Fecha: 19 de septiembre de 2022

O.C.C.I.1.7 -400 -2022

Para: JUAN JOSÉ GÓMEZ VÉLEZ – Jefe Oficina de Planeación y Sistemas

De: OFICINA COORDINADORA DEL CONTROL INTERNO

Asunto: Informe de Auditoría Interna Seguimiento TICS

URGENTE	X	PROYECTAR RESPUESTA	X
PARA SU INFORMACIÓN	X	DAR RESPUESTA INMEDIATA	
FAVOR DAR CONCEPTO		FAVOR TRAMITAR	
		No. FOLIOS	

Respetado Doctor Gómez:

Dando continuidad a la auditoria del asunto, nos permitimos remitir adjunto el informe final de la misma, dicho Informe contiene las respectivas observaciones y recomendaciones, por lo anterior y atendiendo al cronograma establecido y socializado en la comunicación del informe preliminar, le solicitamos se sirva en suscribir el respectivo plan de mejoramiento en el término acá establecido:

Actividad	Fecha
Informe Preliminar	7 de septiembre de 2022
Controversias	8 – 13 de Septiembre de 2022
Informe Final	14 - 19 de septiembre de 2022
Presentación Plan de Mejoramiento	**20 - 27 de Septiembre de 2022**

Cordialmente,

ARNULFO RONCANCIO SANABRIA
Coordinador de Control Interno

FECHA DE EMISIÓN DEL INFORME	**Día:**	06	**Mes:**	09	**Año:**	2022

PROCESO / PROCEDIMIENTO AUDITADO:	Proceso de Apoyo – Gestión de las TIC. OFICINA DE PLANEACIÓN Y SISTEMAS
LÍDER PROCESO AUDITADO:	DR. JUAN JOSÉ GÓMEZ VÉLEZ
Objetivo de la Auditoría:	Realizar seguimiento al cumplimiento del plan de mejoramiento de la auditoría realizada en la vigencia 2021
Alcance de la Auditoría:	La presente auditoría inicia con la revisión de las actividades suscritas en el plan de mejoramiento, las evidencias que soportan el avance y/o cumplimiento de las mismas y finaliza con el informe final y sus observaciones y/o recomendaciones.
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	25	**Mes**	05	**Año**	2022	**Desde**	01/06/2022	**Hasta**	30/06/2022	Día	19	Mes	09	Año	2022

Jefe oficina de Control Interno	**Auditor Líder**
Dr. ARNULFO RONCANCIO SANABRIA	Abogado e Ingeniero ALVARO E. OSPINA R.

EJECUCIÓN DE LA AUDITORIA

Se reviso la auditoría y el plan de mejoramiento suscrito por la oficina responsable donde se verifica cada una de las evidencias aportadas, así:

Ítem	Observación /hallazgo	Causas raíz	Acción correctiva a implementar	Actividad de mejora
1.1	No existe código de error 404	No existe repositorio en el servidor que responda al error 404	No se requiere acción de contingencia, ya que dicho código de error se encuentra presente dentro del servidor.	Mejores tiempos de carga para identificar archivos inexistentes dentro del servidor.

Respuesta del auditado:

El Mensaje de error implementado

Soporte:

Resultado de la verificación:

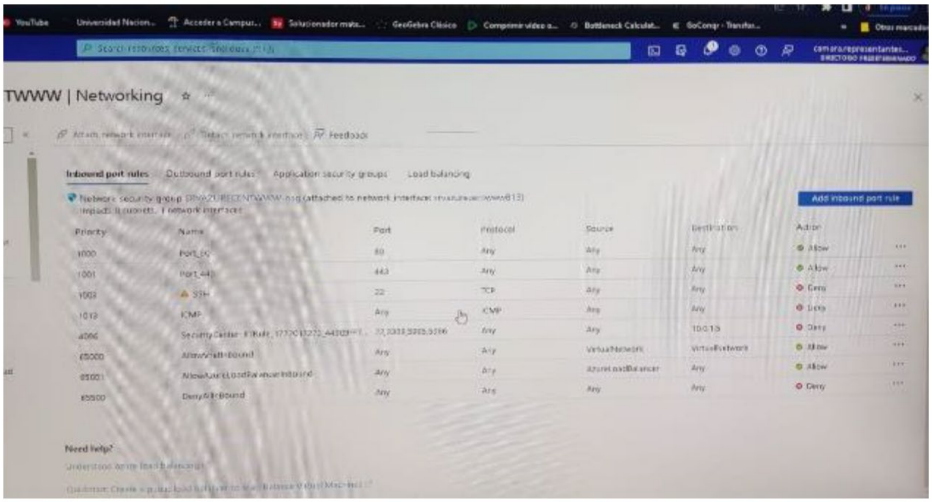
Conforme a la evidencia soportada se verifico el cumplimiento, por lo cual se da como subsanada la observación.
Actividad de mejora cumplida.

