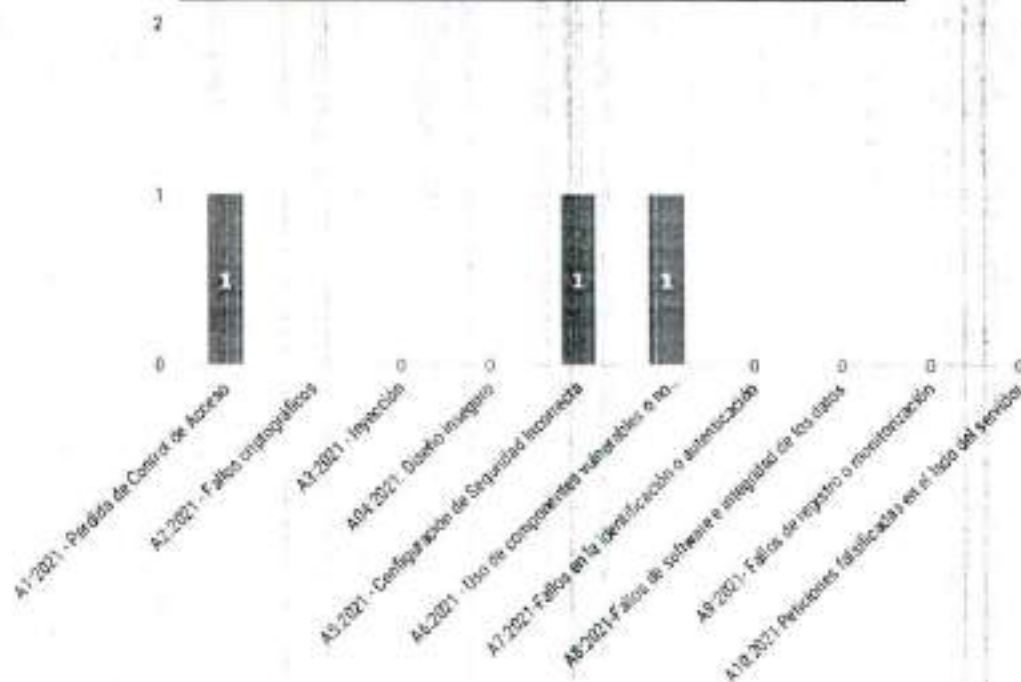
Hallazgos Identificados				
ID	CVSS v3.1	Impacto	Complejidad	Descripción
2024_LOT_CUNDINAMAR CA_AVPT_001	4.6	Medio	Media	Enumeración de Direcciones Email
2024_LOT_CUNDINAMAR CA_AVPT_002	4.0	Medio	Alta	Divulgación de Información
2024_LOT_CUNDINAMAR CA_AVPT_003	2.2	Bajo	Alta	Exposición de Portales Administrativos

A continuación, se muestran diversas gráficas que ilustran los hallazgos de las vulnerabilidades encontradas sobre el aplicativo analizado:

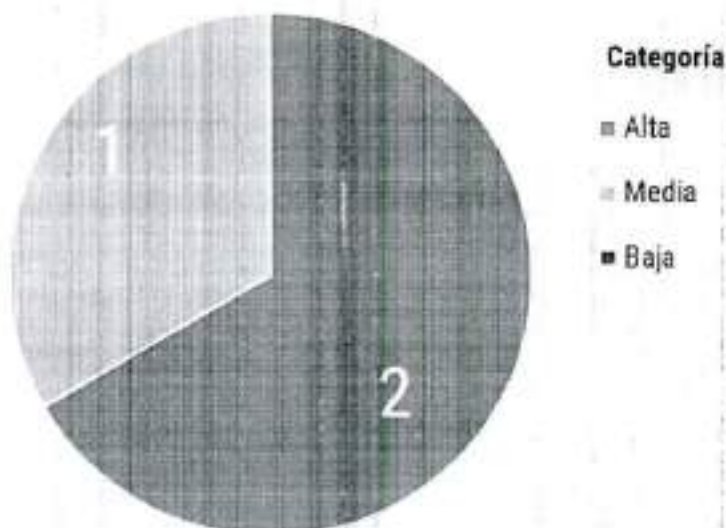
Vulnerabilidades Identificadas



Categorización de las Vulnerabilidades OWASP



Complejidad de explotación de las vulnerabilidades



A continuación, se describen los hallazgos más relevantes identificados durante las pruebas realizadas, así como sus posibles implicaciones:

- Se identificó que el portal de acceso permite la enumeración de correos electrónicos a través del formulario de inicio de sesión, revelando si un correo está registrado o no mediante mensajes de error específicos. Esto podría facilitar ataques de fuerza bruta o phishing. [2024_LOT_CUNDINAMARCA_AVPT_001: Enumeración de Direcciones Email]
- Durante el análisis de la aplicación, se identificó que existen componentes desactualizados con CVE asociados. Esta situación expone a la aplicación a riesgos de seguridad conocidos, ya que los componentes desactualizados pueden ser explotados por atacantes para ejecutar vulnerabilidades previamente documentadas. [2024_LOT_CUNDINAMARCA_AVPT_002: Uso de Componentes con Vulnerabilidades Conocidas.]
- Se detectaron portales de acceso a paneles administrativos accesibles públicamente. Esta exposición aumenta la probabilidad de ataques, como fuerza bruta o phishing, ya que los atacantes pueden intentar acceder a ellos conociendo la URL del portal. [2024_LOT_CUNDINAMARCA_AVPT_003: -Exposición de Portales Administrativos.]

Referencias

Se puede encontrar más información sobre las metodologías usadas en:

- OWASP (2022). *MASTG Mobile Application Security Testing Guide*. Recuperado de: <https://github.com/OWASP/owasp-mastg/releases/tag/v1.5.0>
- OWASP (2020). Wiki. *Open Web Application Security Project*. Recuperado de: http://www.owasp.org/index.php/Testing_Checklist
- OWASP (2022). *MASVS Mobile Application Security Verification Standard*. Recuperado de: <https://github.com/OWASP/owasp-masvs/releases/tag/v1.4.2>
- MITRE (2020). *Common Weakness Enumeration. Weaknesses Originally Used by NVD from 2008 to 2019*. Recuperado de: <http://cwe.mitre.org/data/definitions/635.html>
- NIST (2019). *National Vulnerability Database. Vulnerability Metrics*. Recuperado de: <http://nvd.nist.gov/cvss.cfm>

Por otro lado, es posible verificar las recomendaciones específicas que fueron señaladas a lo largo del informe en:

