

Diseño de un procedimiento formal de gestión de vulnerabilidades técnicas para los
sistemas de información de la CAR

Diego Contreras y Jeferson Benitez

Universidad Piloto de Colombia

Especialización en Seguridad Informática

Ing. Helen Nahir Barbosa Hurtado

Bogotá D.C, Colombia

Tabla de contenido

Introducción	5
Planteamiento de Problema.....	6
Pregunta Problema	8
Justificación	9
Objetivos	10
Objetivos Específicos	10
Hipótesis	11
Hipótesis de investigación.....	11
Hipótesis Nula	11
Variables	11
Variable Independiente.....	12
Variable Dependiente	12
Alcance y limitaciones.....	12
Marco Teórico.....	13
Norma ISO/IEC 27001	13
Control 8.8 – Gestión de vulnerabilidades técnicas	14
Ciclo de gestión de vulnerabilidades técnicas	14
Pruebas de seguridad dinámica (DAST)	15
Pruebas de seguridad estática (SAST).....	15
OWASP Top 10.....	16
CVSS – Common Vulnerability Scoring System.....	16
MSPI y Guía No. 5 de MinTIC	17
Monitoreo y periodicidad del escaneo de vulnerabilidades	18
ISO/IEC 27005 – Gestión de riesgos de seguridad de la información	19
Sistema Integrado de Gestión y normas complementarias.....	19
Marco Referencial.....	20
Corporación Autónoma Regional de Cundinamarca (CAR).....	20
Estructura organizacional de la CAR	22
Sistema Integrado de Gestión Pública de la CAR (SIGESPU)	25
Diseño Metodológico.....	27
Tipo de investigación	27
Desarrollo del Proyecto	27

Fase 1. Definición de la metodología, alcance y criterios técnicos	28
Metodología de evaluación	28
Alcance técnico	30
Roles	31
Periodicidad	32
Criterios de priorización	33
Mecanismos de reporte	34
Fase 2. Documentación del procedimiento	36
Código del procedimiento dentro del SIGESPU	38
Objetivo del procedimiento.....	42
Alcance del procedimiento	43
Definiciones del procedimiento	43
Responsable	45
Responsabilidades.....	45
Generalidades.....	46
Control de cambios	49
GGD-PR-XX-GI-01 (Guía de Priorización de Sistemas de Información)	50
GGD-PR-XX-FR-01 (Ficha Técnica de Configuración de Escaneo).....	51
GGD-PR-XX-FR-02 (Formato de Informe de Resultados de Pruebas de Seguridad)	
.....	52
Fase 3. Validación de la aplicabilidad del procedimiento	53
Consolidación en el Formato de Informe.....	77
Resultados	79
Resultados por objetivo específico	80
Objetivo 1 Definición de la metodología, alcance y criterios técnicos.....	80
Objetivo 2 Documentación del procedimiento formal.....	81
Objetivo 3 Validación de la aplicabilidad mediante un piloto.....	81
Contraste con la hipótesis.....	82
Cumplimiento del objetivo general	83
Conclusiones y Recomendación	84
Referencias.....	87
Anexos	91
Anexo A.....	91
Anexo B.....	100

Anexo C.....	104
Anexo D.....	107
Anexo E.....	109
Anexo F.....	113
Anexo G.....	161
Anexo H.....	170

Introducción

La Corporación Autónoma Regional de Cundinamarca (CAR) soporta sus procesos misionales en múltiples sistemas de información expuestos a internet, pero no cuenta con un procedimiento formal y documentado de gestión de vulnerabilidades técnicas. Esta situación representa un vacío frente al control 8.8 de la norma ISO/IEC 27001:2022, requisito auditable dentro del Sistema de Gestión de Seguridad de la Información, y expone a la entidad al riesgo de que vulnerabilidades no gestionadas sean explotadas por terceros.

El presente proyecto propone el diseño de un procedimiento formal que permita a la entidad identificar, evaluar, priorizar y reportar de manera sistemática las vulnerabilidades técnicas de sus sistemas de información, tomando como referentes el control 8.8 de ISO/IEC 27001:2022, la guía OWASP Web Security Testing Guide, el sistema de puntuación CVSS y los lineamientos del MSPI de MinTIC. Su aplicabilidad será validada mediante un piloto de pruebas de seguridad dinámica (DAST), ejecutado con la herramienta Tenable Web Application Scanning (WAS) en modalidad no autenticada sobre 25 sistemas de información seleccionados bajo ciertos criterios técnicos, cuyos resultados se consolidarán en un informe dirigido al equipo responsable de los sistemas de información de la CAR.

