FECHA DE EMISIÓN DEL INFORME	**Día:**	02	**Mes:**	09	**Año:**	2025

PROCESO / PROCEDIMIENTO AUDITADO:	Proceso de Apoyo – Gestión de las TIC. OFICINA DE PLANEACIÓN Y SISTEMAS
LÍDER PROCESO AUDITADO:	DR, JORGE CASTRO SALCEDO – JEFE OFICINA DE PLANEACIÓN Y SISTEMAS
Objetivo de la Auditoría:	Conocer el nivel de exposición a un ataque externo e Identificar posibles vulnerabilidades de los sistemas de seguridad informática y de la información.
Alcance de la Auditoría:	La presente auditoría se enfocó al plan de mejoramiento de los hallazgos, suscrito para la auditoría realizada a las "TECNOLOGIA DE LA INFORMACIÓN -SEGURIDAD DE LA INFORMACIÓN "en la vigencia 2024 y sus evidencias.
Criterios de la Auditoría:	Ley 23 de 1982, Sobre derechos de autor, Ley 87 de 1993, Decreto 1078 de 2015, Guías de Seguridad de la Información No.1 al No.21 – Mintic, Norma ISO/IEC 27001, Ley 599 de 2000, Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. ISO Guía 73:2002, Anexo 4 - Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	11	**Mes**	06	**Año**	2025	**Desde**	11/06/25 D / M / A	**Hasta**	10/09/25 D / M / A	Día	10	Mes	09	Año	2025

Jefe oficina de Control Interno	**Auditor Líder**
Dr. JEHYMMYS TATIANA SANCHEZ CALA	ALVARO E. OSPINA R. Profesional Universitario Ingeniero de sistemas Abogado

EJECUCIÓN DE LA AUDITORIA

Se realizó el seguimiento a las actividades suscritas en el plan de mejoramiento correspondiente a la vigencia 2024.

EXPLORACIÓN DE VULNERABILIDADES

El área auditada da respuesta a las observaciones en dos ítems, uno corresponde a las vulnerabilidades encontradas en la página web corporativa y el otro a las vulnerabilidades encontradas en el Sistema de Gestión Documental (SGDA).

VULNERABILIDADES DETECTADAS EN LA PÁGINA WEB CORPORATIVA

NIVEL DE RIESGO CRITICO

1. Detección del fin de la vida útil (EOL) del sistema operativo (OS)

GRAVEDAD	ESTADO	ESCANEAR	CALIDAD DE DETECCIÓN	CVSS	PUERTO
Crítico	Abierto	OpenVAS	80% →	10.0 →	general/tcp

Descripción

El sistema operativo (OS) del host remoto ha llegado al final de su vida útil (EOL) y ya no debería utilizarse. Una versión EOL de un SO no recibe actualizaciones de seguridad del proveedor. Un atacante podría aprovechar vulnerabilidades de seguridad no corregidas para comprometer la seguridad de este host.

Recomendación

Actualice el sistema operativo en el host remoto a una versión que aún sea compatible y reciba actualizaciones de seguridad del proveedor.

Respuesta

El sistema operativo sobre el cual está soportada la nueva página es Ubuntu 24.04.3, versión más reciente del OS (sistema operativo), se adjunta captura de pantalla en que se evidencia la versión del OS del Host Remoto.

```
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-78-generic x86_64)
```

Respuesta de la OCCI

Una vez revisada la evidencia se pudo observar que la plataforma actual cumple con los requisitos de actualización en seguridad. Por lo anterior se da por subsanada la misma.

NIVEL DE RIESGO ALTO

(1) SSL/TLS: Informar sobre conjuntos de cifrado vulnerables para HTTPS

GRAVEDAD	ESTADO	ESCANEAR	CALIDAD DE DETECCIÓN	CVSS	PUERTO
Alto	Abierto	OpenVAS	98% →	7.5 →	443/tcp

Descripción
Esta rutina informa sobre todos los conjuntos de cifrados SSL/TLS aceptados por un servicio en el que los vectores de ataque solo existen en servicios HTTPS. Estas reglas se aplican para la evaluación de los conjuntos de cifrados vulnerables: - Cifrado de bloque de 64 bits 3DES vulnerable al ataque SWEET32 (CVE-2016-2183) = *"vulnerabilidad en OpenSSL que permite a un atacante remoto obtener información confidencial de un servidor SSL/TLS y un cliente"*.

Recomendación
La configuración de este servicio debe modificarse para que ya no acepte los conjuntos de cifrados enumerados. Consulte las referencias para obtener más recursos que lo ayuden con esta tarea.

Respuesta
La configuración de la nueva página web de la entidad no acepta los conjuntos de cifrado SSLv2 y SSlv3, así como TLS 1.0 y 1.1. Se adjunta captura de pantalla del informe de pruebas de ciberseguridad realizado por el proveedor del servicio web.

Resumen del Análisis Técnico

Protocolos habilitados:

SSLv2: Deshabilitado

SSLv3: Deshabilitado

TLS 1.0: Deshabilitado

TLS 1.1: Deshabilitado

TLS 1.2: Habilitado

Calle 17 A No 69 – 62 | info@skaphe.com www.skaphe.com | PBX: 601- 927 2937

INFORME MENSUAL DE EJECUCIÓN	skaphe	
	F-TI-021 V.0	octubre/2022

TLS 1.3: Habilitado

Esto es ideal. TLS 1.2 y TLS 1.3 son seguros y recomendados actualmente. Las versiones antiguas están correctamente deshabilitadas.

A02: Cryptographic Failures

Herramienta usada: sslscan

Dominio auditado: hcrpruebas.camara.gov.co

```
└─$ sslscan hcrpruebas.camara.gov.co
Version: 2.1.5
OpenSSL 3.5.0 8 Apr 2025

Connected to 190.71.151.20

Testing SSL server hcrpruebas.camara.gov.co on port 443 using SNI name hcrpruebas.camara.gov.co

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed
```

Respuesta de la OCCI

Una vez revisada la evidencia se observó que la plataforma actual no acepta conjuntos de cifrados enumerados cumpliendo con el criterio de seguridad requerido. Por lo anterior se da por subsanada la observación.