- OWASP TOP 10 (2021). *Broken Access Control*. Recuperado de: https://owasp.org/Top10/es/A01_2021-Broken_Access_Control/

- OWASP TOP 10 (2021). Using Components with Known Vulnerabilities. Recuperado de: https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities
- PORTSWIGGER (2020). Access Control. Recuperado de: <https://portswigger.net/web-security/access-control>



Ciberseguridad Lotería de Cundinamarca Reporte Técnico de Pruebas de Intrusión

•
Tabla de Contenido

FECHA DE APROBACIÓN	3
Introducción	4
Objetivo	5
Metodología	6
Clasificación de las Vulnerabilidades	7
• Alcance	8
Informe Técnico de Hallazgos	9
Resumen de Hallazgos	9
Detalle de Hallazgos	9
2024_LOT_CUNDINAMARCA_AVPT_001. – Enumeración de Direcciones Email.	9
2024_LOT_CUNDINAMARCA_AVPT_002. – Uso de Componentes con Vulnerabilidades Conocidas	14
2024_LOT_CUNDINAMARCA_AVPT_003. – Exposición de Portales Administrativos. .	16
•Referencias	20

CONFIDENCIAL



Empresa: EMPRESA INDUSTRIAL Y COMERCIAL LOTERIA DECUNDINAMARCA.

Ciudad: Bogotá

Dirección: Carrera 30 #49a-10

Contacto: Juan José Crislancho

INFORME GERENCIAL DE PRUEBAS DE INTRUSIÓN

Dirigida a	Rubiela Romero		
Palabras Claves	Pruebas de intrusión, evaluación, seguridad de la información y ciberseguridad.		
Formato	PDF	Reunión Inicial Requerimientos	03/12/2024
Código	EK – EHPT	Versión:	1.0
Autor y consultor	Ing. Miguel Javier Felizzola Figueredo - Pentester		
Revisó	Victoria Alzate – Product Manager		

APROBÓ	CARGO	FECHA DE APROBACIÓN
		16/12/2024

	
Realizó: Ing. Miguel Javier Felizzola Figueredo	Aprobó: Victoria Alzate

Introducción

Las pruebas de intrusión constituyen un elemento fundamental para la gestión de riesgos tecnológicos, ya que permite la **identificación de vulnerabilidades y brechas de seguridad**, lo que ayuda a diseñar con exactitud e implementar un plan de acciones preventivas y correctivas para mejorar los controles técnicos de seguridad.

Lotería de Cundinamarca preocupado por garantizar la eficiencia en la prestación de servicios, poniendo especial énfasis en la seguridad de la información, ha decidido realizar pruebas de intrusión sobre **su aplicativo web expuesto en la red externa**, dicha aplicación a evaluar es empleada para la prestación de diversas tareas y servicios de la organización.

Enterkey realizó pruebas de penetración en la modalidad de Caja Negra que permiten identificar las vulnerabilidades existentes en los activos tecnológicos e identificar el riesgo derivado del aprovechamiento exitoso de estos. Las pruebas de caja negra son aquellas que se realizan sin el conocimiento de los activos que están bajo evaluación y sin ningún tipo de credenciales válidas.

El presente informe describe las vulnerabilidades tecnológicas encontradas en la infraestructura tecnológica de **Lotería de Cundinamarca** con corte el día 16 de diciembre del 2024.

Como parte del constante esfuerzo de **Lotería de Cundinamarca** en el fortalecimiento de su postura de seguridad, solicitó a **ENTERKEY** la ejecución de pruebas de intrusión a su aplicativo web, permitiendo identificar el estado actual de la seguridad que guardan sus activos. A continuación, se presentan los objetivos particulares del ejercicio:

- Identificación de vulnerabilidades tecnológicas en los activos bajo evaluación a través del **análisis automatizado y manual**.
- **Informar de manera técnica y ejecutiva** sobre los hallazgos realizados durante las pruebas realizadas, clasificándolos por su impacto.
- Aportación de recomendaciones que permitan la mitigación de las vulnerabilidades identificadas dentro del contexto de la organización, con el fin de **eleva la postura de seguridad**.

Para la ejecución de pruebas técnicas sobre **lotería de Cundinamarca**, se utilizó una metodología que contempla un set robusto de pruebas técnicas automatizadas y manuales basadas en los estándares y normas alineadas al framework de pruebas del **Open Web Application Security Project** (OWASP, por sus siglas en inglés) y **The Penetration Testing Execution Standard** (PTES, por sus siglas en inglés). A continuación, se muestran las actividades que el framework contempla como parte de la metodología de las pruebas técnicas.

Reconocimiento

El reconocimiento es la **parte de enumerar y obtener toda la información posible del organismo, ya sea mediante fuentes públicas o privadas** (técnicas sigilosas) para así poder dibujar un diagrama de cómo está construida la empresa y analizar cuáles podrían ser unas posibles entradas y/o identificar sus puntos más débiles.

Modelo de Amenazas

El análisis de modelo de amenaza (**TMA**) es un análisis que ayuda a determinar los riesgos de seguridad que supone para un producto, aplicación, red o entorno, y cómo se pueden ver los ataques. El objetivo es determinar qué amenazas requieren mitigación y cómo mitigarlas.

Escaneos – Análisis de vulnerabilidades

En esta fase se realizan escaneos a todo lo identificado anteriormente **para analizar y detectar vulnerabilidades**, las cuales pueden ser aprovechadas en las siguientes fases.

Explotación

Esta fase consiste en **aprovechar alguna vulnerabilidad identificada** en las fases anteriores para obtener acceso a cierto lugar (sistema, aplicativo, servidor, etc) para forzar cambios en el flujo de ejecución con posibilidad de ser controlados a voluntad. Se valorarán las posibles vulnerabilidades a explotar con el líder de proyecto asignado por la organización y, una vez que se obtenga la aprobación de este, se utilizarán exploits previamente probados en el laboratorio de **ENTERKEY**, para corroborar las vulnerabilidades críticas identificadas en un intento de obtener acceso a la aplicación y/o infraestructura de soporte.

Post-explotación

Esta fase consta de mantener el acceso al equipo comprometido y hacer reconocimiento del sistema y poder elevar privilegios explotando alguna otra vulnerabilidad, poder meter persistencia, poder realizar movimientos laterales, hacer volcado de la memoria RAM, entre

otras actividades.

Generación de recomendaciones y reportes

Se realizará la documentación de los resultados del diagnóstico y se revisarán con el líder del proyecto. Una vez validado se generarán los escenarios de riesgo y la recomendación para la solución de las vulnerabilidades.