Planteamiento de Problema

La CAR Cundinamarca administra procesos misionales a través de múltiples sistemas de información expuestos a Internet y de interés para la ciudadanía. Actualmente la entidad no cuenta con un procedimiento formal y documentado de gestión de vulnerabilidades técnicas, por lo que las actividades relacionadas con la identificación y tratamiento de estas vulnerabilidades se han manejado de forma reactiva, dependiendo de la contratación de terceros y sin una metodología institucionalizada que defina roles, periodicidad, criterios de priorización, herramientas a utilizar y flujos de reporte.

Esta ausencia de un procedimiento formal es crítica frente al control 8.8 (Gestión de vulnerabilidades técnicas) de la norma ISO/IEC 27001:2022, el cual exige a las organizaciones contar con un proceso estructurado, repetible y auditable para identificar, evaluar y tratar oportunamente las vulnerabilidades de sus activos de información. La dependencia actual de servicios externos, sin un procedimiento propio que respalde y oriente dicha contratación, genera dificultad para demostrar cumplimiento ante auditorías del Sistema de Gestión de Seguridad de la Información y expone a la entidad al riesgo de que vulnerabilidades no gestionadas de forma sistemática sean explotadas por terceros, comprometiendo la confidencialidad, integridad y/o disponibilidad de la información institucional y de los ciudadanos que interactúan con dichos sistemas.

Para atender esta necesidad, el presente proyecto propone el diseño de un procedimiento formal que permita a la CAR identificar, evaluar, priorizar y reportar de manera sistemática las vulnerabilidades técnicas presentes en sus sistemas de información expuestos a internet, formalizando así un proceso hoy inexistente en la entidad. Se propone validar el procedimiento mediante un piloto de pruebas de seguridad dinámica (DAST), ejecutado con la herramienta

Tenable Web Application Scanning (WAS) sobre 25 sistemas de información seleccionados bajo ciertos criterios técnicos, en modalidad no autenticada, es decir sobre la superficie expuesta a Internet. El reporte de las vulnerabilidades se materializará mediante un informe dirigido al equipo responsable de los sistemas de información, el cual consolidará los hallazgos clasificados por severidad y tipo, junto con las recomendaciones de remediación priorizadas, sirviendo como insumo para su posterior tratamiento por parte de dicho equipo.

Pregunta Problema

¿Cómo diseñar un procedimiento formal de gestión de vulnerabilidades técnicas para los sistemas de información de la CAR, alineado al control 8.8 de la norma ISO/IEC 27001:2022, que permita a la entidad identificar, evaluar, priorizar y reportar de manera sistemática dichas vulnerabilidades?

Justificación

La CAR, al no contar con un procedimiento formal de gestión de vulnerabilidades técnicas, enfrenta un vacío frente al control 8.8 (Gestión de vulnerabilidades técnicas) de la norma ISO/IEC 27001:2022, requisito verificable en las auditorías del Sistema de Gestión de Seguridad de la Información (SGSI). Diseñar este procedimiento permite formalizar un proceso que actualmente no existe documentado en la entidad, reduciendo la dependencia de contrataciones externas puntuales y sentando una base metodológica propia, reutilizable y escalable a otros activos de información en ciclos posteriores. Adicionalmente, contar con un procedimiento documentado y alineado a dicho control brinda a la CAR evidencia objetiva de cumplimiento ante auditorías internas y externas, reduciendo el riesgo de observaciones o no conformidades dentro del SGSI.

Desde la perspectiva de seguridad de la información, la gestión sistemática de vulnerabilidades técnicas disminuye la ventana de exposición ante posibles ataques, protegiendo la confidencialidad, integridad y disponibilidad de la información institucional y de los ciudadanos que interactúan con los sistemas de información de la entidad.

Objetivos

Diseñar un procedimiento formal de gestión de vulnerabilidades técnicas para los sistemas de información de la CAR, alineado al control 8.8 de la norma ISO/IEC 27001:2022, que permita a la entidad identificar, evaluar, priorizar y reportar de manera sistemática dichas vulnerabilidades.