Ítem	Observación /hallazgo	Causas raíz	Acción correctiva a implementar	Actividad de mejora
1.2	Puertos TCP (22, 80, 433) Abiertos	No existe cobertura del firewall al servidor.	Implementar una conexión de seguridad de escaneos TCP desde el firewall, para el servidor local donde está alojada la web de la entidad, generando un filtro IP que proteja el servidor.	El puerto 22 se habilita cuando se requiere hacer un cambio en el servidor y los puertos 80 y 433 no deben cerrarse. Implementar un filtro IP, mediante un VPN, desde los dispositivos conectados al dominio y a la red, de modo que se permita proteger la IP local donde se encuentra el servidor de la web de la entidad.

Respuesta del auditado:

Puertos de tipo TCP cerrados y con acceso denegado desde protocolos SSH. Dichos puertos solo son de acceso local y no se permite entrar desde un equipo que no pertenezca al dominio de la entidad.

Soporte:



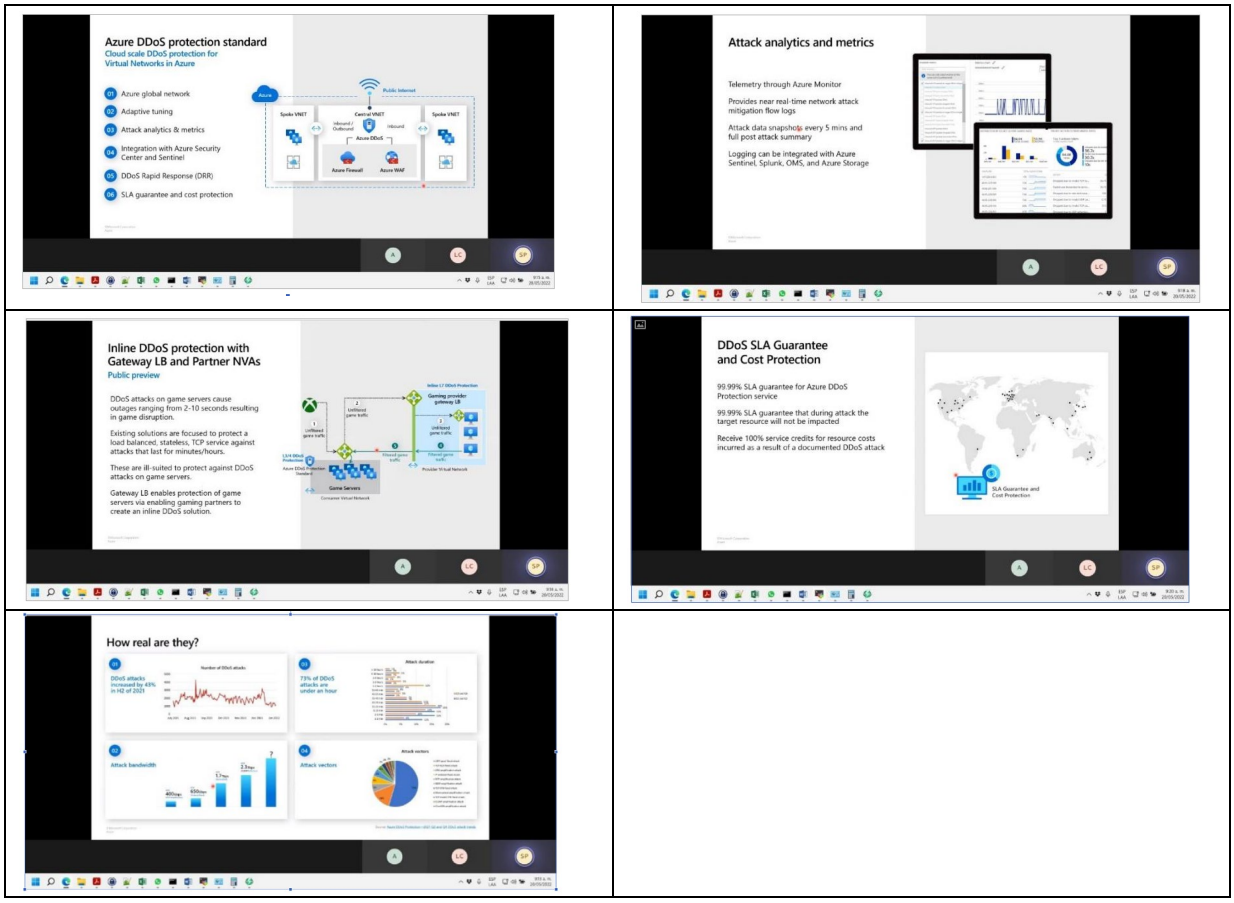
Resultado de la verificación:

Se realiza visita para verificar el cumplimiento, corroborando la evidencia aportada, por lo cual se da como subsanada la observación.
Actividad de mejora cumplida.