Clasificación de la vulnerabilidad

La ponderación de la severidad de las vulnerabilidades se realiza de acuerdo con la NVD (National Vulnerability Database) Vulnerability Severity Ratings (**CVSS v3.1**), el cual establece que de 0 a 3.9 la vulnerabilidad es de **severidad baja**, de 4.0 a 6.9 es de **severidad media**, de 7.0 a 8.9 es de **severidad alta** y de 9.0 a 10 es **Crítica**.

Impacto	Rango del CVSS V3.1	Definición
Crítico	9.0-10.0	La explotación es sencilla y generalmente da como resultado un compromiso total o parcial a nivel del sistema. Se aconseja formar un plan de acción y mitigar inmediatamente.
Alto	7.0-8.9	La explotación es complicada, pero podría causar potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda formar un plan de acción y mitigar tan pronto como sea posible.
Medio	4.0-6.9	Las vulnerabilidades existen, pero no tienen un impacto elevado sobre la seguridad de la información. Se recomienda formar un plan de acción y mitigar después de que se hayan resuelto los problemas de alta prioridad.
Bajo	0.1-3.9	Las vulnerabilidades existen, pero es difícil poder explotarlas, aunque reducen la superficie de ataque de la organización. Se recomienda formar un plan de acción y mitigar durante la próxima ventana de mantenimiento.
Informativo	N/A	No existe ninguna vulnerabilidad. Sino que proporciona información adicional sobre elementos observados durante las pruebas, controles estrictos y documentación adicional.

Las pruebas de intrusión se realizaron sobre diversos activos. A continuación, se detalla la información.

Ámbito	Detalle			
Activos	Las pruebas de intrusión se centraron en los siguientes activos de información:			
	<table> <tr> <th>URL</th><th>IP</th></tr> <tr> <td>https://www.loteriadecondinamarca.com.co</td><td>104.21.80.26</td></tr> </table>	URL	IP	https://www.loteriadecondinamarca.com.co
URL	IP			
https://www.loteriadecondinamarca.com.co	104.21.80.26			
Periodo de ejecución	Las pruebas de intrusión fueron realizadas del 13 de diciembre al 16 de diciembre del 2024 (3 días).			
Tipo de análisis	Desde el punto de vista del conocimiento previo: Caja Negra			
Equipamiento y herramientas utilizadas durante las pruebas	<p>Las pruebas de intrusión se realizaron utilizando los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> - Kali Penetration Testing and Ethical Hacking Linux Distribution - Windows 10 <p>Durante el análisis se utilizaron varias aplicaciones de auditoría de seguridad, entre las cuales se destacan:</p> <ul style="list-style-type: none"> - Burp Suite Professional - Nuclei - Netsparker - Metasploit - Nessus Tenable 			

Al realizar la prueba de penetración, se sigue la metodología establecida por **ENTERKEY** que está alineada con las recomendaciones de frameworks como OWASP, PTES y el NIST. Para el proyecto, se realizaron todas las pruebas descritas en la Guía de pruebas de OWASP (Versión 4), incluidas, entre otras, las siguientes:

- Pruebas de gestión de configuración e implementación
- Pruebas de gestión de identidad
- Pruebas de autenticación y autorización
- Pruebas de la Gestión de la Sesión
- Pruebas de validación de entrada
- Pruebas de manejo de errores
- Pruebas de criptografía débil

- Pruebas de lógica de negocios y pruebas del lado del cliente

Informe Técnico de Hallazgos

Resumen de Hallazgos

En la siguiente tabla se muestran los detalles de los hallazgos obtenidos durante las pruebas de intrusión:

ID	Hallazgos Identificados			
	CVSS v3.1	Impacto	Complejidad	Descripción
2024_LOT_CUNDINAMAR CA_AVPT_001	4.6	Medio	Media	Enumeración de Direcciones Email
2024_LOT_CUNDINAMAR CA_AVPT_002	4.0	Medio	Alta	Uso de Componentes con Vulnerabilidades Conocidas
2024_LOT_CUNDINAMAR CA_AVPT_003	2.2	Bajo	Alta	Exposición de Portales Administrativos

Detalle del Hallazgo

2024_LOT_CUNDINAMAR_CA_AVPT_001-Enumeración de Direcciones Email

La vulnerabilidad de enumeración de correos electrónicos a través del formulario de inicio de sesión ocurre cuando una aplicación web revela, mediante mensajes específicos, si un correo electrónico está registrado o no en su sistema. Este comportamiento suele manifestarse cuando los mensajes de error distinguen entre un correo electrónico inexistente y uno con credenciales incorrectas.

Por ejemplo:

- Al introducir un correo no registrado, se muestra un mensaje como *"El correo electrónico no está registrado"*.
- Al introducir un correo registrado con una contraseña incorrecta, se muestra un mensaje como *"Contraseña incorrecta para este correo"*.

Este comportamiento permite a un atacante realizar ataques de fuerza bruta o utilizar listas predefinidas de correos electrónicos para identificar cuentas válidas en la plataforma. Esta información podría ser utilizada posteriormente en ataques de phishing, fuerza bruta de contraseñas o ataques dirigidos.

Funcionalidad

Tras la ejecución de las pruebas, se identificó que el portal de acceso permite la enumeración de direcciones de correo electrónico registradas en el sistema.

Elemento afectado		Categoría	Puntaje
https://www.loteriadecundinamarca.com.co/?view=login		Base Score	5.3
		Temporal Score	4.6
		Environmental Score	4.6
Complejidad de Explotación	Media	Calificación	4.6
OWASP Web (2021)	A01:2021 – Control de Acceso Roto		

CVSS 3.1:

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:R/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N

Evidencia

Durante las pruebas realizadas, se identificó que el portal de acceso (Login) permite la enumeración de direcciones de correo electrónico registradas en el sistema. Este comportamiento ocurre debido a la diferenciación de los mensajes de error según el estado del correo electrónico ingresado:

- Al ingresar un correo no registrado, el sistema devuelve el mensaje: *"Email no existe en nuestro sistema"*.
- Al ingresar un correo registrado, como **admin@loteriacundinamarca.com.co** con una contraseña incorrecta, el sistema responde con el mensaje: *"Verifique contraseña"*.

Este comportamiento confirma la existencia de la cuenta asociada al correo electrónico ingresado y permite a un atacante distinguir entre direcciones de correo válidas e inválidas. Esto se puede observar a continuación:

CONFIDENCIAL



loteriadecundinamarca.com.co/view/login



Iniciar sesión

admin@loteriadecundinamarca.com.co

☐ Recuérdame

Iniciar sesión

Intranet Mercado

Copyright © 2004 Lotería de Cundinamarca. derechos reservados.