Objetivos Específicos

- Definir la metodología, alcance y criterios técnicos del procedimiento de gestión de vulnerabilidades técnicas (roles, periodicidad, criterios de priorización y mecanismos de reporte), tomando como referencia el control 8.8 de ISO/IEC 27001:2022, buenas prácticas como el OWASP Testing Guide, y marcos de clasificación de riesgo como el OWASP Top 10.
- Documentar el procedimiento formal de gestión de vulnerabilidades técnicas para la CAR, consolidando las fuentes, guías y el paso a paso definido para su aplicación, conforme a los lineamientos del Sistema Integrado de Gestión Pública (SIGESPU) de la entidad.
- Validar la aplicabilidad del procedimiento diseñado mediante la ejecución de un piloto de pruebas de seguridad dinámica (DAST) con la herramienta Tenable Web Application Scanning (WAS), en modalidad no autenticada, sobre 25 sistemas de información seleccionados bajo criterios técnicos, clasificando los hallazgos según severidad y tipo y consolidándolos en un informe con recomendaciones de remediación priorizadas.

Hipótesis

Hipótesis de investigación

El diseño de un procedimiento formal de gestión de vulnerabilidades técnicas, alineado al control 8.8 de la norma ISO/IEC 27001:2022, **permitirá** identificar, evaluar, priorizar y reportar sistemáticamente las vulnerabilidades técnicas en al menos el 90% de los sistemas de información evaluados en el piloto, clasificando los hallazgos conforme al sistema CVSS v3.1 y a la categorización OWASP Top 10:2021.

Hipótesis Nula

El diseño de un procedimiento formal de gestión de vulnerabilidades técnicas, alineado al control 8.8 de la norma ISO/IEC 27001:2022, **no permitirá** identificar, evaluar, priorizar y reportar sistemáticamente las vulnerabilidades técnicas en al menos el 90% de los sistemas de información evaluados en el piloto, ni clasificar los hallazgos conforme al sistema CVSS v3.1 y la categorización OWASP Top 10:2021.

Variables

Variable Independiente

Procedimiento formal de gestión de vulnerabilidades técnicas, alineado al control 8.8 de la norma ISO/IEC 27001:2022.

Variable Dependiente

Nivel de aplicabilidad del procedimiento, evidenciado en la capacidad de identificar, evaluar, priorizar y reportar de manera sistemática las vulnerabilidades técnicas de los sistemas de información de la CAR.

Alcance y limitaciones

El presente proyecto abarca el diseño de un procedimiento formal de gestión de vulnerabilidades técnicas para los sistemas de información de la CAR, cubriendo las etapas de identificación, evaluación, priorización y reporte, conforme al control 8.8 de ISO/IEC 27001:2022. La validación práctica del procedimiento se realiza mediante un piloto de pruebas de seguridad dinámica (DAST) con la herramienta Tenable Web Application Scanning (WAS), ejecutado en modalidad no autenticada sobre 25 sistemas de información seleccionados bajo criterios técnicos.

Las etapas de remediación y verificación de las vulnerabilidades identificadas no forman parte de los entregables del presente proyecto. El procedimiento diseñado deja definidos los roles, plazos y criterios para su ejecución, pero dicha ejecución es responsabilidad del equipo técnico de desarrollo y administración de los sistemas de información de la CAR, dado que

implica cambios sobre los sistemas y sus tiempos de implementación exceden el horizonte del proyecto.

Asimismo, el proyecto se limita a los sistemas de información de la entidad, sin extenderse a otros activos de información como redes o bases de datos, y el piloto se restringe a pruebas no autenticadas sobre la superficie expuesta a Internet de los sistemas evaluados, quedando las pruebas autenticadas y la ampliación a los 23 sistemas restantes (sobre un universo total de 48 sistemas de información) como líneas de trabajo para ciclos posteriores.

Marco Teórico

Norma ISO/IEC 27001

ISO/IEC 27001 es el estándar internacional más reconocido para los Sistemas de Gestión de Seguridad de la Información (SGSI). Este documento especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización, e incluye los requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de cada entidad (**International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2022a**). Los requisitos establecidos son de carácter genérico y aplicables a todas las organizaciones sin importar su tipo, tamaño o naturaleza, y no es aceptable excluir ninguno de los requisitos especificados en las cláusulas 4 a 10 cuando una organización declara conformidad con la norma (**ISO/IEC, 2022a**).

