FECHA DE EMISIÓN DEL INFORME FINAL	Día:	28	Mes:	07	Año:	2026

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:	Determinar el estado de seguridad del portal institucional respecto a vulnerabilidades técnicas, configuraciones inseguras y riesgos de ciberseguridad, verificando la existencia de controles adecuados para proteger la disponibilidad, integridad y confidencialidad de la información institucional.
Alcance de la Auditoría:	La auditoría comprendió el análisis de los resultados obtenidos mediante las herramientas OpenVAS, Nmap (TCP y UDP), SSLyze, Nuclei y OWASP ZAP Passive Scan, las cuales permitieron evaluar la infraestructura de red, los puertos TCP y UDP, los certificados digitales, la configuración de los protocolos SSL/TLS, los servicios expuestos, la configuración HTTP, las vulnerabilidades conocidas (CVE), las bibliotecas JavaScript utilizadas, la seguridad de las aplicaciones web, los encabezados HTTP y la configuración criptográfica, con el propósito de identificar vulnerabilidades, verificar el nivel de seguridad de los activos tecnológicos y establecer oportunidades de mejora para fortalecer la postura de ciberseguridad de la entidad.
Criterios de la Auditoría:	La presente auditoría se desarrolló con fundamento en el marco normativo aplicable en materia de control interno, transparencia, protección de datos personales, gobierno y seguridad digital, gestión del riesgo y ciberseguridad, considerando, entre otras disposiciones, la Constitución Política de Colombia, las Leyes 87 de 1993, 1581 de 2012, 1712 de 2014 y 2195 de 2022, los Decretos 1078 de 2015 y 338 de 2022, el Modelo de Seguridad y Privacidad de la Información (MSPI), el Modelo Integrado de Planeación y Gestión (MIPG), así como las buenas prácticas y estándares internacionales contenidos en las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, el NIST Cybersecurity Framework 2.0 y el OWASP Top 10, los cuales constituyen el referente técnico para la evaluación de los controles de seguridad de la información y la gestión de riesgos cibernéticos.

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	10	Mes	06	Año	2026	Desde	11/06/26 D / M / A	Hasta	23/07/26 D / M / A	Día	28	Mes	07	Año	2026

Jefe oficina de Control Interno	Auditor Líder
Dr. LUIS EDUARDO VELASQUEZ	ALVARO ERNESTO OSPINA RAMÍREZ NIDIA C HERNANDEZ BAQUERO EMANUEL ALVAREZ PENAGOS LAURA FERNADA FIGUEROA ANGIE LILIANA PAEZ HERNANDEZ

EJECUCIÓN DE LA AUDITORIA

La oficina Coordinadora del Control interno en el marco de sus competencias legales y en cumplimiento al Plan anual de Auditorías Internas, realiza Evaluación de la Seguridad Tecnológica del nuevo Portal Web Institucional de la Cámara de Representantes. Para lo anterior se utilizaron las herramientas de análisis de seguridad OpenVAS, Nmap TCP, Nmap UDP, Nuclei, OWASP ZAP y SSLyze.

La evaluación se realizó mediante revisión documental de los informes técnicos generados por las herramientas de escaneo automatizado, los cuales se adjuntan al presente informe.

Se efectuó un análisis comparativo entre los resultados obtenidos con cada herramienta, consolidando los hallazgos conforme a su severidad, impacto potencial y probabilidad de explotación.

RESULTADOS GENERALES

Consolidado de herramientas

Herramienta	Resultado
Nmap TCP	Sin vulnerabilidades críticas; pocos puertos abiertos.
Nmap UDP	Sin servicios UDP expuestos.
OpenVAS	2 vulnerabilidades medias y 1 baja.
OWASP ZAP	Hallazgos asociados principalmente al hardening de la aplicación web.
SSLyze	Sin vulnerabilidades SSL/TLS.
Nuclei	No encontró vulnerabilidades conocidas.

Estado general

En general se identificó una infraestructura tecnológica con adecuados controles de seguridad.

No fueron encontradas vulnerabilidades críticas como vulnerabilidades explotables de alta severidad en infraestructura; certificados inseguros; protocolos criptográficos obsoletos; vulnerabilidades Heartbleed; ROBOT Attack; CCS Injection.

Análisis de los Resultados

No. 1. Fortalezas en la infraestructura tecnológica

Condición

Los resultados obtenidos mediante Nmap, SSLyze y Nuclei evidencian que la infraestructura presenta una reducida superficie de exposición, que los protocolos criptográficos se encuentran actualizados, que no existen vulnerabilidades críticas, el certificado digital es válido, únicamente permanecen habilitados TLS 1.2 y TLS 1.3 y no se identificaron vulnerabilidades conocidas de alto impacto.

Criterio: ISO 27001, Controles tecnológicos del MSPI, NIST CSF

Conclusión: La infraestructura tecnológica demuestra un adecuado nivel de madurez en materia de seguridad perimetral y protección de comunicaciones.

Riesgo: Bajo.

No. 2. Exposición de configuraciones susceptibles de fortalecimiento

Condición

OpenVAS identificó una posible exposición del archivo web.config, además, una susceptibilidad teórica al ataque BREACH; y una divulgación mediante TCP Timestamp.

OWASP ZAP identificó bibliotecas JavaScript desactualizadas, ausencia de mecanismos Anti-CSRF, políticas CSP permisivas, ausencia de Subresource Integrity y oportunidades de mejora en encabezados HTTP.