Mensaje de error cuando el Email se encuentra registrado en el sistema.

CONFIDENCIAL

loteriadecundinamarca.com.co/view/login#

896



The screenshot shows the login interface of the Lotería de Cundinamarca website. The background is dark with a white geometric pattern on the left. The logo, featuring a stylized 'K' and the text 'Lotería de Cundinamarca Los lunes, hágase rico', is in the top right. The login form is a white box with the title 'Iniciar sesión'. It contains two input fields: the first has the placeholder 'enterkey@loteriadecundinamarca.com.co' and the second has masked characters '*****'. A red arrow points from the first field to the second. A 'Iniciar sesión' button is at the bottom right of the form. Below the form, a message states 'Email no está en nuestro sistema'.

Mensaje de error cuando el Email no se encuentra registrado en el sistema.

5. Intruder attack of https://loteriadecundinamarca.com.co

Results Posters Payloads Resource pool Settings

Intruder attack results filter showing all items

Request	Payload	Status code	Response received
1	admin@loteriadecundinamarca.com.co	200	204
2	admin@loteriadecundinamarca.com.co	200	403
3	operaciones@loteriadecundinamarca.com.co	200	200
4	informatica@loteriadecundinamarca.com.co	200	241
5	informatica@loteriadecundinamarca.com.co	200	406
6	informatica@loteriadecundinamarca.com.co	200	246
7	marketing@loteriadecundinamarca.com.co	200	244
8	gerencia@loteriadecundinamarca.com.co	200	267
9	info@loteriadecundinamarca.com.co	200	247
10	relaciones_publicas@loteriadecundinamarca.com.co	200	250
11	compras@loteriadecundinamarca.com.co	200	434
12	gerencia@loteriadecundinamarca.com.co	200	287
13	administracion@loteriadecundinamarca.com.co	200	356
14	pagos@loteriadecundinamarca.com.co	200	202
15	comunicaciones@loteriadecundinamarca.com.co	200	217
16	servicio@loteriadecundinamarca.com.co	200	266
17	comunicacion@loteriadecundinamarca.com.co	200	263
18	desarrollo@loteriadecundinamarca.com.co	200	254
19	contacto@loteriadecundinamarca.com.co	200	345
20	gerencia@loteriadecundinamarca.com.co	200	235
21	comunicacion@loteriadecundinamarca.com.co	200	244
22	compras@loteriadecundinamarca.com.co	200	210
23	archivo@loteriadecundinamarca.com.co	200	410
24	legislacion@loteriadecundinamarca.com.co	200	257
25	informacion@loteriadecundinamarca.com.co	200	232
26	promociones@loteriadecundinamarca.com.co	200	272
27	legal@loteriadecundinamarca.com.co	200	245
28		200	244

Request Response

Problemas Error

```

Expires: Thu, 19 Nov 1992 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
CF-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https://a.nel.cloudflare.com/reports/v4?token=286752410x500x127019F00x5a75800x1A284
Kb2P0Ae"}], "group": "cf-nel", "max_age": 604800}
NEL: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
Strict-Transport-Security: max-age=0, includeSubDomains
X-Content-Type-Options: nosniff
Server: cloudflare
CF-Ray: 8f2cb8f0af87325a-09e
Alt-Svc: h3="443", max=0400
Server-Timing: cfLd, desc="FrontendTCP",rt=630756ms,rtt=564225rtt_var=224756sent=288recvr=115lost=00retr=00sent
<div class="alert alert-form alert-warning text-danger">
  Verifique contraseña
</div>

```

Finished

Enumeracion de emails de manera automatizada.

Recomendaciones

- Configurar los mensajes de error del portal de acceso para que no distingan entre correos electrónicos válidos e inválidos. Por ejemplo, utilizar un mensaje genérico como: "Credenciales incorrectas. Por favor, intente nuevamente."
- Implementar un mecanismo de protección contra fuerza bruta, como el bloqueo temporal de la cuenta después de un número determinado de intentos fallidos.

- Incorporar un CAPTCHA en el formulario de inicio de sesión para mitigar intentos automatizados de enumeración de correos electrónicos.
- Implementar un sistema de monitoreo y registro de actividad para detectar intentos inusuales de acceso, como múltiples intentos fallidos desde una misma dirección IP. Establecer alertas para estos eventos.

Referencias

[1] https://owasp.org/Top10/es/A01_2021-Broken_Access_Control/

[2] <https://portswigger.net/web-security/access-control>

[3] <https://sucuri.net/guides/what-is-broken-access-control/>

Se refiere al uso de bibliotecas, frameworks, software de terceros o cualquier tipo de componente que contiene vulnerabilidades de seguridad identificadas públicamente. Estas fallas suelen estar documentadas en bases de datos de seguridad como el CVE (Common Vulnerabilities and Exposures) y representan un riesgo significativo si no se gestionan adecuadamente.

Cuando los desarrolladores o administradores de sistemas integran estos componentes sin asegurarse de que están actualizados o corregidos, exponen su sistema a posibles ataques, ya que los atacantes pueden aprovecharse de estas vulnerabilidades conocidas para comprometer el sistema.

Las causas comunes de este tipo de vulnerabilidad incluyen:

- Uso de versiones antiguas de software que ya no se mantienen.
- Falta de gestión adecuada de dependencias y actualizaciones.
- Falta de monitoreo de bases de datos de vulnerabilidades conocidas.

Funcionalidad

Tras las pruebas realizadas, se identificó que existen componentes desactualizados con CVE asociados.