Un SGSI implementado conforme a esta norma preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos, y brinda confianza a las partes interesadas de que los riesgos se gestionan adecuadamente **(ISO/IEC, 2022a)**. La norma se complementa con ISO/IEC 27002:2022, la cual desarrolla en detalle los controles de seguridad de la información referenciados en el Anexo A, describiendo su propósito y directrices de implementación; dichos controles incluyen políticas, reglas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware **(ISO/IEC, 2022b)**. Es dentro de los controles tecnológicos de este catálogo donde se ubica el control 8.8, objeto central del presente proyecto.

Control 8.8 – Gestión de vulnerabilidades técnicas

El control 8.8 de ISO/IEC 27002:2022 establece que las organizaciones deben obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización a tales vulnerabilidades y tomar las medidas apropiadas para prevenir su explotación **(ISO/IEC, 2022b)**. El cumplimiento de este control exige a las organizaciones contar con un proceso estructurado y repetible, con roles y responsabilidades definidos, soportado en actividades técnicas periódicas y documentadas de identificación y evaluación de vulnerabilidades **(ISO/IEC, 2022b)**.

Ciclo de gestión de vulnerabilidades técnicas

En la literatura técnica de referencia, la gestión de vulnerabilidades se describe como un ciclo de vida continuo y no como una actividad puntual. El National Institute of Standards and Technology, en su publicación especial SP 800-40 Rev. 4, describe el ciclo de vida de la gestión de vulnerabilidades de software como un proceso que comprende conocer cuándo nuevas

vulnerabilidades afectan los activos de la organización, planificar la respuesta al riesgo evaluando el riesgo de cada vulnerabilidad identificada, seleccionando el tipo de respuesta y determinando la mejor forma de remediarlo y ejecutar dicha respuesta, incluyendo su preparación, implementación, verificación y monitoreo continuo (**National Institute of Standards and Technology [NIST], 2022**). Asimismo, el NIST plantea cuatro tipos de respuesta frente al riesgo derivado de vulnerabilidades de software: aceptar, mitigar, transferir y evitar (**NIST, 2022**). Este enfoque cíclico constituye el referente conceptual del presente proyecto, cuyo procedimiento aborda las etapas de identificación, evaluación, priorización y reporte de vulnerabilidades, dejando las etapas de remediación y verificación como responsabilidad del equipo técnico de los sistemas de información, a partir del informe generado.

Pruebas de seguridad dinámica (DAST)

Las pruebas de seguridad dinámica (Dynamic Application Security Testing, DAST) evalúan una aplicación en tiempo de ejecución, sin acceso a su código fuente, simulando el comportamiento de un atacante externo. Para estructurar este tipo de pruebas de manera sistemática, la fundación Open Web Application Security Project desarrolló la OWASP Web Security Testing Guide, un marco de referencia que proporciona una metodología consistente, repetible y definida para las pruebas de seguridad de aplicaciones web, organizando los escenarios de prueba en categorías identificadas y trazables entre versiones del documento (**Open Web Application Security Project [OWASP], 2020**).

Pruebas de seguridad estática (SAST)

Frente al enfoque dinámico, existe también la prueba de seguridad estática (Static Application Security Testing, SAST), un método de caja blanca que analiza el código fuente de

la aplicación para identificar vulnerabilidades sin necesidad de ejecutarla. Si bien ambos enfoques se consideran complementarios dentro de un programa integral de seguridad de aplicaciones, la evidencia empírica reciente confirma que cada uno presenta fortalezas distintas: SAST resulta particularmente efectivo para la detección de hallazgos de severidad alta mediante el análisis detallado del código, mientras que DAST evidencia un mejor desempeño en la identificación de determinadas categorías de vulnerabilidades explotables desde una perspectiva externa (Qadir et al., 2025).

OWASP Top 10

La fundación OWASP publica también el OWASP Top 10, un listado de los riesgos más críticos identificados en aplicaciones web, actualizado periódicamente a partir de datos recopilados de la industria (OWASP, 2021). La versión OWASP Top 10 – 2021 es el referente utilizado en el presente proyecto para categorizar, según su nivel de riesgo, las pruebas técnicas DAST ejecutadas durante el piloto mediante la herramienta Tenable Web Application Scanning (WAS).