2. Inyección SQL

(URI: https://www.camara.gov.co/core/assets/vendor/modernizr/modernizr.min.js?v=3.3.1+AND+1%3D1+--+)

GRAVEDAD	ESTADO	ESCANEAR
Alto	Abierto	OWASP ZAP Activo

Descripción

Alta posibilidad de una inyección SQL: Tipo de ciberataque encubierto en donde se inserta un código en un sitio web para vulnerar la seguridad y acceder a datos protegidos, pudiendo controlar la base de datos del sitio web y secuestrar la información de los usuarios. consecuencias. La vulnerabilidad se detectó al recuperar con éxito más datos de los que se devolvieron originalmente, mediante la manipulación del parámetro.

Recomendaciones

- ✓ No confíe en la entrada del lado del cliente, incluso si existe una validación del lado del cliente.
- ✓ En general, verifique el tipo de todos los datos en el lado del servidor.
- ✓ Si la aplicación utiliza JDBC, utilice PreparedStatement o CallableStatement, con parámetros pasados por '?'
- ✓ Si la aplicación utiliza ASP, utilice objetos de comando ADO con una verificación de tipo fuerte y consultas parametrizadas.
- ✓ Si se pueden utilizar procedimientos almacenados de base de datos, utilícelos.
- ✓ No concatene cadenas en consultas en el procedimiento almacenado, ni utilice 'exec', 'exec emergency' o una funcionalidad equivalente
- ✓ No crear consultas SQL dinámicas utilizando una concatenación de cadenas simple.
- ✓ Evitar todos los datos recibidos del cliente.
- ✓ Aplicar una 'lista de permitidos' de caracteres permitidos, o una 'lista de denegados' de caracteres no permitidos en la entrada del usuario.
- ✓ Aplicar el principio del mínimo privilegio utilizando el usuario de base de datos con menos privilegios posible.
- ✓ En particular, evite utilizar los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto. Otorgar el acceso mínimo a la base de datos que sea necesario para la aplicación.

Respuesta

El motor de base de datos de la nueva página web tiene la resiliencia suficiente, en las pruebas realizadas por el proveedor no se encuentra una vulnerabilidad de inyección SQL. Se adjunta captura de pantalla del informe entregado por el proveedor del servicio web.

A02: Cryptographic Failures

Herramienta usada: sslscan

Dominio auditado: hcrpruebas.camara.gov.co

```
└─$ sslscan hcrpruebas.camara.gov.co
Version: 2.1.5
OpenSSL 3.5.0 8 Apr 2025

Connected to 190.71.151.20

Testing SSL server hcrpruebas.camara.gov.co on port 443 using SNI name hcrpruebas.camara.gov.co

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed
```

```
able
It looks like the back-end DBMS is 'IBM DB2'. Do you want to skip test payloads specific for other DBM
Ses? [Y/n] Y
[22:50:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[22:50:25] [INFO] automatically extending ranges for UNION query injection technique tests as there is
 at least one other (potential) technique found
[22:50:28] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[22:50:32] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[22:51:03] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[22:51:33] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[22:52:02] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[22:52:31] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[22:53:01] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[22:53:32] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[22:54:01] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[22:54:30] [INFO] checking if the injection point on Referer parameter 'Referer' is a false positive
[22:54:31] [WARNING] false positive or unexploitable injection point detected
[22:54:31] [WARNING] parameter 'Referer' does not seem to be injectable
[22:54:31] [INFO] testing if parameter 'Host' is dynamic
[22:54:33] [WARNING] parameter 'Host' does not appear to be dynamic
[22:54:34] [WARNING] heuristic (basic) test shows that parameter 'Host' might not be injectable
[22:54:37] [INFO] testing for SQL injection on parameter 'Host'
[22:54:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:58:37] [WARNING] reflective value(s) found and filtering out
[22:58:58] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[23:01:14] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[23:05:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[23:08:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[23:09:40] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[23:10:31] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[23:10:58] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[23:11:47] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:11:54] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[23:11:59] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[23:12:04] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[23:12:08] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[23:12:13] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[23:17:23] [INFO] testing 'Generic inline queries'
[23:17:24] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:19:25] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[23:21:37] [WARNING] parameter 'Host' does not seem to be injectable
[23:21:37] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there
is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper'
(e.g. '--tamper=space2comment') and/or switch '--random-agent'
[23:21:37] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 5280 times

[*] ending @ 23:21:37 /2025-07-06/
```

Resultado General de la Prueba A03: Inyección SQL

Evaluación

Parámetros evaluados:

id: no vulnerable

User-Agent: no vulnerable

Respuesta de la OCCI

Una vez revisada la evidencia se pudo observar que la plataforma no es vulnerable ante una inyección SQL. Por lo anterior se da por subsanada la misma.

4. CSP: Directiva de comodines (URI: https://intranet.camara.gov.co/)

GRAVEDAD	ESTADO	ESCANEAR	LOS 10 MEJORES DE OWASP
Medio	Abierto	ZAP de OWASP	Mala configuración de seguridad →

Descripción

La Política de Seguridad de Contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos (entre otros) ataques de secuencias de comandos entre sitios (XSS) y de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración de sitios o la distribución de malware. La CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deben poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos integrables como subprogramas Java, ActiveX, archivos de audio y video.

Recomendación

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. estén configurados correctamente para establecer el encabezado Content-Security-Policy. Verifique que la información proporcionada no sea confidencial.

Respuesta

El servidor web de la nueva página web de la entidad cuenta con la configuración correcta, de manera tal que se establecen las cabeceras HTTP necesarias para garantizar la declaración de fuentes de contenido aprobadas. Se adjunta captura de pantalla del informe de ciberseguridad realizado por el proveedor del servicio web.

Análisis de Hallazgos:

1. Encabezados HTTP

Se detectaron correctamente varias cabeceras de seguridad, lo cual es **positivo**:

- Referrer-Policy: strict-origin-when-cross-origin ✔
- Content-Security-Policy (CSP) definido ✔
- X-Frame-Options: SAMEORIGIN ✔
- X-Content-Type-Options: nosniff ✔
- Permissions-Policy ✔