Ítem	Observación /hallazgo	Causas raíz	Acción correctiva a implementar	Actividad de mejora
1.4	Protocolo TLS desactualizado	EL protocolo de seguridad TLS se encuentra en versión 1.1	Se debe habilitar la compatibilidad con los protocolos TLS 1.2 y 1.3	Se plantea realizar en conjunto con el proveedor del certificado, un concepto basado en los errores marcados, con la finalidad del plantear de mejoras en este punto de manera global.
1.3	Cifrados CBC en el servidor SSL	El servidor está configurado con el cifrado cipher block chaining	Se debe reestructurar y re configurar el cifrado SSL presente en el servidor local como en el servidor remoto. Teniendo en cuenta lo siguiente: 1. Las firmas de los cifrados deben ser verificadas de extremo a extremo, por la arquitectura de seguridad perimetral instalada en el servidor local y por el certificado brindado en el servidor remoto o máquina virtual. 2. Se debe cambiar el tipo de cifrado CBC por uno más eficiente, teniendo en cuenta el esquema de seguridad de firewall presentado. 3. Se debe replantear el gestor que va a generar el cifrado SSL, tanto en el servidor local como en el remoto.	
1.5	Cifrados de intensidad media SSl	El servidor SSL permite cifrados de intensidad media con claves de al menos 64 bits y menos de 112 bits		
1.6	Confiabilidad del cifrado SSL	La cadena de certificados SSL presenta diferentes falencias en el proceso de certificación de la información, debido a la baja confiabilidad de las firmas de dicho certificado.		
1.7	Autofirmado SSL	La parte superior de la cadena de certificados se encontraba Autofirmado		

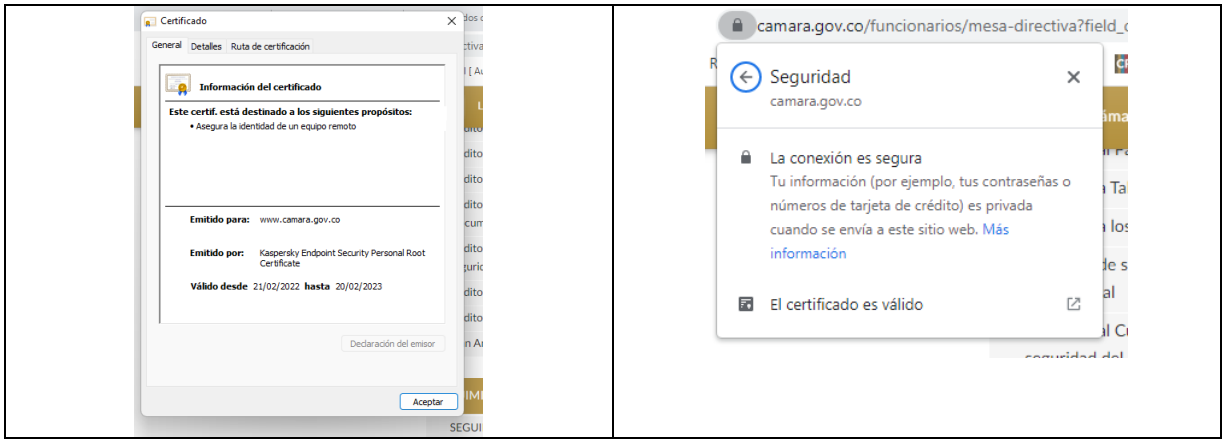
Respuesta del auditado:

Se inició el proceso de actualización del certificado SSL y se pusieron en marcha filtros nuevos dentro del protocolo TLS, en conjunto con el proveedor del servicio que en este caso es Microsoft y Azure. Aún hacen falta unas estimaciones y generar la llave privada que mejora la firma de los certificados, pero el proceso de actualización de seguridad SSL ya está en marcha.



Resultado de la verificación:

Se pudo establecer que los certificados fueron actualizados.
Actividad de mejora cumplida.