CVSS – Common Vulnerability Scoring System

Para evaluar de forma estandarizada la severidad de las vulnerabilidades identificadas se emplea el Common Vulnerability Scoring System (CVSS), un marco abierto, propiedad de FIRST.Org, que proporciona una metodología de puntuación de vulnerabilidades estandarizada e independiente de fabricantes y plataformas (FIRST.Org, Inc., 2019). El CVSS está compuesto por tres grupos de métricas: Base, Temporal y Ambiental, donde la puntuación Base refleja la severidad intrínseca de la vulnerabilidad, constante en el tiempo y común a todos los entornos, mientras que las métricas Temporales la ajustan según factores cambiantes, como la

disponibilidad de código de explotación, y las métricas Ambientales la adaptan al entorno de cómputo específico de la organización **(FIRST.Org, Inc., 2019)**.

Cabe precisar que la especificación de la versión 3.1 aclaró que la puntuación CVSS refleja exclusivamente la gravedad técnica intrínseca de la vulnerabilidad, por lo que resulta insuficiente como criterio único para dimensionar el riesgo real que esta representa para una organización **(Instituto Nacional de Ciberseguridad [INCIBE], 2019)**. En consecuencia, la puntuación base debe complementarse con un análisis contextual que aproveche las métricas temporales y ambientales, junto con factores externos no contemplados por el CVSS, como la exposición y la amenaza. Esta distinción es relevante para el proyecto, dado que el puntaje CVSS se usará como criterio técnico de evaluación y priorización, complementado por el contexto propio de los sistemas de información de la CAR.

MSPI y Guía No. 5 de MinTIC

En el contexto de las entidades públicas colombianas, el Ministerio de Tecnologías de la Información y las Comunicaciones estableció el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital, adoptado mediante la Resolución 500 de 2021. Mediante la Resolución 2277 de 2025 se actualizó el Anexo 1 de dicha resolución, alineando el modelo con la norma ISO/IEC 27001:2022 y derogando los lineamientos, guías y estándares anteriores contrarios a esta norma técnica **(Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2025)**. El MSPI actualizado incorpora lineamientos para la protección de los activos de información del Estado, estableciendo controles físicos, lógicos y administrativos que permiten a las entidades públicas gestionar de forma más eficaz sus riesgos tecnológicos **(MinTIC, 2025)**, e incluye dentro de sus

lineamientos la identificación, inventario y clasificación de los activos de información, insumo fundamental para la priorización de los sistemas sobre los cuales se aplican los controles de seguridad (**MinTIC, 2025**).

Complementariamente, MinTIC publicó la Guía No. 5 – Gestión y Clasificación de Activos de Información, la cual establece la metodología para valorar los activos de información de una entidad según los atributos de Confidencialidad, Integridad y Disponibilidad, asignando a cada uno un nivel de Alta, Media o Baja, con el fin de determinar su criticidad global (**MinTIC, 2016**). Esta metodología constituye el referente directo adoptado en la Guía de Priorización de Sistemas de Información elaborada como parte del presente proyecto, la cual combina dicha valoración con criterios adicionales de exposición a Internet y volumen de usuarios para calcular el orden de evaluación de los sistemas en cada ciclo del procedimiento.

Este marco es especialmente relevante para el presente proyecto, dado que la CAR, como entidad pública colombiana, está sujeta a los lineamientos del MSPI, cuya alineación con la norma ISO/IEC 27001:2022 brinda respaldo institucional y normativo al procedimiento de gestión de vulnerabilidades técnicas propuesto.

Monitoreo y periodicidad del escaneo de vulnerabilidades

Además del ciclo de vida general de gestión de vulnerabilidades, el NIST establece en su publicación Security and Privacy Controls for Information Systems and Organizations el control RA-5 (Vulnerability Monitoring and Scanning), el cual exige a las organizaciones monitorear y escanear sus sistemas en busca de vulnerabilidades con una frecuencia definida por la propia organización, en función de la categorización de seguridad y el nivel de riesgo de sus activos (**National Institute of Standards and Technology [NIST], 2020**). A diferencia de otros

estándares de la industria que prescriben frecuencias fijas para contextos específicos, el NIST delega esta decisión a cada organización, reconociendo que la periodicidad óptima depende de factores como la criticidad de los sistemas, la capacidad técnica disponible y el contexto operativo particular de cada entidad.