A06: Vulnerable and Outdated Components

```
└─$ wpscan --url https://hcrpruebas.camara.gov.co --disable-tls-checks --enumerate vt,ap,cb --force
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://hcrpruebas.camara.gov.co/ [190.71.151.20]
[+] Started: Sun Jul  6 17:16:06 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - server: openresty
 |  - referrer-policy: strict-origin-when-cross-origin
 |  - content-security-policy: default-src 'self' https://camara.gov.co https://*.camara.gov.co; scrip
t-src 'self' 'unsafe-inline' 'unsafe-eval' blob: https://camara.gov.co https://*.camara.gov.co https:/
/*.googletagmanager.com https://*.google-analytics.com https://*.google.com https://*.gstatic.com http
s://translate.googleapis.com https://translate-pa.googleapis.com https://cdn.userway.org https://*.use
rway.org https://userway.org https://unpkg.com https://cdnjs.cloudflare.com https://code.jquery.com ht
tps://maps.googleapis.com https://platform.twitter.com https://connect.facebook.net https://apis.googl
e.com https://www.gstatic.com https://*.youtube.com https://www.youtube.com https://www.youtube-nocook
ie.com; style-src 'self' 'unsafe-inline' https://camara.gov.co https://*.camara.gov.co https://fonts.g
oogleapis.com https://cdn.userway.org https://*.userway.org https://userway.org https://unpkg.com http
s://cdnjs.cloudflare.com https://www.gstatic.com; font-src 'self' data: https://camara.gov.co https://
*.camara.gov.co https://fonts.gstatic.com https://cdn.userway.org https://*.userway.org https://userwa
y.org https://cdnjs.cloudflare.com https://demotiles.maplibre.org; img-src 'self' data: blob: https://
camara.gov.co https://*.camara.gov.co https://*.google-analytics.com https://secure.gravatar.com https
://s.w.org https://*.wpmet.com https://premiumaddons.com https://cdn.userway.org https://*.userway.org
 https://userway.org https://cdnjs.cloudflare.com https://pbs.twimg.com https://abs.twimg.com https://
syndication.twitter.com https://ssl.gstatic.com https://www.gstatic.com https://fonts.gstatic.com http
s://www.google.com https://translate.google.com https://translate.googleapis.com https://i.ytimg.com h
ttps://s.ytimg.com; connect-src 'self' https://camara.gov.co https://*.camara.gov.co https://ragapi.ca
mara.gov.co https://*.google-analytics.com https://api.userway.org https://*.userway.org https://userw
ay.org https://maps.googleapis.com https://syndication.twitter.com https://cdn.ampproject.org https://
cdnjs.cloudflare.com https://translate.googleapis.com https://translate-pa.googleapis.com https://demo
tiles.maplibre.org https://www.google.com https://www.gstatic.com ws: wss:; frame-src 'self' https://c
amara.gov.co https://*.camara.gov.co https://*.googletagmanager.com https://*.google.com https://www.r
ecaptcha.net https://*.gstatic.com https://platform.twitter.com https://www.facebook.com https://www.y
outube.com https://*.youtube.com https://cdn.userway.org https://*.userway.org https://userway.org htt
```

```
ps://cdnjs.cloudflare.com; worker-src 'self' blob:; object-src 'self' data: https://camara.gov.co http
s://*.camara.gov.co; media-src 'self' https://camara.gov.co https://*.camara.gov.co https://*.youtube.
com https://www.youtube.com; form-action 'self' https://camara.gov.co https://*.camara.gov.co; manifes
t-src 'self' https://camara.gov.co https://*.camara.gov.co; base-uri 'self' https://camara.gov.co http
s://*.camara.gov.co; upgrade-insecure-requests
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] WordPress readme found: https://hcrpruebas.camara.gov.co/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Debug Log found: https://hcrpruebas.camara.gov.co/wp-content/debug.log
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | Reference: https://codex.wordpress.org/Debugging_in_WordPress

[+] This site has 'Must Use Plugins': https://hcrpruebas.camara.gov.co/wp-content/mu-plugins/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 80%
 | Reference: http://codex.wordpress.org/Must_Use_Plugins

Fingerprinting the version - Time: 00:00:11 <====================> (702 / 702) 100.00% Time: 00:00:11
[i] The WordPress version could not be detected.

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
[!] No WPScan API Token given, as a result vulnerability data has not been output.3.22%  ETA: 00:00:26
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Jul  6 17:16:22 2025
[+] Requests Done: 1365
[+] Cached Requests: 6
[+] Data Sent: 330.728 KB
[+] Data Received: 31.088 MB
[+] Memory used: 310.27 MB
[+] Elapsed time: 00:00:15

Scan Aborted: The number of themes detected reached the threshold of 20 which might indicate False Pos
itive. It would be recommended to use the --exclude-content-based option to ignore the bad responses.
```

Respuesta de la OCCI
Una vez revisada la evidencia se pudo observar que la plataforma permite la configuración correcta para establecer el encabezado "Content-Security-Policy". Por lo anterior se da por subsanada la misma.

5. Biblioteca JS vulnerable
(URI:
https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/data-min.js?v=1.12.1
https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js

https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Scripts/bootstrap.min.js

Biblioteca JS Vulnerable

GRAVEDAD	ESTADO	ESCANEAR	LOS 10 MEJORES DE OWASP
Medio	Abierto	ZAP de OWASP	Uso de componentes con vulnerabilidades conocidas →

Descripción
Biblioteca de Javascript vulnerable: Las bibliotecas identificadas jquery-ui, versión 1.12.1, jQuery versión 2.1.1, bootstrap versión 3.3.7 son vulnerables.

Recomendación
Actualice a la última versión.

Respuesta
Las bibliotecas de JavaScript se encuentran actualizadas y la librería Bootstrap fue reemplazada por una librería compatible con el nuevo ecosistema de la página web. Se adjuntan capturas de pantalla donde se evidencia la versión actual de cada una de las librerías mencionadas.

JQuery actualizado:

```
112 <script src="https://intra.camara.gov.co/wp-includes/js/jquery/jquery.js?ver=3.7.1" id="jquery-core-js"></script>
113 <script src="https://intra.camara.gov.co/wp-includes/js/jquery/jquery-migrate.js?ver=3.4.1" id="jquery-migrate-js"></script>
114 <script id="jquery-js-after">
```

JQuery-Ui actualizado:

```
2664 <script src="https://intra.camara.gov.co/wp-includes/js/jquery/ui/core.js?ver=1.13.3" id="jquery-ui-core-js"></script>
```

Bootstrap reemplazado:

```
14 <link rel='stylesheet' id='astra-theme-css-css' href='https://intra.camara.gov.co/wp-content/themes/astra/assets/css/minified/main.min.css?ver=4.11.9' media='all' />
15 <style id='astra-theme-css-inline-css'>
```

Respuesta de la OCCI
Una vez revisada la evidencia se pudo observar que los componentes susceptibles de ser vulnerables fueron remplazados y actualizados por librerías con nuevos protocolos. Por lo anterior se da por subsanada la misma.