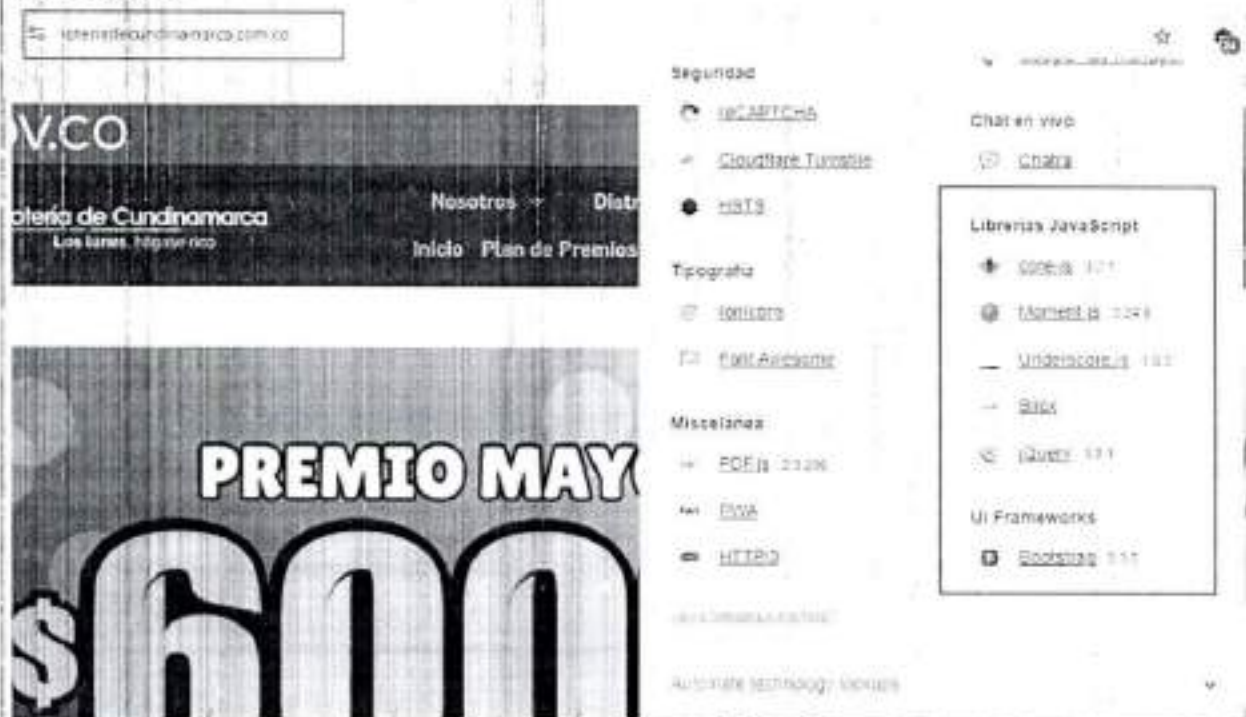
Elemento afectado		Categoría	Puntaje
https://www.loteriadecundinamarca.com.co		Base Score	3.8
		Temporal Score	3.2
		Environmental Score	4.0
Complejidad de Explotación	Alta	Calificación	4.0
OWASP Web (2021)	A6:2021 - Uso de componentes vulnerables o no actualizados		

CVSS 3.1:

AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:U/CR:M/IR:L/AR:L/MAV:N/MAC:L/MPR:
L/MUI:N/MS:U/MC:L/MI:L/MA:N

Evidencia

Tras la ejecución de las pruebas, se identificó que el sitio utiliza componentes con vulnerabilidades conocidas debido a que emplea versiones desactualizadas de dichos componentes.



Versión de componentes con vulnerabilidades conocidas.

A partir de este hallazgo, se elaboró una tabla que detalla los CVE asociados a los componentes vulnerables identificados:

Componente Vulnerable	CVE Asociado
Moments.js v2.24.0	CVE-2022-24785
	CVE-2022-31129
	CVE-2017-18214
jQuery v3.3.1	CVE-2020-11023
	CVE-2020-11022
	CVE-2019-11358
Bootstrap v3.3.7	CVE-2016-10735
	CVE-2018-14040
	CVE-2018-20677
	CVE-2022-26624

Es importante destacar que no fue posible explotar ninguno de los CVEs identificados, ya que requieren privilegios específicos en el sistema o son vulnerabilidades de alcance interno.

Recomendaciones

- Asegurarse de que todos los componentes, bibliotecas y dependencias estén actualizados a las versiones más recientes que hayan corregido las vulnerabilidades. Esto incluye core-js 3.39.0, jQuery 3.6.0 y Bootstrap 5.x, que abordan diversos problemas de seguridad.
- Si es posible, eliminar bibliotecas antiguas que ya no se actualizan ni mantienen. En su lugar, optar por soluciones modernas que no dependan de componentes con vulnerabilidades conocidas.
- Es importante aplicar parches de seguridad tan pronto como se publiquen. Así como realizar pruebas de intrusión recurrentemente.

Referencias

[1] [https://owasp.org/www-project-top-ten/2017/A9_2017-](https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities)

Using_Components_with_Known_Vulnerabilities

[2] <https://keepcoding.io/blog/uso-de-componentes-vulnerabilidades-conocidas/>

Esto ocurre cuando un portal de administración es accesible a través del acceso público, es decir, mediante un formulario de login. Esto permite que los atacantes intenten autenticar sus credenciales y accedan a interfaces administrativas, como paneles de control, configuraciones de seguridad y gestión de usuarios.

Aunque el portal de administración puede estar protegido mediante autenticación, el hecho de que esté expuesto a través de un portal de login público incrementa el riesgo de ataques como fuerza bruta o phishing, ya que el atacante solo necesita conocer la URL del portal para intentar vulnerarlo.

Además, si el portal de login no está adecuadamente asegurado (por ejemplo, mediante protección contra ataques de repetición, CAPTCHA o autenticación multifactor), puede ser fácilmente blanco de ataques.

Funcionalidad

Tras la ejecución de las pruebas, se identificaron varios portales de acceso a paneles administrativos, los cuales permanecen expuestos y accesibles de manera pública.

Elemento afectado	Categoría	Puntaje
https://loteriadecundinamarca.com.co:2083	Base Score	3.1
https://loteriadecundinamarca.com.co:2087	Temporal Score	2.8
https://loteriadecundinamarca.com.co:2096	Environmental Score	2.2

Complejidad de Explotación	Alta	Calificación	2.2
OWASP Web (2021)	A05:2021 – Mala Configuración de Seguridad		

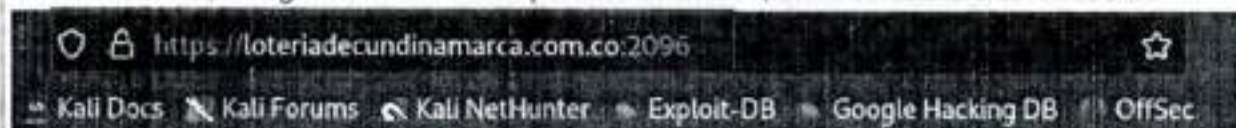
CVSS 3.1:

AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C/CR:L/IR:X/AR:X/MAV:N/MAC:H/MPR:L/MUI:N/MS:U/MC:L/MI:N/MA:N

Evidencia

Durante las pruebas realizadas, se identificaron múltiples portales de acceso administrativo como cPanel, los cuales permanecen accesibles de manera pública sin ningún tipo de restricción. Esto se debe a que dichos portales están expuestos en endpoints predeterminados, como el puerto 2083, 2096, entre otros, los cuales son bien conocidos debido a que corresponden a puertos por defecto utilizados por cPanel.