ISO/IEC 27005 – Gestión de riesgos de seguridad de la información

La norma ISO/IEC 27005:2022 proporciona los lineamientos para la gestión de riesgos de seguridad de la información dentro de un SGSI, complementando los requisitos generales de ISO/IEC 27001:2022. Esta versión de la norma incorporó, junto a los enfoques cualitativo y cuantitativo ya existentes, un tercer enfoque semicuantitativo de valoración de riesgos, en el cual algunos aspectos como el nivel de criticidad de un activo se valoran mediante escalas cualitativas (por ejemplo, Alta, Media o Baja) a las que se asigna un valor numérico, permitiendo combinar y comparar objetivamente distintos criterios de riesgo dentro de un mismo puntaje (International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2022c). Este enfoque semicuantitativo es el adoptado en la Guía de Priorización de Sistemas de Información del presente proyecto, donde el nivel de criticidad, la exposición a Internet y el volumen de usuarios de cada sistema se valoran cualitativamente y se combinan en un puntaje numérico único que determina el orden de priorización.

Sistema Integrado de Gestión y normas complementarias

Además de ISO/IEC 27001:2022, existen otras normas de sistemas de gestión con las que las organizaciones suelen integrar sus procesos institucionales bajo un enfoque común. La norma

ISO 9001 establece los requisitos para un Sistema de Gestión de la Calidad, orientado a la mejora continua de los procesos y la satisfacción del usuario; la norma **ISO 14001** establece los requisitos para un Sistema de Gestión Ambiental, orientado a la gestión de los impactos ambientales de la organización; y la norma **ISO 45001** establece los requisitos para un Sistema de Gestión de Seguridad y Salud en el Trabajo, orientado a la prevención de lesiones y enfermedades laborales. Estas tres normas, junto con ISO/IEC 27001:2022, comparten una estructura de alto nivel común (Anexo SL), lo cual facilita su integración bajo un único sistema de gestión institucional, tal como ocurre en el Sistema Integrado de Gestión Pública (SIGESPU) de la CAR, descrito en el Marco Referencial del presente proyecto.

Marco Referencial

Corporación Autónoma Regional de Cundinamarca (CAR)

La Corporación Autónoma Regional de Cundinamarca (CAR) es un ente corporativo de carácter público, creado por la ley, integrado por las entidades territoriales que por sus características constituyen geográficamente un mismo ecosistema o conforman una unidad geopolítica, biogeográfica o hidrogeográfica, dotado de personería jurídica, autonomía administrativa y financiera y patrimonio propio e independiente, encargado por la ley de administrar, dentro del área de su jurisdicción, el medio ambiente y los recursos naturales renovables y propender por su desarrollo sostenible, de conformidad con las disposiciones legales y las políticas del Ministerio de Ambiente y Desarrollo Sostenible (Congreso de Colombia, 1993, art. 23).

La entidad tiene su origen en la Corporación Autónoma Regional de la Sabana de Bogotá y de los Valles de Ubaté y Chiquinquirá, creada mediante la Ley 3ª del 31 de enero de 1961. Posteriormente, la Ley 62 de 1983 modificó su denominación a Corporación Autónoma Regional de las Cuencas de los Ríos Bogotá, Ubaté y Suárez, hasta que la Ley 99 de 1993 estableció su nombre actual, Corporación Autónoma Regional de Cundinamarca (CAR) (Congreso de Colombia, 1993). Actualmente, la entidad tiene la responsabilidad de proteger el medio ambiente en un territorio de 18.706,4 km², que comprende 104 municipios: 98 pertenecientes al departamento de Cundinamarca, 6 al departamento de Boyacá y la zona rural del Distrito Capital de Bogotá D.C. (Corporación Autónoma Regional de Cundinamarca [CAR], s.f.-a). Su jurisdicción está integrada por nueve cuencas hidrográficas de primer orden, correspondientes a los ríos Bogotá, Negro, Sumapaz, Magdalena, Ubaté-Suárez, Minero, Machetá, Blanco y Gachetá, y atiende una población cercana a los diez millones de habitantes al incluir a la capital del país (CAR, s.f.-a).

Su misión institucional es **"ejercer como máxima autoridad ambiental en su jurisdicción, ejecutando políticas, planes, programas y proyectos ambientales, a través de la construcción de tejido social, para contribuir al desarrollo sostenible y armónico de la región"** (CAR, s.f.-b). Sus funciones, establecidas en la Ley 99 de 1993, incluyen la ejecución de las políticas, planes y programas nacionales y regionales en materia ambiental, el ejercicio de la función de máxima autoridad ambiental en el área de su jurisdicción, el otorgamiento de concesiones, permisos, autorizaciones y licencias ambientales, y el recaudo de contribuciones, tasas y multas por el uso y aprovechamiento de los recursos naturales renovables (CAR, s.f.-b).