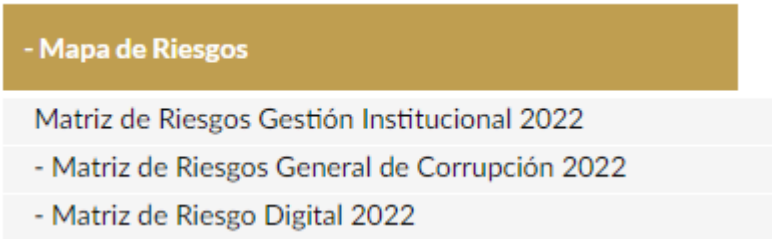
Ítem	Observación /hallazgo	Causas raíz	Acción correctiva a implementar	Actividad de mejora
3	Mapas de Riesgos no Actualizados	La alta rotación de personal no permite la continuidad de los procesos	Actualización de Mapas de Riesgos	Ya fueron actualizados los Mapas de Riesgos (Vigencia 2022)

Respuesta del auditado:

Fueron actualizados los Mapas de Riesgos (Vigencia 2022)
1. Matriz de Riesgos de Gestión Institucional
2. Matriz de Riesgos de Corrupción
3. Matriz de Riesgos Digital
https://www.camara.gov.co/mapa-de-riesgos

Resultado de verificación:

Se pudo establecer que fueron actualizados los mapas de riesgos y debidamente publicados. **Actividad de mejora cumplida.**



Ítem	Observación /hallazgo	Causas raíz	Acción correctiva a implementar	Actividad de mejora
4	Métricas que permitan monitorear las Políticas de Seguridad	No existen Métricas de Seguridad	Implementar métricas para medir el cumplimiento de las políticas de Seguridad	Crear métricas para medir el cumplimiento de las políticas de Seguridad

Respuesta del auditado:

En reunión con el Ingeniero Alejandro Muñoz de la Oficina de Planeación y Sistemas manifestó que “Acción pendiente de realizar”.

Resultado de la verificación:

La acción propuesta se encuentra vencida, toda vez que se suscribió como fecha de inicio y final “Mayo 2022 - Julio 2022”.

Actividad de mejora incumplida.

Ítem	Observación /hallazgo	Causas raíz	Acción correctiva a implementar	Actividad de mejora
5	Procesos y Procedimientos relacionados con Seguridad Informática	No se encuentran Procesos y Procedimientos relacionados con Seguridad Informática	Implementar Procedimientos relacionados con Seguridad Informática	En el Comité Institucional de Gestión y Desempeño realizado el 16 de diciembre del 2021 y mediante Acta No.3 se aprobaron los siguientes procedimientos: 1. Procedimiento de Backup y Restauración 2. Procedimiento de Control de Acceso 3. Procedimiento de Control de Incidentes 4. Procedimiento de Gestión de Activos de Información 5. Procedimiento de Recursos Humanos 6. Procedimiento de Seguridad Física y del Entorno 7. Procedimiento de Adquisición, Mantenimiento y Desarrollo de Sistemas de Información

Respuesta del auditado:

En el Comité Institucional de Gestión y Desempeño realizado el 16 de diciembre del 2021 y mediante Acta No.3 se aprobaron los siguientes Procedimientos:

1. Procedimiento de Backup y Restauración
2. Procedimiento de Control de Acceso
3. Procedimiento de Control de Incidentes
4. Procedimiento de Gestión de Activos de Información
5. Procedimiento de Recursos Humanos
6. Procedimiento de Seguridad Física y del Entorno
7. Procedimiento de Adquisición, Mantenimiento y Desarrollo de Sistemas de Información

Los anteriores documentos pueden ser consultados en el siguiente link:
https://www.camara.gov.co/procedimientos-de-ti

Resultado de la verificación:

Se pudo constatar que existen los documento actualizados y publicados.
Actividad de mejora cumplida.

Procedimientos
1. Procedimiento de Backup y Restauración
2. Procedimiento de Control de Acceso
3. Procedimiento de Control de Incidentes
4. Procedimiento de Gestión de Activos de Información
5. Procedimiento de Recursos Humanos
6. Procedimiento de Seguridad Física y del Entorno
7. Procedimiento de Adquisición, Mantenimiento y Desarrollo de Sistemas de Información

Ítem	Observación /hallazgo	Causas raíz	Acción correctiva a implementar	Actividad de mejora
6	Políticas de Seguridad de la Información	No se encuentra actualizado el documento de la Políticas de Seguridad de la Información, según los lineamientos de la norma ISO/IEC 27001	Actualizar las Políticas de Seguridad de la Información de la Entidad, según los lineamientos de la norma ISO/IEC 27001	En el Comité Institucional de Gestión y Desempeño realizado el 16 de diciembre del 2021 y mediante Acta No.3 se aprobaron las siguientes políticas: 1. Política de Backup 2. Política de Control de Acceso 3. Política de Gestión de Incidentes 4. Política de Gestión de Activos de Información 5. Política General de Seguridad y Privacidad de la Información 6. Política de Capacitación y Sensibilización 7. Política de Escritorio Limpio 8. Política de Privacidad y Confidencialidad 9. Política de Integridad 10. Política de No Repudio 11. Política de Uso Aceptable de Activos de Información

Respuesta del auditado.