Como resultado, se logró identificar varios portales de acceso, como se detalla a continuación:



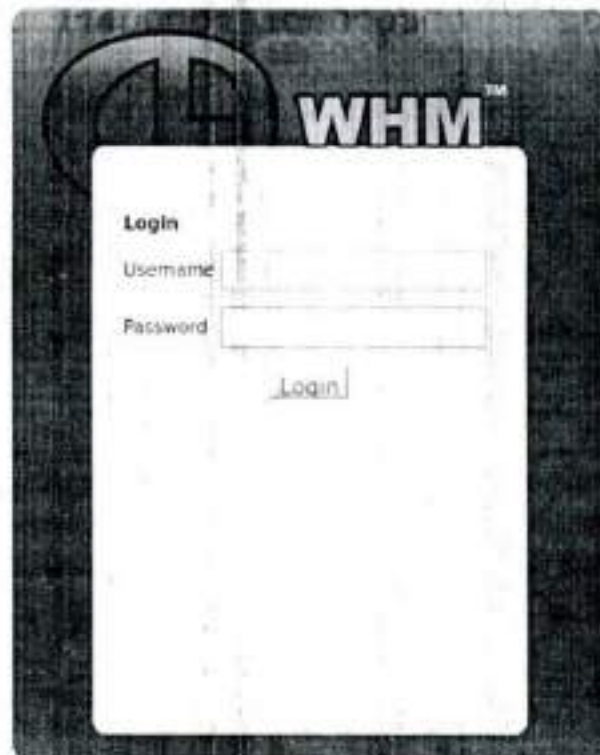
© cPanel, L.L.C. 2019

Portal de acceso Webmail.



© cPanel, L.L.C. 2019

Portal de acceso cPanel.



Portal de acceso WHM.

Tener expuestos estos portales en puertos por defecto representa un grave riesgo, ya que un atacante podría localizarlos fácilmente y, mediante técnicas como escaneo de puertos o ataques de fuerza bruta, intentar obtener acceso no autorizado.

La exposición de estos portales sin las debidas restricciones de seguridad facilita que los atacantes puedan explotar vulnerabilidades conocidas en cPanel o en otros servicios, lo que podría resultar en la alteración de configuraciones críticas, el robo de datos sensibles o incluso el control total del servidor.

Recomendaciones

- Modificar los puertos predeterminados utilizados por cPanel para dificultar su localización por parte de un atacante. Utilizar puertos no estándar reduce la probabilidad de que un atacante pueda encontrarlos mediante un escaneo de puertos.

- Configurar el servidor para que el acceso a los portales administrativos solo sea permitido desde direcciones IP internas o listas blancas de IPs específicas. Esto limita el acceso a usuarios autorizados y previene el acceso público no deseado.
- Activar la autenticación multifactor (MFA) en todos los portales administrativos para agregar una capa extra de seguridad en el proceso de inicio de sesión.
- Asegurar que el firewall esté configurado para bloquear todos los accesos no autorizados a los puertos de administración. Se debe permitir el acceso solo desde redes internas o IPs específicas, y bloquear todo tráfico externo hacia esos puertos.

Referencias

[1] https://owasp.org/Top10/es/A05_2021-Security_Misconfiguration/

[2] <https://docs.cpanel.net/knowledge-base/general-systems-administration/how-to-configure-your-firewall-for-cpanel-services/>

Se puede encontrar más información sobre las metodologías usadas en:

- OWASP (2022). *MASTG Mobile Application Security Testing Guide*. Recuperado de: <https://github.com/OWASP/owasp-mastg/releases/tag/v1.5.0>
- OWASP (2020). Wiki, *Open Web Application Security Project*. Recuperado de: http://www.owasp.org/index.php/Testing_Checklist
- OWASP (2022). *MASVS Mobile Application Security Verification Standard*. Recuperado de: <https://github.com/OWASP/owasp-masvs/releases/tag/v1.4.2>
- MITRE (2020). *Common Weakness Enumeration. Weaknesses Originally Used by NVD from 2008 to 2019*. Recuperado de: <http://cwe.mitre.org/data/definitions/635.html>
- NIST (2019). *National Vulnerability Database. Vulnerability Metrics*. Recuperado de: <http://nvd.nist.gov/cvss.cfm>

Por otro lado, es posible verificar las recomendaciones específicas que fueron señaladas a lo largo del informe en:

- OWASP TOP 10 (2021). *Broken Access Control*. Recuperado de: https://owasp.org/Top10/es/A01_2021-Broken_Access_Control/

CONFIDENCIAL



- OWASP TOP 10 (2021). *Using Components with Known Vulnerabilities*. Recuperado de: https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities
- PORTSWIGGER (2020). *Access Control*. Recuperado de: <https://portswigger.net/web-security/access-control>

Bogotá D.C., 02 de diciembre de 2024

CERTIFICACIÓN DE CUMPLIMIENTO DEL PAGO DE APORTES AL SISTEMA DE SEGURIDAD SOCIAL INTEGRAL Y PARAFISCALES Y DE CUMPLIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO - SG SST
(Ley 789 de 2002 y Decreto 052 de 2017)

Yo Rosa Yaneth Borda Romero, identificada con cedula de ciudadanía No. 52.433.000, en mi calidad de Revisor Fiscal de la empresa **TECH AND KNOWLEDGE SAS** con NIT: **900.529.191-5** (en adelante "la empresa") manifiesto bajo la gravedad del juramento que la empresa ha cumplido durante los seis (6) meses anteriores a la fecha de entrega de la presente certificación, con los pagos al sistema de seguridad social en salud, pensiones y riesgos profesionales y con los aportes parafiscales correspondientes a todos sus empleados vinculados por contrato de trabajo, por lo que declaro que se encuentra a PAZ Y SALVO con las Empresas Promotoras de Salud -EPS-, Fondos de Pensiones, Administradoras de Riesgos Profesionales - ARP-, Caja de Compensación Familiar, Instituto Colombiano de Bienestar Familiar -ICBF- y Servicio Nacional de Aprendizaje -SENA-.



Rosa Yaneth Borda Romero
Revisor Fiscal
T.P. 100098 T

República de Colombia
Ministerio de Educación Nacional

**JUNTA CENTRAL DE CONTADORES
TARJETA PROFESIONAL
DE CONTADOR PUBLICO**

100098-T

**ROSA YANETH
BORDA ROMERO
C.C. 52433000**

**RESOLUCION INSCRIPCION 26
UNIVERSIDAD LA GRAN COLOMBIA**



PRESIDENTE

LUZ MYRIAM DÍAZ MUÑOZ

109902

FIRMA DEL TITULAR

Esta tarjeta es el único documento que lo acredita como
CONTADOR PUBLICO de acuerdo con lo establecido en
la Ley 43 de 1990.