Para el cumplimiento de sus funciones misionales y la atención a la ciudadanía, la CAR soporta sus procesos en múltiples sistemas de información, varios de ellos expuestos a Internet,

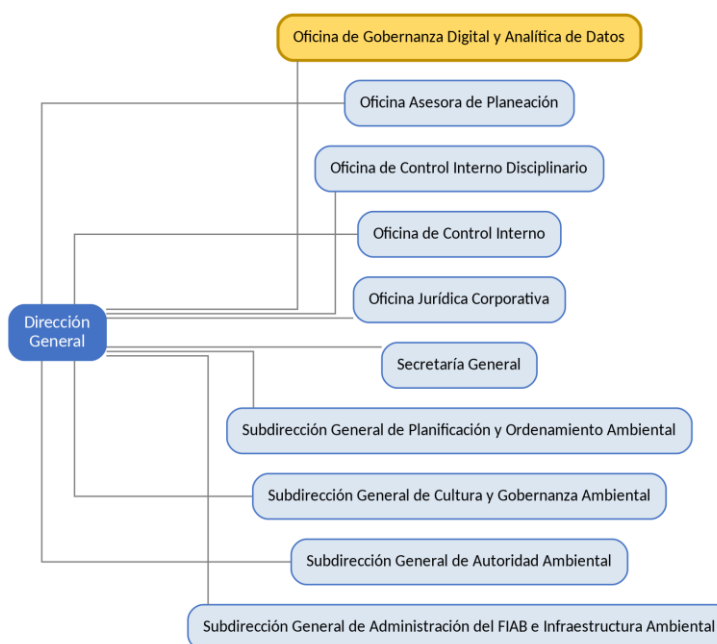
mediante los cuales gestiona trámites ambientales, permisos, licencias y servicios de interés público. Como entidad pública del orden nacional, la CAR está sujeta a los lineamientos de la Política de Gobierno Digital y, en particular, al Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, actualizado mediante la Resolución 2277 de 2025 y alineado con la norma ISO/IEC 27001:2022 (MinTIC, 2025). Es en este contexto institucional y normativo donde se desarrolla el presente proyecto, orientado al diseño de un procedimiento formal de gestión de vulnerabilidades técnicas para los sistemas de información de la entidad.

Estructura organizacional de la CAR

La estructura interna de la CAR está determinada por el Acuerdo No. 27 del 5 de septiembre de 2025, expedido por el Consejo Directivo de la Corporación, mediante el cual se establece la estructura orgánica y las funciones de las dependencias que la conforman (Consejo Directivo CAR, 2025). Bajo la Dirección General se ubican diez dependencias de primer nivel: la Oficina de Gobernanza Digital y Analítica de Datos, la Oficina Asesora de Planeación, la Oficina de Control Interno Disciplinario, la Oficina de Control Interno, la Oficina Jurídica Corporativa, la Secretaría General y cuatro subdirecciones generales orientadas a la gestión ambiental (Consejo Directivo CAR, 2025). La Figura 1 presenta la ubicación de estas dependencias dentro de la estructura organizacional de la entidad.

Figura 1

Estructura organizacional de la Corporación Autónoma Regional de Cundinamarca (CAR)



Nota. elaboración propia, con base en el Acuerdo No. 27 de 2025, "Por el cual se determina la estructura interna de la Corporación Autónoma Regional de Cundinamarca, se establecen las funciones y responsabilidades de las dependencias que la conforman y se dictan otras disposiciones" (Consejo Directivo CAR, 2025).