En el Comité Institucional de Gestión y Desempeño realizado el 16 de diciembre del 2021 y mediante Acta No.3 se aprobaron las siguientes Políticas:

1. Política de Backup
2. Política de Control de Acceso
3. Política de Gestión de Incidentes
4. Política de Gestión de Activos de Información
5. Política General de Seguridad y Privacidad de la Información
6. Política de Capacitación y Sensibilización

7. Política de Escritorio Limpio
8. Política de Privacidad y Confidencialidad
9. Política de Integridad
10. Política de No Repudio
11. Política de Uso Aceptable de Activos de Información

Los anteriores documentos pueden ser consultados en el siguiente link:
https://www.camara.gov.co/politicas-de-ti

Resultado de la verificación:

Se constató que se adoptaron las políticas mencionadas y fueron debidamente publicadas. Actividad de mejora cumplida.

- Políticas

1. Política de Backup
2. Política de control de acceso
3. Política de Gestión de Incidentes
4. Política de Gestión de Activos de Información
5. Política General de Seguridad y Privacidad de la Información
6. Política de Capacitación y Sensibilización
7. Política de Escritorio Limpio
8. Política de Privacidad y Confidencialidad
9. Política de Integridad
10. Política de No Repudio
11. Política de Uso Aceptable de Activos de Información

Ítem	Observación /hallazgo	Causas raíz	Acción correctiva a implementar	Actividad de mejora
7	Planes y Programas	Falta implementación de un Sistema de Gestión en Seguridad de la Información SGSI.	Socialización de Políticas de Seguridad y Privacidad de la Información	Realizar socialización de Políticas de Seguridad y Privacidad de la Información
			Solicitud de recursos ante el Min Hacienda y el DNP para llevar a cabo la implementación del SGSI	Gestionar la solicitud de recursos ante el Min Hacienda y el DNP para llevar a cabo la implementación del SGSI

Una vez realizado el seguimiento de las actividades de mejora suscritas, con el fin de determinar si las acciones o actividades suscritas en relación a la seguridad de la página web de la entidad fueron efectivas, se realiza un diagnóstico externo de la misma con las herramientas ZAP scaning y NMAP escaning, herramientas de auditar la seguridad web de código abierto, cuyos resultados fueron los siguientes:

Informe de escaneo
21 de agosto de 2022
Resumen

Riesgos más recientes

	TÍTULO	TIPO DE SCANEADO	OBJETIVO	NIVEL DE AMENAZA	VAS ABIERTAS QOD
>	SSL/TLS: Informar conjuntos de cifrado vulnerables para HTTPS	OPENVAS	https://www.camara.gov.co/	ALTO	98%
>	Métodos de depuración HTTP (TRACE/TRACK) habilitados	OPENVAS	https://www.camara.gov.co/	MEDIO	99%
>	SSL/TLS: certificado caducado	OPENVAS	https://www.camara.gov.co/	MEDIO	99%
>	SSL/TLS: Detección de protocolo TLSv1.0 y TLSv1.1 en desuso	OPENVAS	https://www.camara.gov.co/	MEDIO	98%
>	Marcas de tiempo de TCP	OPENVAS	https://www.camara.gov.co/	BAJO	80%

"*Este documento informa sobre los resultados de un análisis de seguridad automático. Todas las fechas se muestran utilizando la zona horaria Hora universal coordinada, que se abrevia como UTC. La tarea era 6302a488d2fc07004beaa369-6302a488d2fc07004beaa370. El escaneo comenzó el domingo 21 de agosto a las 21:33:31 2022 UTC y finalizó el domingo 21 de agosto a las 21:43:58 2022 UTC. El informe primero resume los resultados encontrados. Luego, para cada host, el informe describe cada problema encontrado.*

Tenga en cuenta los consejos que se dan en cada descripción para corregir el problema."

1- Resumen de Resultados:

Host	High	Medium	Low	Log	False Positive
23.96.32.104	1	3	1	31	0
Total: 1	1	3	1	31	0

1. **Las actualizaciones de seguridad del proveedor no son de confianza.**
2. **Las anulaciones (Overrides) están desactivadas. Incluso cuando un resultado tiene una anulación, este informe utiliza la amenaza real del resultado.**
3. **La información sobre anulaciones se incluye en el informe.**
4. **Las notas se incluyen en el informe.**
5. **Es posible que este informe no muestre detalles de todos los problemas que se encontraron.**

Solo se mostrarán los resultados desde una QoD mínima (*Calidad de detección (QoD) es un valor entre 0-100 % que describe la confiabilidad de una detección de vulnerabilidad/detección de producto ejecutada*) de 70%.
Este informe contiene los 36 resultados seleccionados por el filtro descrito anteriormente. Antes de aplicar el filtro había 177 resultados.