6. SSL/TLS: detección de protocolos TLSv1.0 y TLSv1.1 obsoletos

GRAVEDAD	ESTADO	ESCANEAR	CALIDAD DE DETECCIÓN	CVSS	PUERTO
Medio	Abierto	OpenVAS	98% →	4.3 →	443/tcp

Descripción
Fue posible detectar el uso del protocolo TLSv1.0 y/o TLSv1.1 en desuso en este sistema. Los protocolos TLSv1.0 y TLSv1.1 contienen fallas criptográficas conocidas como: - CVE-2011-3389: Exploit de navegador contra SSL/TLS (BEAST) - CVE-2015-0204: Ataque de factorización en claves RSA-EXPORT con relleno de Oracle en cifrado heredado degradado (FREAK) Un atacante podría usar las fallas criptográficas conocidas para espiar la conexión

entre los clientes y el servicio para obtener acceso a datos confidenciales transferidos dentro de la conexión segura. Además, las vulnerabilidades recién descubiertas en estos protocolos ya no recibirán actualizaciones.

Recomendación

Se recomienda deshabilitar los protocolos TLSv1.0 y/o TLSv1.1 obsoletos en favor de los protocolos TLSv1.2+. Consulte las referencias para obtener más información.

Respuesta

La configuración de la nueva página web de la entidad no acepta los conjuntos de cifrado TLS 1.0 y 1.1, la configuración de la nueva página web solo tiene habilitados los protocolos TLS 1.2 y 1.3. Se adjunta captura de pantalla del informe de pruebas de ciberseguridad realizado por el proveedor del servicio web.

A02: Cryptographic Failures

Herramienta usada: sslscan

Dominio auditado: hcrpruebas.camara.gov.co

```
└─$ sslscan hcrpruebas.camara.gov.co
Version: 2.1.5
OpenSSL 3.5.0 8 Apr 2025

Connected to 190.71.151.20

Testing SSL server hcrpruebas.camara.gov.co on port 443 using SNI name hcrpruebas.camara.gov.co

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed
```

Resumen del Análisis Técnico

Protocolos habilitados:

SSLv2: Deshabilitado

SSLv3: Deshabilitado

TLS 1.0: Deshabilitado

TLS 1.1: Deshabilitado

TLS 1.2: Habilitado

TLS 1.3: Habilitado

Esto es ideal. TLS 1.2 y TLS 1.3 son seguros y recomendados actualmente. Las versiones antiguas están correctamente deshabilitadas.

Respuesta de la OCCI
Una vez revisada la evidencia se pudo observar que los protocolos TLSv1.0 y/o TLSv1.1 se encuentran deshabilitados y se encuentran habilitados protocolos actualizados. Por lo anterior se da por subsanada la misma.

7. Ausencia de tokens anti-CSRF (URI: https://intranet.camara.gov.co/)

GRAVEDAD	ESTADO	ESCANEAR	LOS 10 MEJORES DE OWASP
Medio	Abierto	ZAP de OWASP	Control de acceso roto →

Descripción

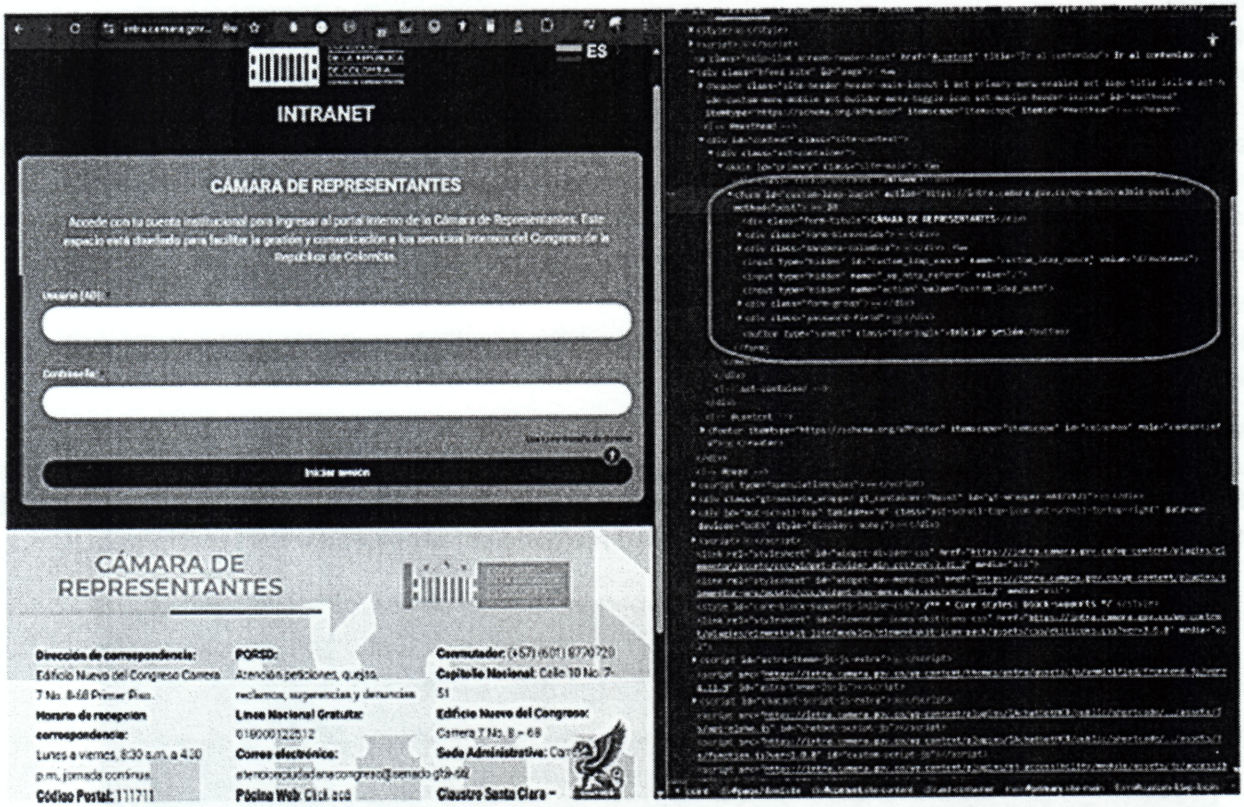
No se encontraron tokens anti-CSRF en un formulario de envío HTML. Una falsificación de solicitud entre sitios es un ataque que implica obligar a una víctima a enviar una solicitud HTTP a un destino objetivo sin su conocimiento o intención para realizar una acción como la víctima. La causa subyacente es la funcionalidad de la aplicación que utiliza acciones predecibles de URL/formulario de forma repetible. La naturaleza del ataque es que CSRF explota la confianza que un sitio web tiene para un usuario. Por el contrario, la secuencia de comandos entre sitios (XSS) explota la confianza que un usuario tiene para un sitio web. Al igual que XSS, los ataques CSRF no son necesariamente entre sitios, pero pueden serlo. La falsificación de solicitud entre sitios también se conoce como CSRF, XSRF, ataque de un clic, conducción de sesión, diputado confundido y surf en el mar. Los ataques CSRF son efectivos en varias situaciones, entre ellas: * La víctima tiene una sesión activa en el sitio de destino. * La víctima está autenticada a través de la autenticación HTTP en el sitio de destino. * La víctima está en la misma red local que el sitio de destino. CSRF se ha utilizado principalmente para ejecutar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero recientemente se han descubierto técnicas para divulgar información obteniendo acceso a la respuesta. El riesgo de divulgación de información aumenta drásticamente cuando el sitio objetivo es vulnerable a XSS, porque XSS se puede utilizar como plataforma para CSRF, lo que permite que el ataque funcione dentro de los límites de la política del mismo origen.