Agradecemos a quien encuentre esta tarjeta devolverla
al Ministerio de Educación Nacional - Junta Central de
Contadores.



UNIDAD
ADMINISTRATIVA
ESPECIAL

**JUNTA CENTRAL
DE CONTADORES**



Certificado No:

B007R137F70AE075

**LA REPUBLICA DE COLOMBIA
MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
UNIDAD ADMINISTRATIVA ESPECIAL
JUNTA CENTRAL DE CONTADORES**

**CERTIFICA A:
QUIEN INTERESE**

Que el contador público **ROSA YANETH BORDA ROMERO** identificado con CÉDULA DE CIUDADANÍA No 52433000 de BOGOTÁ, D.C. (BOGOTÁ D.C) Y Tarjeta Profesional No 100098-T Si tiene vigente su inscripción en la Junta Central de Contadores y desde los últimos 5 años.

NO REGISTRA ANTECEDENTES DISCIPLINARIOS *****

EL CONTADOR PUBLICO NO HA CUMPLIDO CON LA OBLIGACION DE ACTUALIZAR EL REGISTRO

Dado en BOGOTÁ a los 27 días del mes de Noviembre de 2024 con vigencia de (3) Meses, contados a partir de la fecha de su expedición.


SANDRA MILENA BARRIOS PULIDO
DIRECTOR GENERAL

ESTE CERTIFICADO DIGITAL TIENE PLENA VALIDEZ DE CONFORMIDAD CON LO ESTABLECIDO EN EL ARTICULO 2 DE LA LEY 527 DE 1999, DECRETO UNICO REGLAMENTARIO 1074 DE 2015 Y ARTICULO 6 PARAGRAFO 3 DE LA LEY 962 DEL 2005

Para confirmar los datos y veracidad de este certificado, lo puede consultar en la página web www.jcc.gov.co digitando el número del certificado



DAVIVIENDA

Banco Davivienda S.A.

CERTIFICACION

BOGOTA D.C., DISTRITO CAPITAL, 18/11/2024

Por medio de la presente hacemos constar que nuestro cliente **TECH AND KNOWLEDGE SAS** con NIT **900.529.191-5** posee en el Banco Davivienda:

CUENTA DE AHORROS DAMAS

Número

006301200967

Cordialmente,

BANCO DAVIVIENDA

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 02 Actualización

4. Número de formulario

141120399738



(415) 710 7211 489984 (8020) 000014112039973 8

5. Número de identificación Tributaria (NIT)

6. DV

12. Dirección seccional

14. Buzón electrónico

9 0 0 5 2 9 1 9 1

Trasera en Bogotá

3 2

IDENTIFICACIÓN

34. Tipo de contribuyente

35. Tipo de documento

36. Número de identificación

37. Fecha expedición

Persona jurídica

1

Lugar de expedición

38. País

39. Departamento

40. Ciudad/Municipio

31. Primer apellido

32. Segundo apellido

33. Primer nombre

34. Otros nombres

35. Razón social

TECH AND KNOWLEDGE S.A.S

36. Nombre comercial

37. Tipo

T.A.K

UBICACIÓN

38. País

COLOMBIA

1 6 9

39. Departamento

Bogotá D.C.

1 1

40. Ciudad/Municipio

Bogotá D.C.

0 0 1

41. Dirección principal

AV CL 127 70 G 88 OF 315

42. Correo electrónico

directorfinanciero@takcolombia.com

43. Código postal

1 1 0 1 1 1

44. Teléfono 1

6 0 1 7 7 0 4 8 6 5

45. Teléfono 2

3 0 1 3 1 7 1 2 6 4

CLASIFICACIÓN

Actividad económica

Ocupación

Actividad principal

Actividad secundaria

Otras actividades

46. Código

47. Fecha inicio actividad

48. Código

49. Fecha inicio actividad

50. Código

51. Código

52. Número establecimiento

6 2 0 1

2 0 1 2 0 5 3 1

6 2 0 2

2 0 1 2 0 5 3 1

6 2 0 9

6 3 1 1

Responsabilidades, Calidades y Atributos

53. Código

5 7 1 4 4 2 4 8 6 2 5 5

05- Impo. renta y compl. régimen ordinario

07- Retención en la fuente a título de renta

14- Informante de expropiación

42- Obligado a llevar contabilidad

48- Impuesto sobre las ventas - IVA

52 - Facturador electrónico

55 - Informante de Beneficiarios Fijos

Usuarios aduaneros

Exportadores

54. Código

1 2 3 4 5 6 7 8 9 10

11 12 13 14 15 16 17 18 19 20

55. Forma

56. Tipo

Servicio

1

2

3

57. Modo

58. CPC

IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación.

Para uso exclusivo de la DIAN

59. Anexos

SI

NO

X

60. No. de Folios

0

61. Fecha

2024-08-29 11:29:04

La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso. Penúltimo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y aceptó la política de tratamiento de datos ley 1581 de 2012.

Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice

Firma autorizada:

964. Nombre

GARZON OCHOA CARLOS ALBERTO

965. Cargo

Representante legal Certificado

Espacio reservado para la DIAN

4. Número de formulario

141120399738



[415]7707212409984[0020]0000141120399738

5. Número de Identificación Tributaria (NIT)

8. DV

12. Dirección seccional

14. Ruzón electrónico

9 0 0 5 2 9 1 9 1 5

Instituto de Registro

3 2

Características y formas de las organizaciones

62. Naturaleza

2

63. Formas asociativas

1 2

65. Fondos

66. Cooperativas

68. Sin personería jurídica

69. Otras organizaciones no clasificadas

54. Entidades o institutos de derecho público de orden nacional, departamental, municipal y distritales
67. Sociedades y organismos extranjeros
70. Beneficio