2- Resultado por Host

2.1- 23.96.32.104

La exploración del host inicia el domingo 21 de agosto a las 21:34:03 de 2022 UTC.
El escaneo del host finaliza el dom. 21 de agosto a las 21:43:50 2022 UTC.

Service (Port)	Threat Level
443/tcp	High
443/tcp	Medium
general/tcp	Low
80/tcp	Log
general/tcp	Log
general/CPE-T	Log
443/tcp	Log

Se tomará los resultados de riesgo alto y medio de vulnerabilidad más relevantes, los demás podrán ser consultados en el informe de resultados original.

2.1.1 High 443/tcp

High (CVSS - Common Vulnerability Scoring System: 7.5).
NVT (Network Vulnerability Test): SSL/TLS: Informar conjuntos de cifrado vulnerables para HTTPS.

Resumen
Esta rutina informa todos los conjuntos de cifrado SSL/TLS aceptados por un servicio donde los vectores de ataque existen solo en los servicios HTTPS.

Resultado de la detección de vulnerabilidad:
Conjuntos de cifrado 'vulnerables' aceptados por este servicio a través del protocolo TLSvl.O:
TLS DHE RSA WITH 3DES EDE CBC SHA (SWEET32)
TLS-ECDHE RSA WITH 3DES EDE CBC SHA (SWEET32)
TLS RSA WITH 3DES EDE CBC SHA (SWEET32)
Conjuntos de cifrado vulnerables aceptados por este servicio a través del protocolo TLSvl. 1:
TLS DHE RSA WITH 3DES EDE CBC SHA (SWEET32)
TLS ECDHE RSA WITH 3DES EDE CBC SHA (SWEET32)
TLS_RSA_CON_3DES_EDE_CBC_SHA (SWEET32)
Conjuntos de cifrado 'vulnerables' aceptados por este servicio a través del protocolo TLSvl.2:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA(SWEET32)
TLS_RSA_CON_3DES_EDE_CBC_SHA (SWEET32)

Solución:
Tipo de solución: Mitigación
La configuración de estos servicios debe cambiarse para que ya no acepte los conjuntos de cifrado enumerados.

Consulte las referencias para obtener más recursos que lo ayuden con esta tarea.

Software/SO afectado
Servicios que aceptan suites de cifrado SSL/TLS vulnerables a través de HTTPS.

Perspectiva de vulnerabilidad
Estas reglas se aplican para la evaluación de los conjuntos de cifrado vulnerables:
- Cifrado de bloques de 64 bits 3DES vulnerable al ataque SWEET32 (CVE-2016-2183).

Método de detección de vulnerabilidades
Detalles: SSL/TLS: Informar conjuntos de cifrado vulnerables para HTTPS
OID (Object ID):1.3.6.1.4.1.25623.1.0.108031
Versión utilizada: 2022-08-01T10:11:45Z

2.1.2 Medium 443/tcp

Medium (CVSS: 5.8).
NVT: HTTP Método de depuración (TRACE/TRACK) habilitado.

Resumen
El servidor web remoto admite los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.

Resultado de la detección de vulnerabilidad
El servidor web tiene habilitados los siguientes métodos HTTP: TRACE

Impacto
Un atacante puede usar esta falla para engañar a sus usuarios web legítimos para que le den sus credenciales.

Solución:
Tipo de solución: Mitigación
Deshabilite los métodos TRACE y TRACK en la configuración de su servidor web.
Consulte el manual de su servidor web o las referencias para obtener más información.

Software/SO afectado
Servidores web con métodos TRACE y/o TRACK habilitados.

Perspectiva de vulnerabilidad
Se ha demostrado que los servidores web que admiten estos métodos están sujetos a ataques de secuencias de comandos entre sitios, denominados XST por Cross-Site-Tracing, cuando se usan junto con varias debilidades en los navegadores.

Método de detección de vulnerabilidades
Comprueba si los métodos HTTP como TRACE y TRACK están habilitados y se pueden usar.
Detalles: métodos de depuración HTTP (TRACE/TRACK) habilitados.
OID: 1.3.6.1.4.1.25623.1.0.11213
Versión utilizada: 2022-05-12T09: 32: 012

Medio (CVSS: 5.0)
NVT: SSL/TLS: certificado caducado

Resumen
El certificado SSL/TLS del servidor remoto ya ha caducado.