Recomendación

Fase: Arquitectura y diseño Utilice una biblioteca o un marco de trabajo examinados que no permitan que se produzca esta debilidad o que proporcionen construcciones que faciliten su evitación. Por ejemplo, utilice paquetes anti-CSRF como OWASP CSRFGuard. Fase: Implementación Asegúrese de que su aplicación esté libre de problemas de secuencias de comandos entre sitios, ya que la mayoría de las defensas CSRF se pueden eludir mediante secuencias de comandos controladas por el atacante. Fase: Arquitectura y diseño Genere un nonce único para cada formulario, coloque el nonce en el formulario y verifique el nonce al recibir el formulario. Asegúrese de que el nonce no sea predecible (CWE-330). Tenga en cuenta que esto se puede eludir mediante XSS. Identifique operaciones especialmente peligrosas. Cuando el usuario realiza una operación peligrosa, envíe una solicitud de confirmación independiente para asegurarse de que el usuario tenía la intención de realizar esa operación. Tenga en cuenta que esto se puede eludir mediante XSS. Utilice el control de administración de sesiones ESAPI. Este control incluye un componente para CSRF. No utilice el método GET para ninguna solicitud que active un cambio de estado. Fase: Implementación Verifique el encabezado HTTP Referer para ver si la solicitud se originó desde una página esperada. Esto podría interrumpir la funcionalidad legítima, ya que los usuarios o servidores proxy pueden haber deshabilitado el envío del Referer por razones de privacidad.

Respuesta

Se han implementado los controles anti-CSRF. Manteniendo Con nonces verificados en servidor, cookies endurecidas, CSP y refuerzo WAF, el riesgo de CSRF se mantiene mitigado bajo el principio de defensa en profundidad. Se adjunta captura de pantalla del informe de seguridad realizado por el proveedor del servicio.



Tenemos

- **Campo oculto de nonce (custom_ldap_nonce) → es el token anti-CSRF.**
- **Campo _wp_http_referer → ayuda a WordPress a saber desde dónde se envió el formulario.**
- **Acción (custom_ldap_auth) → define la función que procesa la petición en el servidor.**

Respuesta de la OCCI
Se pudo observar que se implementaron los controles anti-CSRF (Cross-Site Request Forgery), como medida de seguridad preventiva al realizar la autenticación, lo que permite evitar que un atacante logre que el usuario realice operaciones no deseadas en la aplicación web. Conforme a lo anterior se da por subsanada la observación.

9. CSP: script-src inseguro en línea (URI: https://intranet.camara.gov.co/)
10. CSP: estilo-fuente-inseguro-en-línea (URI: https://intranet.camara.gov.co/)

GRAVEDAD	ESTADO	ESCANEAR	LOS 10 MEJORES DE OWASP
Medio	Abierto	ZAP de OWASP	Mala configuración de seguridad →

Descripción

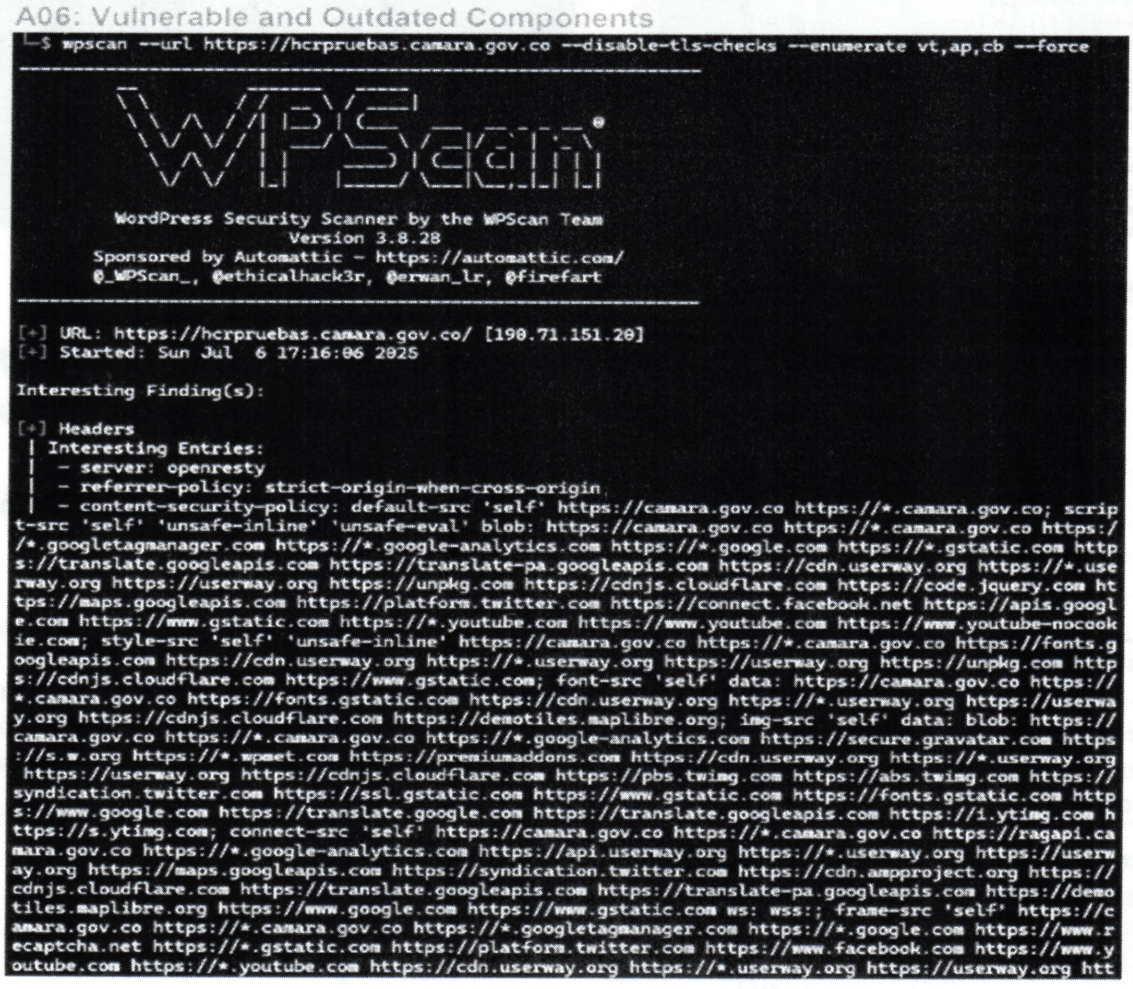
La Política de Seguridad de Contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos los ataques de inyección de datos y de secuencias de comandos entre sitios (XSS). Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración de sitios o la distribución de malware. La CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deben poder cargar en esa página. Los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos integrables como subprogramas Java, ActiveX, archivos de audio y video.