Criterio: OWASP Top 10, ISO 27002, MSPI.

Causas: Las configuraciones obedecen principalmente a criterios de operación y compatibilidad de la plataforma, así como a la necesidad de fortalecer el proceso de endurecimiento (hardening) de la infraestructura y de la aplicación web.

Efecto: Aunque no representan una vulnerabilidad crítica, estas configuraciones incrementan la superficie potencial de ataque y podrían facilitar actividades de reconocimiento, explotación de componentes desactualizados o ataques contra la capa de aplicación si no son gestionadas oportunamente.

Riesgo: Medio.

No. 3. Gestión de componentes de terceros

Condición

OWASP ZAP detectó versiones de bibliotecas JavaScript susceptibles de actualización.

Consecuencias

Podrían presentarse vulnerabilidades futuras si no existe un adecuado proceso de gestión de dependencias.

Análisis Integral

Los resultados muestran una situación consistente entre todas las herramientas.

Las herramientas OpenVAS y OWASP ZAP identifican oportunidades de mejora relacionadas con configuraciones y componentes de la aplicación, Nmap, SSLyze y Nuclei evidencian que la infraestructura base presenta un adecuado nivel de protección.

En términos generales, no se identificaron indicadores que evidencien compromiso de servidores, presencia de software malicioso (malware), explotación activa de vulnerabilidades, exposición de servicios inseguros ni vulnerabilidades críticas que representen un riesgo significativo para la infraestructura tecnológica evaluada. Las observaciones identificadas corresponden principalmente a oportunidades de mejora relacionadas con el fortalecimiento de las configuraciones de seguridad (hardening), la actualización tecnológica de los activos y la implementación de acciones orientadas al mejoramiento continuo de la postura de ciberseguridad de la entidad.

Evaluación del Riesgo

Riesgo	Valoración
Confidencialidad	Bajo
Integridad	Bajo
Disponibilidad	Bajo
Riesgo tecnológico global	Bajo

CONCLUSIÓN DE AUDITORÍA

Como resultado de la evaluación realizada a los informes de seguridad correspondientes al portal institucional **www.camara.gov.co**, se concluye que la infraestructura tecnológica presenta una **postura de seguridad favorable**, sustentada en la implementación de controles adecuados para la protección de las comunicaciones, la gestión de certificados digitales, la restricción de servicios expuestos y la adopción de configuraciones criptográficas acordes con las buenas prácticas internacionales.

Las herramientas utilizadas no identificaron vulnerabilidades críticas ni evidencias de explotación activa. Los hallazgos detectados se concentran principalmente en aspectos de fortalecimiento de la configuración de la aplicación web, actualización de componentes de terceros y endurecimiento de controles de seguridad, sin que ello represente un riesgo inmediato para la continuidad de la operación del portal institucional.

En consecuencia, el nivel de riesgo residual se considera **bajo**, condicionado a que la entidad mantenga un proceso continuo de gestión de vulnerabilidades, actualización tecnológica y monitoreo permanente.

RECOMENDACIONES

1. Actualizar las bibliotecas JavaScript identificadas como susceptibles de mejora y establecer un procedimiento formal para la gestión de dependencias de software.
2. Implementar mecanismos de protección contra ataques **Cross-Site Request Forgery (CSRF)** en todos los formularios que procesen información sensible o requieran autenticación.
3. Fortalecer la **Content Security Policy (CSP)**, restringiendo el uso de directivas permisivas (unsafe-inline, unsafe-eval) y limitando el empleo de comodines, cuando la arquitectura de la aplicación lo permita.
4. Verificar y restringir el acceso a archivos de configuración, como web.config, para evitar la exposición de información técnica del servidor.
5. Revisar la necesidad operativa del puerto TCP 81 y limitar su acceso únicamente a redes autorizadas, si corresponde.
6. Habilitar **OCSP Stapling** y revisar periódicamente la configuración SSL/TLS para mantener el cumplimiento de los estándares criptográficos vigentes.
7. Fortalecer las cabeceras HTTP de seguridad, implementar **Subresource Integrity (SRI)** en recursos externos y revisar la configuración **CORS** conforme a las recomendaciones de OWASP.
8. Consolidar un **Programa Institucional de Gestión de Vulnerabilidades**, que incluya escaneos periódicos, pruebas de penetración, seguimiento a los planes de remediación e indicadores de eficacia, articulado con el MSPI y el Sistema de Control Interno.

9. Incorporar los hallazgos y acciones de mejora en el **Plan de Tratamiento de Riesgos de Seguridad Digital** y en el **Plan de Mejoramiento Institucional**, definiendo responsables, plazos e indicadores de seguimiento.

Para constancia se firma en Bogotá D.C., a los veintiocho (28) días del mes de julio del año 2026.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**
LUIS EDUARDO VELASQUEZ	COORDINADOR OFICINA COORDINADORA DEL CONTROL INTERNO	
ALVARO ERNESTO OSPINA RAMÍREZ	PROFESIONAL UNIVERSITARIO OCCI	
NIDIA C HERNANDEZ BAQUERO	PROFESIONAL UNIVERSITARIO OCCI	
LAURA FERNANDA FIGUEROA	AUDITOR	
EMANUEL ALVAREZ PENAGOS	AUDITOR	
ANGIE LILIANA PAEZ HERNANDEZ	APOYO	