Resultado de la detección de vulnerabilidad
El certificado del servicio remoto venció el 2021-02-24 21:01:29.
Detalles del certificado:
huella digital (SHA-1) | 743227A78143B14CF56526051455BBC9DC225BDE
huella digital (SHA-256) | 7BBA518E362086382F3552576819A313FB0D35BC0F099F43551CD85169715081
emitido por | 1.2.840.113549.1.9.1=#726F6F7440535256415A55524543454E54575757,CN=SRVAZURECE
NTW WW,OU=SomeOrganizationalUnit,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
tamaño de clave pública (bits) | 2048
serie | 7315
algoritmo de firma | sha256WithRSAEncryption
sujeto | 1.2.840.113549.1.9.1=#726F6F7440535256415A55524543454E54575757,CN=SRVAZURECENT
WWW,OU=SomeOrganizationalUnit,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
Nombres alternativos del sujeto (SAN) | Ninguno
válido desde el | 2020-02-25 21:01:29 UTC
válido hasta el | 2021-02-24 21:01:29 UTC

Solución:
Tipo de solución: Mitigación
Reemplace el certificado SSL/TLS por uno nuevo.

Perspectiva de vulnerabilidad
Este script comprueba las fechas de caducidad de los certificados asociados con los servicios habilitados para SSL/TLS en el destino e informa si alguno ya ha caducado.

Método de detección de vulnerabilidades
Detalles: SSL/TLS: certificado caducado OID:1.3.6.1.4.1.25623.1.0.103955
Versión utilizada: 2021-11-22T15:32:392

Medio (CVSS: 4.3)
NVT: SSL/TLS: Detección de protocolo TLSv1.0 y TLSv1.1 en desuso

Resumen
Fue posible detectar el uso del protocolo obsoleto TLSv1.0 y/o TLSv1.1 en este sistema.

Resultado de la detección de vulnerabilidad
Además de TLSv1.2+, el servicio también proporciona los protocolos obsoletos TLSv1.0 y TLSv1.1 y admite uno o más cifrados. Esos cifrados admitidos que pueden encontrarse en 'SSL/TLS: Informe de conjuntos de cifrado admitidos' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impacto
Un atacante podría utilizar las fallas criptográficas conocidas para espiar la conexión entre los clientes y el servicio para obtener acceso a los datos confidenciales transferidos dentro de la conexión segura.

Además, las vulnerabilidades descubiertas recientemente en estos protocolos no recibirán actualizaciones de seguridad.

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

Software/SO afectado
Todos los servicios que proporcionan una comunicación encriptada utilizando los protocolos TLSv1.0 y/o TLSv1.1.

Perspectiva de vulnerabilidad
Los protocolos TLSv1.0 y TLSv1.1 contienen fallas criptográficas conocidas como:

- CVE-2011-3389: Explotación del navegador contra SSL/TLS (BEAST)
- CVE-2015-0204: Ataque de factorización en el relleno de claves RSA-EXPORT Oracle en el cifrado heredado degradado (FREAK)

Método de detección de vulnerabilidades
Consulte los protocolos TLS utilizados de los servicios proporcionados por este sistema.
Detalles: SSL/TLS: Detección de protocolo TLSv1.0 y TLSv1.1 en desuso
OID:1.3.6.1.4.1.25623.1.0.117274
Versión utilizada: 2021-07-19T08:11:482

2.1.3 Low general/tcp

Bajo (CVSS: 2.6)
NVT: timestamps (Sellado de Tiempo) TCP

Resumen
El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.

Resultado de la detección de vulnerabilidad
Se detectó que el host implementa RFC1323/RFC7323.
Las siguientes marcas de tiempo se recuperaron con un retraso de 1 segundo entre ellas:
Paquete 1: 937950294
Paquete 2: 937951342

Impacto
Un efecto secundario de esta función es que, a veces, se puede calcular el tiempo de actividad del host remoto.

Solución:
Tipo de solución: Mitigación
Para deshabilitar las marcas de tiempo de TCP en Linux, agregue la línea 'net.ipv4.tcp_timestamps 0' a /etc/sysctl.conf. Ejecute 'sysctl -p' para aplicar la configuración en tiempo de ejecución.
Para deshabilitar las marcas de tiempo de TCP en Windows, ejecute 'netsh int tcp set global timestamps disabled'
A partir de Windows Server 2008 y Vista, el sellado de tiempo no se puede desactivar por completo.
El comportamiento predeterminado de la pila TCP/IP en este sistema es no usar las opciones de sellado de tiempo al iniciar conexiones TCP, pero sí usarlas si el par TCP que está iniciando la comunicación las incluye en su segmento sincronizado (SYN).
Consulte las referencias para obtener más información.

Software/SO afectado
Implementaciones de TCP que implementan RFC1323/RFC7323.

Perspectiva de vulnerabilidad
El host remoto implementa marcas de tiempo TCP, según lo definido por RFC1323/RFC7323.