Recomendación

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. estén configurados para establecer el encabezado Content-Security-Policy.

Respuesta a los numerales 9 y 10

El servidor web de la nueva página web de la entidad cuenta con la configuración correcta, de manera tal que se establecen las cabeceras HTTP necesarias para garantizar la declaración de fuentes de contenido aprobadas. Se adjunta captura de pantalla del informe de ciberseguridad realizado por el proveedor del servicio web



```
ps://cdnjs.cloudflare.com; worker-src 'self' blob:; object-src 'self' data: https://camara.gov.co http
s://*.camara.gov.co; media-src 'self' https://camara.gov.co https://*.camara.gov.co https://*.youtube.
com https://www.youtube.com; form-action 'self' https://camara.gov.co https://*.camara.gov.co; manifes
t-src 'self' https://camara.gov.co https://*.camara.gov.co; base-uri 'self' https://camara.gov.co http
s://*.camara.gov.co; upgrade-insecure-requests
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] WordPress readme found: https://hcrpruebas.camara.gov.co/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Debug Log found: https://hcrpruebas.camara.gov.co/wp-content/debug.log
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | Reference: https://codex.wordpress.org/Debugging_in_WordPress

[+] This site has 'Must Use Plugins': https://hcrpruebas.camara.gov.co/wp-content/mu-plugins/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 80%
 | Reference: http://codex.wordpress.org/Must_Use_Plugins

Fingerprinting the version - Time: 00:00:11 <=====================> (702 / 702) 100.00% Time: 00:00:11
[i] The WordPress version could not be detected.

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
[!] No WPScan API Token given, as a result vulnerability data has not been output.3.22%  ETA: 00:00:26
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Jul  6 17:16:22 2025
[+] Requests Done: 1365
[+] Cached Requests: 6
[+] Data Sent: 330.728 KB
[+] Data Received: 31.088 MB
[+] Memory used: 310.27 MB
[+] Elapsed time: 00:00:15

Scan Aborted: The number of themes detected reached the threshold of 20 which might indicate False Pos
itive. It would be recommended to use the --exclude-content-based option to ignore the bad responses.
```

Análisis de Hallazgos:

1. Encabezados HTTP

Se detectaron correctamente varias cabeceras de seguridad, lo cual es **positivo**:

- Referrer-Policy: strict-origin-when-cross-origin ✔
- Content-Security-Policy (CSP) definido ✔
- X-Frame-Options: SAMEORIGIN ✔
- X-Content-Type-Options: nosniff ✔
- Permissions-Policy ✔

Respuesta de la OCCI

Se pudo observar que se estableció en la configuración de las cabeceras la Política de Seguridad del Contenido (CSP), lo que permite controlar los recursos que se pueden cargar para la página, protegiendo la página contra un ataque de scripts entre sitios. Conforme a lo anterior se da por subsanada la observación.

VULNERABILIDADES ENCONTRADAS EN EL ENLACE AL SISTEMA DE GESTIÓN DOCUMENTAL (SGDA)

NIVEL DE RIESGO CRITICO

3. Biblioteca JS vulnerable
(URI: https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Scripts/jquery.validate.js)

GRAVEDAD	ESTADO	ESCANEAR
Alto	Abierto	OWASP ZAP Activo

Descripción
Biblioteca de Javascript vulnerable: La biblioteca identificada jquery -validation, versión 1.17.0 es vulnerable.

Recomendación
La configuración de este servicio debe modificarse para que ya no acepte los conjuntos de cifrados enumerados. Consulte las referencias para obtener más recursos que lo ayuden con esta tarea.

NIVEL DE RIESGO MEDIO

1. Configuración incorrecta entre dominios
(**URI:** https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx)

GRAVEDAD	ESTADO	ESCANEAR	LOS 10 MEJORES DE OWASP
Medio	Abierto	ZAP de OWASP	Control de acceso roto →

Descripción
La carga de datos del navegador web puede ser posible debido a una configuración incorrecta de uso compartido de recursos de origen cruzado (CORS) en el servidor web.

Recomendación
Asegúrese de que los datos confidenciales no estén disponibles de forma no autenticada (por ejemplo, mediante la inclusión de direcciones IP en listas blancas). Configure el encabezado HTTP "Access-Control-Allow-Origin" con un conjunto de dominios más restrictivo o elimine todos los encabezados CORS por completo para permitir que el navegador web aplique la Política del mismo origen (SOP) de una manera más restrictiva.

2. Encabezado anti-clickjacking faltante
(URI: https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx)

GRAVEDAD	ESTADO	ESCANEAR	LOS 10 MEJORES DE OWASP
Medio	Abierto	ZAP de OWASP	Mala configuración de seguridad →

Descripción
La respuesta no protege contra ataques de "ClickJacking". Debe incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.