1

Constitución, Registro y Última Reforma

Composición del Capital

Documento

1. Constitución

2. Reforma

71. Clave

0 4

72. Número

0 1

73. Fecha

2 0 1 2 0 5 3 1

2 0 2 1 1 2 0 7

74. Número de registro

0 3

0 3

75. Entidad de registro

2 0 1 2 0 6 0 6

2 0 2 1 1 2 2 9

76. Fecha de registro

0 2 2 2 2 1 6 5

0 2 2 2 2 1 6 5

77. No. Matricula mercantil

1 1

1 1

78. Departamento

4

4

79. Ciudad/Municipio

82. Nacional

1 0 0 %

83. Nacional público

0 0 %

84. Nacional privado

1 0 0 0 %

85. Extranjero

0 %

86. Extranjero público

0 0 %

87. Extranjero privado

0 0 %

Entidad de vigilancia y control

88. Entidad de vigilancia y control

Superintendencia de Sociedades

5

Estado y Beneficio

Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV
1	8 0	2 0 2 3 1 1 0 7		
2				
3				
4				
5				

Vinculación económica

93. Vinculación económica	94. Nombre del grupo económico y/o empresarial	95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	96. DV
97. Nombre o razón social de la matriz o controlante			
170. Número de identificación tributaria otorgado en el exterior	171. País	172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP			

Espacio reservado para la DIAN

4. Número de formulario

141120399738



(415)710712469964(8020) 000014112039973 8

5. Número de identificación Tributaria (NIT)

6. DV

12. Dirección sectorial
Provincia de Bogotá

14. Buzón electrónico

9 0 0 5 2 9 1 9 1

5

3 2

Representación

98. Representación	99. Fecha inicio ejercicio representación		
REPRS LEGAL PRIN	1 8 2 0 2 1 1 2 0 7		
100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cedula de Ciudadanía	1 3 8 0 0 5 9 9 4 2		
104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
GARZON	OCHOA	CARLOS	ALBERTO
108. Número de identificación Tributaria (NIT)	109. DV	110. Razón social representante legal	
98. Representación	99. Fecha inicio ejercicio representación		
100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
108. Número de identificación Tributaria (NIT)	109. DV	110. Razón social representante legal	
98. Representación	99. Fecha inicio ejercicio representación		
100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
108. Número de identificación Tributaria (NIT)	109. DV	110. Razón social representante legal	
98. Representación	99. Fecha inicio ejercicio representación		
100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
108. Número de identificación Tributaria (NIT)	109. DV	110. Razón social representante legal	
98. Representación	99. Fecha inicio ejercicio representación		
100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
108. Número de identificación Tributaria (NIT)	109. DV	110. Razón social representante legal	

Espacio reservado para la DIAN

4. Número de formulario

141120399738



5. Número de identificación Tributaria (NIT)

6. DV

12. Dirección seccional
Impuestos de Renta

14. Buzón electrónico

9 0 0 5 2 9 1 9 1 5

3 2

Revisor Fiscal y Contador

Revisor fiscal principal

124. Tipo de documento

125. Número de identificación

126. DV 127. Número de tarjeta profesional

Cédula de Ciudadanía 1 3

5 2 4 3 3 0 0 0

1 0 0 0 9 8 7

128. Primer apellido

129. Segundo apellido

130. Primer nombre

131. Otros nombres

BORDA

ROMERO

ROSA

YANETH

132. Número de identificación Tributaria (NIT)

133. DV

134. Sociedad o firma designada

135. Fecha de nombramiento

2 0 1 9 0 1 0 1

Revisor fiscal suplente

136. Tipo de documento

137. Número de identificación

138. DV 139. Número de tarjeta profesional

140. Primer apellido

141. Segundo apellido

142. Primer nombre

143. Otros nombres

144. Número de identificación Tributaria (NIT)

145. DV

146. Sociedad o firma designada

147. Fecha de nombramiento

Contador

148. Tipo de documento

149. Número de identificación

150. DV 151. Número de tarjeta profesional

Cédula de Ciudadanía 1 3

5 2 5 4 5 1 6 2

2 2 3 6 7 0

152. Primer apellido

153. Segundo apellido

154. Primer nombre

155. Otros nombres

BARRIOS

MORALES

BEATRIZ

ADRIANA

156. Número de identificación Tributaria (NIT)

157. DV

158. Sociedad o firma designada

159. Fecha de nombramiento

2 0 1 8 0 9 0 4

Ejecución del Contrato

☐ Porcentaje ☐ Recepción de artículos

Plan de Pagos

Id de pago	% de facturación previsto	Número de factura	Fecha prevista de emisión	Fecha de emisión	Fecha de recepción	Valor total previsto	Valor neto de la factura	Valor total de la factura	Valor a pagar	Estado
Pago 001	100	626		20/12/2024 12:16 PM PDT - 8 horas	23/12/2024 12:00 PM PDT - 8 horas	0 COP	19.816.909 COP	22.845.700 COP	22.845.700 COP	Aprobado
Pago 002		627		20/12/2024 12:34 PM PDT - 8 horas			19.816.909 COP	22.845.700 COP	22.845.700 COP	Enviado

Proveedor

Balance de pagos y Balance de entregas

		% del valor del contrato	% del valor amortizado
Valor total contrato:	45.291.400.00 COP	-	-
Valor anticipo:	0.00 COP	0%	-
Valor de las entregas:	0.00 COP	0%	-
Valor facturado:	22.845.700.00 COP	50%	-
Valor facturado pendiente de pago:	22.845.700.00 COP	50%	-
Valor pagado:	0.00 COP	0%	-
Valor amortizado del anticipo:	0.00 COP	0%	0%
Valor pendiente de amortizar:	0.00 COP	0%	0%
Valor pendiente de ejecución:	45.291.400.00 COP	100%	-
Valor pendiente de entrega:	45.291.400.00 COP	100%	-

Ver Pago de Proveedores Colombia

Fecha de Impresión 26/12/2024

[Imprimir](#)

[Cerrar](#)

Información de Pago

Cuenta Originadora	0075109330 - CC9330 - \$
Fecha de Pago	24/12/2024
Frecuencia	Una Sola Vez
Estado	Procesado
Número de Transacción	24662035
Código de Motivo de Devolución/Descripción	Procesado

Beneficiarios

Nombre ID	ID del Banco Nombre del Banco	Número de Cuenta Tipo de Cuenta	Monto	Número de Factura	Estado Prenotificación Vencida	Adenda	Estado de Beneficiario	Código de Motivo de Devolución/ Descripción
TECH AND KNOWLEDGE SAS 9005291915	051 BANCO DAVIVIENDA	006301300967 Cuenta de Ahorros	\$17.694.215,00	1329	Activo	DESARROLLO DE PRUEBAS TECNICAS Y TACTICAS INNOVACION TECNOLÓGICA	Procesado	Transaccion Procesada Exitosamente
Total de Beneficiarios		1			Monto Total		\$17.694.215,00	
Total de Beneficiarios Procesados		1			Total de Beneficiarios Devueltos		0	
Total de Beneficiarios Pendientes		0						

Cancelar