Método de detección de vulnerabilidades
Los paquetes de IP especiales se falsifican y se envían con un poco de retraso a la IP de destino. Las respuestas se buscan por marcas de tiempo. Si se encuentran, se informan las marcas de tiempo.
Detalles: marcas de tiempo de TCP
OID:1.3.6.1.4.1.25623.1.0.80091
Versión utilizada: 2020-08-24T08:40:102

Los siguientes registros podrán ser consultados en el informe adjunto:

Puerto de servicio	Nivel de amenaza
80/tcp	LOG
general/tcp	LOG
general/CPE-T	LOG
443/tcp	LOG

RECOMENDACIONES

- ✓ Esta oficina recomienda que se realicen las actividades de mejora dentro de los términos y/o plazos suscritos en el plan mejoramiento.

- ✓ Que se evalúe la pagina web de la entidad en términos de seguridad y accesibilidad, con el fin de determinar si esta cumple con los estándares actuales establecidos en la Resolución 1519 de 2020 "*Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos*".

- ✓ Con respecto a las políticas de Seguridad Digital adoptadas e implementadas por la entidad, se recomienda que se dé seguimiento al cumplimiento estricto de las mismas, en especial, a la restricción de permisos en las estaciones de trabajo, con el fin de evitar que se descarguen y/o instalen aplicaciones sin licenciamiento legal y así evitar ataques de virus y/o malware, además, de problemas legales para la entidad y/o los funcionarios y contratistas que lo realicen. En el mismo sentido, es necesario, que se realicen talleres de forma presencial para la socialización de las Políticas de Seguridad de la Información adoptadas por la entidad.

- ✓ En lo que corresponde a la evaluación de seguridad de la página web, se observó en el resultado del escaneo (1) riesgo de vulnerabilidad alto en el puerto 443, (3) de nivel medio, (1) de nivel bajo y (4) registros sin nivel de riesgos. Es necesario resaltar que dentro de este proceso se vuelve a encontrar una observación relacionada con el código de "error 404" así:
  "*está [mal] configurado en el sentido de que no devuelve los códigos de error '404 No encontrado' cuando se solicita un archivo inexistente, tal vez devolviendo un mapa del sitio, una página de búsqueda, una página de autenticación o una redirección en su lugar.*

  no responde en un tiempo razonable a varias solicitudes HTTP enviadas por este VT(Test de vulnerabilidad). Para mantener el tiempo total de análisis en una cantidad razonable, es posible que no se pruebe el servidor web remoto. Si se debe probar el servidor remoto, debe repararse para que responda a los escáneres."

  Conforme a lo anterior, se recomienda realizar una revisión atendiendo al resultado de vulnerabilidad detectado en razón a la velocidad de respuesta que dice así:

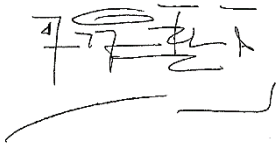
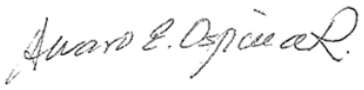
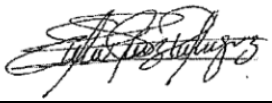
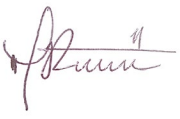
"*Resultado de la detección de vulnerabilidad*
El host devuelve un código de error 30x (por ejemplo, 301) cuando se solicita un archivo que no existe. Se han deshabilitado algunas comprobaciones relacionadas con HTTP."

- ✓ De acuerdo a los resultados obtenidos en la presente auditoría, esta oficina recomienda, la implementación y puesta en operación del "*Modelo de Seguridad y Privacidad de la Información*" y se establezca el respectivo "*Plan de Operación de Continuidad del Negocio*" de manera urgente.

CONCLUSIONES DE LA AUDITORÍA

El equipo auditor pudo observar que se suscribieron (9) actividades de mejora de la cuales se ejecutaron (6) en los términos establecidos, (1) se incumplió por vencimiento de plazos y se encuentran en ejecución (2). Lo que corresponde a una ejecución del 67%, un incumplimiento del 11% y pendiente por ejecutar el 22%. En el mismo sentido, se observa que sigue habiendo falencias en la seguridad de la página web, situación que se debe evaluar y estudiar, la viabilidad de la implementación y/o actualización de la página web de la entidad atendiendo a los nuevos estándares de seguridad digital.

Para constancia se firma en Bogotá D.C., a los 06 días del mes de Septiembre del año 2022

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**
ARNULFO RONCANCIO SANABRIA	COORDINADOR	
ALVARO ERNESTO OSPINA RAMÍREZ	PROFESIONAL UNIVERSITARIO	
NIDIA CLEMENCIA HERNANDEZ BAQUERO	PROFESIONAL UNIVERSITARIO	
WILSON ESTIVEN GÓMEZ RODRÍGUEZ	CONTRATISTA	
JENNILER MOSQUERA ROGELES	CONTRATISTA	

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.