Recomendación

Los navegadores web modernos admiten los encabezados HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que uno de ellos esté configurado en todas las páginas web que devuelva su sitio o aplicación. Si espera que la página solo esté enmarcada por páginas de su servidor (por ejemplo, si es parte de un FRAMESET), deberá utilizar SAMEORIGIN; de lo contrario, si nunca espera que la página esté enmarcada, deberá utilizar DENY. Como alternativa, considere implementar la directiva "frame-ancestors" de Content Security Policy.

3. Direcciones IP potenciales encontradas en Viewstate

(URI: https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx)

GRAVEDAD	ESTADO	ESCANEAR	LOS 10 MEJORES DE OWASP
Medio	Abierto	ZAP de OWASP	Diseño inseguro →

Descripción

Se encontraron las siguientes direcciones IP potenciales serializadas en el campo viewstate.

Method	GET
Parameter	
Attack	
Evidence	
Other Info	[017.1.228.45]
Request Header	GET https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx HTTP/1.1 host: sgdea.camara.gov.co user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0 pragma: no-cache cache-control: no-cache referer: https://www.camara.gov.co/profiles/*.css$
Request Body	
Response Header	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/10.0 Set-Cookie: ASP.NET_SessionId=egrv20ay21rvkjavhz21hqpr; path=/; HttpOnly; SameSite=Lax X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Access-Control-Allow-Origin: * Date: Tue, 26 Nov 2024 22:47:46 GMT Content-Length: 36009
Response Body (truncated)	<!DOCTYPE html> <html> <head><meta charset="utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><title> Sistema PQR Ciudadano - PQR</title><link href="../Content/bootstrap.css" rel="stylesheet" /><link href="../Content/bootstrap.min.css" rel="stylesheet" /><link href="../Content/Site.css" rel="stylesheet" /><li nk href="../Content/Global.css" rel="stylesheet" /><link href="../Content/Contraste.css" rel="stylesheet" /> <script src="//ajax.googleapis.co...(truncated)
Instances	1
Solution	Verify the provided information isn't confidential.
Reference	
CWE Id	642
WASC Id	14
Plugin Id	10032

Recomendación

Verifique que la información proporcionada no sea confidencial.

8. Encabezado de la Política de seguridad de contenido (CSP) no configurado
(URI: https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx)

GRAVEDAD	ESTADO	ESCANEAR	LOS 10 MEJORES DE OWASP
Medio	Abierto	ZAP de OWASP	Mala configuración de seguridad →

Descripción
La Política de Seguridad de Contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos los ataques de inyección de datos y de secuencias de comandos entre sitios (XSS). Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración de sitios o la distribución de malware. La CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deben poder cargar en esa página. Los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos integrables como subprogramas Java, ActiveX, archivos de audio y video.

Recomendación
Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. estén configurados para establecer el encabezado Content-Security-Policy.

Respuesta del área SGDA
Dando respuesta a todas las vulnerabilidades relacionadas con SGDEA, se remite la respuesta recibida por la empresa proveedora del servicio:

"Sobre los hallazgos técnicos identificados en la auditoría interna de seguridad informática, nos permitimos informar que después de la revisión, análisis y verificación con la Dirección de desarrollo se evidencia que las librerías mencionadas se encuentran obsoletas, por lo que se concluye que la manera más practica y rápida para subsanarlas, es realizando la actualización del sitio al nuevo PQRSD que se encuentra en Blazor en el cual se atacaron los hallazgos mencionados y se encuentran subsanados, este sitio ya se encuentra desarrollado y disponible para su implementación inmediata, garantizando continuidad en el funcionamiento de dicho módulo, especialmente frente a los procesos actualmente soportados por la Cámara de Representantes, por lo cual se dio inicio con la implementación en el ambiente de pruebas lo que permitirá proceder a realizar el flujo completo para garantizar el funcionamiento correspondiente a través de la realización de las pruebas funcionales con la participación de Cámara de Representantes con el propósito de obtener autorización para programar el paso a producción con la próxima actualización que se va a realizar al gestor dado que se requiere por el consumo de servicios establecidos.

Este cambio implica unas adaptaciones a nivel de desarrollo de código necesarias para la integración de PQRSD ya existente entre Senado de la República de Colombia y Cámara de Representantes, para las cuales se iniciará con el levantamiento del documento SRSS ó HU para revisar el impacto frente a ese canal de entrada, cabe aclarar que estos cambios afectan el canal de entrada de portal WEB y no toda la integración que ya está desarrollada en el gestor, estas adaptaciones se realizaran en paralelo al funcionamiento vigente, de modo que, al momento de la aprobación de la entrada en producción tanto de parte de Senado como Cámara de Representantes de la integración, la plataforma esté actualizada y en cumplimiento de los estándares de seguridad requeridos. Esta

estrategia asegura tanto la mitigación de los hallazgos identificados como el fortalecimiento de seguridad a nivel de la aplicación hacia un modelo más robusto y seguro."

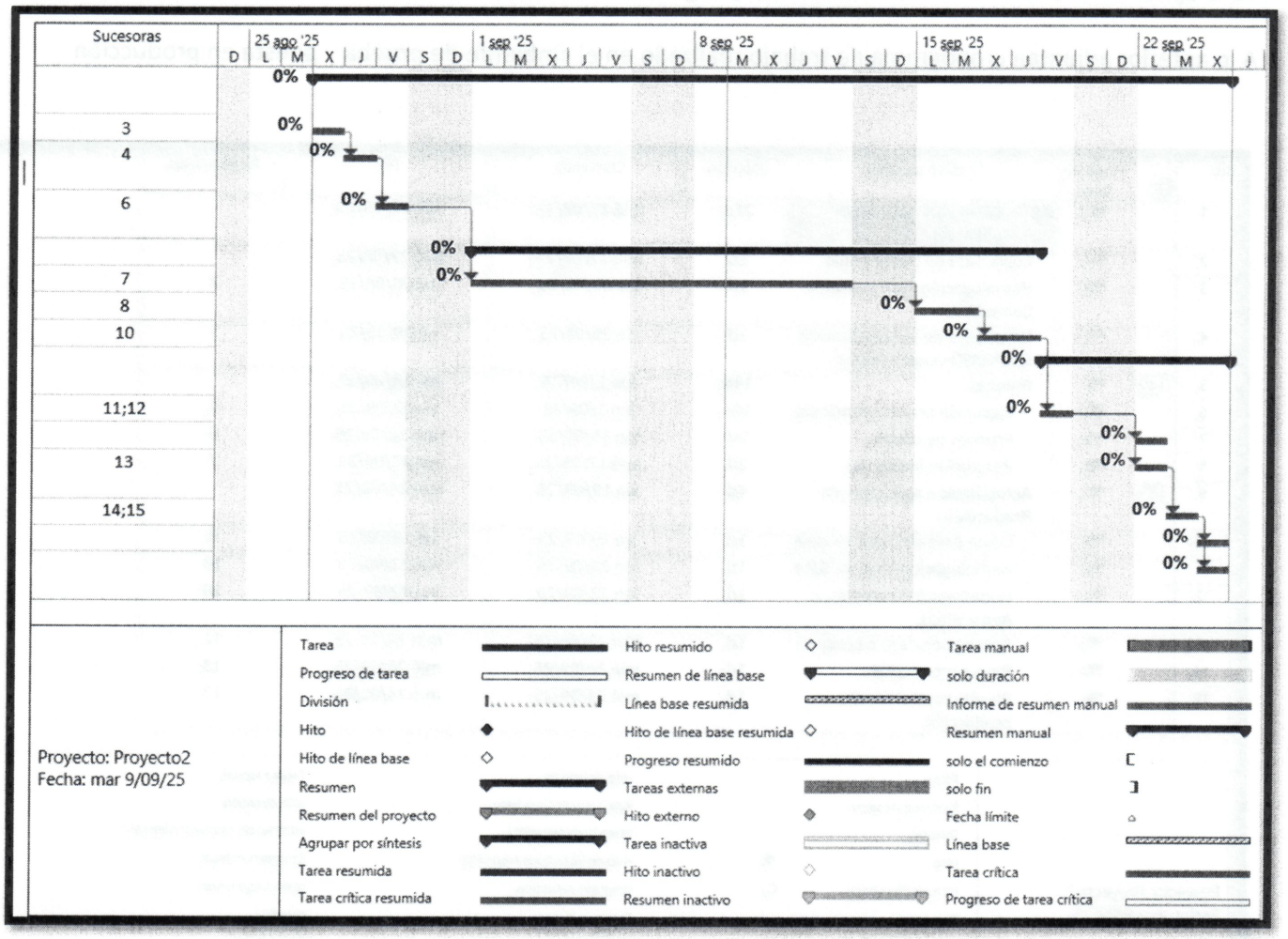
A lo anterior adjuntan cronograma de trabajo realizado en el ambiente de prueba y puesta en producción

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		**ACTUALIZACION AMBIENTE PQRSD (Blazor)**	**21d**	**mié 27/08/25**	**mié 24/09/25**	
2		Copia Base de Datos Y Sitio	1d	mié 27/08/25	mié 27/08/25	
3		Homologación Base de Datos ControlDoc	1d	jue 28/08/25	jue 28/08/25	2
4		Despliegue de la Actualización del PQRSD version Blazor	1d	vie 29/08/25	vie 29/08/25	3
5		**Pruebas**	**14d**	**lun 1/09/25**	**jue 18/09/25**	
6		Ejecución pruebas funcional	10d	lun 1/09/25	vie 12/09/25	4
7		Pruebas de cliente	2d	lun 15/09/25	mar 16/09/25	6
8		Resolución incidentes	2d	mié 17/09/25	jue 18/09/25	7
9		**Actualización aplicativo en Producción**	**4d**	**vie 19/09/25**	**mié 24/09/25**	
10		Copia Base de Datos y Copia	1d	vie 19/09/25	vie 19/09/25	8
11		Homologación Base de Dato	1d	lun 22/09/25	lun 22/09/25	10
12		Homologación carpetas y Appsettings	1d	lun 22/09/25	lun 22/09/25	10
13		Aprobación paso a producci	1d	mar 23/09/25	mar 23/09/25	12
14		Paso a producción	1d	mié 24/09/25	mié 24/09/25	13
15		Prueba controlada en producción	1d	mié 24/09/25	mié 24/09/25	13

Proyecto: Proyecto2
Fecha: mar 9/09/25

Tarea		Hito resumido	Tarea manual
Progreso de tarea		Resumen de línea base	solo duración
División		Línea base resumida	Informe de resumen manual
Hito	◆	Hito de línea base resumida	Resumen manual
Hito de línea base	◇	Progreso resumido	solo el comienzo
Resumen		Tareas externas	solo fin
Resumen del proyecto		Hito externo	Fecha límite
Agrupar por síntesis		Tarea inactiva	Línea base
Tarea resumida		Hito inactivo	Tarea crítica
Tarea crítica resumida		Resumen inactivo	Progreso de tarea crítica

Página 1



Respuesta de la OCCI

Conforme a la respuesta remitida desde el área de SGDA frente a las observaciones realizadas, se concluye, que se han venido realizando las correcciones correspondientes; que una vez puesta la aplicación en ambiente de producción se realizara el respectivo seguimiento. Conforme a lo anterior se da por subsanada la observación.

CONCLUSIONES Y RECOMENDACIONES

Teniendo en cuenta las evidencias aportadas a cada una de las observaciones, de manera general se concluye, que la entidad ha realizado el mayor esfuerzo en materia de ciberseguridad para subsanar las falencias detectadas en el sitio web, que en algunos casos se pueden ver estas correcciones de forma concreta y en otros casos, estas correcciones se han realizado, pero se encuentran en un ambiente de prueba en espera de llevarlos a un ambiente de producción.

Esta oficina recomienda que se continuo con el trabajo y se ponga en producción lo más pronto posible la nueva página web, con el fin de ofrecer de cara a la ciudadanía y al interior de la entidad un sitio web accesible, amigable y robusto.

Para constancia se firma en Bogotá D.C., a los 05 días del mes de septiembre del año 2025

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**
JEHYMMYS TATIANA SANCHEZ CALA	COORDINADORA	
ALVARO ERNESTO OSPINA RAMÍREZ	PROFESIONAL UNIVERSITARIO	
NIDIA CLEMENCIA HERNANDEZ BAQUERO	PROFESIONAL UNIVERSITARIO	
JUAN PABLO ALVAREZ MOSQUERA	PROFESIONAL UNIVERSITARIO	
ANGIE LILIANA PAEZ HERNANDEZ	CONTRATISTA DE APOYO	

CONTROL DE CAMBIOS

Nº VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	01/01/2016	Versión inicial del formato
2	28/01/2022	La 2da versión fue aprobada acta 1 Comité Institucional de Gestión y Desempeño llevado a cabo el 28 de enero de 2022 y reformula todo el formato.