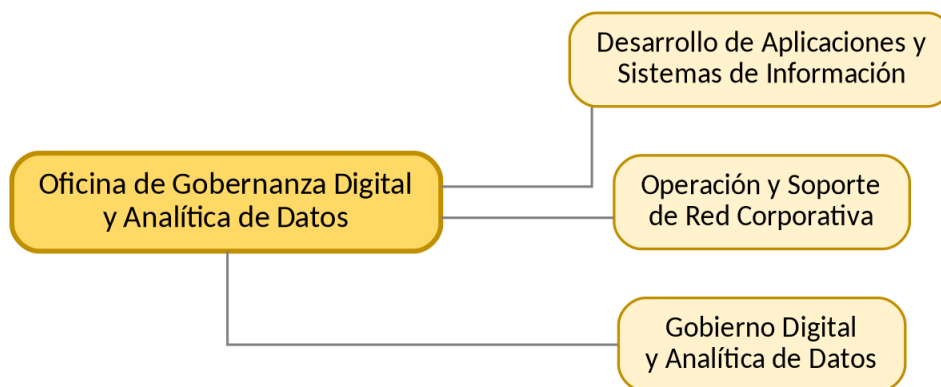
El presente proyecto se enmarca en la Oficina de Gobernanza Digital y Analítica de Datos, dependencia de primer nivel adscrita directamente a la Dirección General, responsable de la seguridad de la información, la infraestructura tecnológica y la transformación digital de la Corporación. Según el Artículo 8 del Acuerdo No. 27 de 2025, esta oficina tiene como propósito desarrollar la gestión segura y eficiente de las tecnologías de la información, administrar la plataforma central que habilita y soporta las operaciones de la CAR, liderar la transformación digital de la entidad y generar valor misional a través de la analítica de datos, garantizando en especial la integración y el control de los sistemas de información de la Corporación (Consejo Directivo CAR, 2025). Entre sus funciones se destacan la implementación y gestión de las

políticas, controles y el modelo de seguridad y privacidad de la información para proteger los activos de información, así como la administración, operación y aseguramiento del funcionamiento de la infraestructura tecnológica y los sistemas de información de la entidad (Consejo Directivo CAR, 2025).

Internamente, la Oficina de Gobernanza Digital y Analítica de Datos se organiza en tres líneas estratégicas: Desarrollo de Aplicaciones y Sistemas de Información, Operación y Soporte de Red Corporativa, y Gobierno Digital y Analítica de Datos, esta última no debe confundirse con el nombre de la oficina que la contiene, pese a la similitud (CAR, 2026b), tal como se ilustra en la Figura 2. El presente proyecto se desarrolla en el marco de esta última línea, responsable de liderar la gobernanza digital y de datos de la entidad, dentro de la cual se ubica la gestión de vulnerabilidades técnicas de los sistemas de información.

Figura 2

Estructura interna de la Oficina de Gobernanza Digital y Analítica de Datos



Nota. elaboración propia, con base en el Plan Anual de Vacantes 2026 de la CAR (Corporación Autónoma Regional de Cundinamarca, 2026b).

Sistema Integrado de Gestión Pública de la CAR (SIGESPU)

La CAR gestiona sus procesos institucionales a través del Sistema Integrado de Gestión Pública (SIGESPU), el cual integra los requisitos del Sistema de Gestión de la Calidad (ISO 9001), el Sistema de Gestión Ambiental (ISO 14001), el Sistema de Gestión de Seguridad y Salud en el Trabajo (ISO 45001) y el Sistema de Gestión de Seguridad de la Información (ISO 27001), siendo la Oficina Asesora de Planeación la dependencia responsable de administrar la información documentada de dichos sistemas (CAR, 2026a). El SIGESPU se estructura bajo un Modelo de Operación por Procesos (MOP), entendido como un enfoque de gestión que organiza las actividades institucionales en procesos interrelacionados; estos procesos son clasificados en cuatro tipos: procesos estratégicos, procesos misionales, procesos de apoyo y procesos de evaluación.

Figura 3

Sistema Integrado de Gestión Pública CAR Cundinamarca



Nota. Tomado de Sistema Integrado de Gestión Pública [Mapa de procesos], por Corporación Autónoma Regional de Cundinamarca, 2026c (<https://www.car.gov.co/vercontenido/6>).

Dentro de los procesos estratégicos del SIGESPU se ubica el proceso "Gestión de la Gobernanza Digital", el cual pertenece a la Oficina de Gobernanza Digital y Analítica de Datos. La información documentada que se genera en el marco del SIGESPU, incluyendo manuales, caracterizaciones, procedimientos, guías, instructivos y formatos, se organiza en una estructura jerárquica de cuatro niveles y debe cumplir con los lineamientos de creación, codificación, control de cambios y publicación establecidos por la entidad. En este marco documental institucional se enmarca el procedimiento formal diseñado en el presente proyecto (CAR, 2026a).

Diseño Metodológico

Tipo de investigación

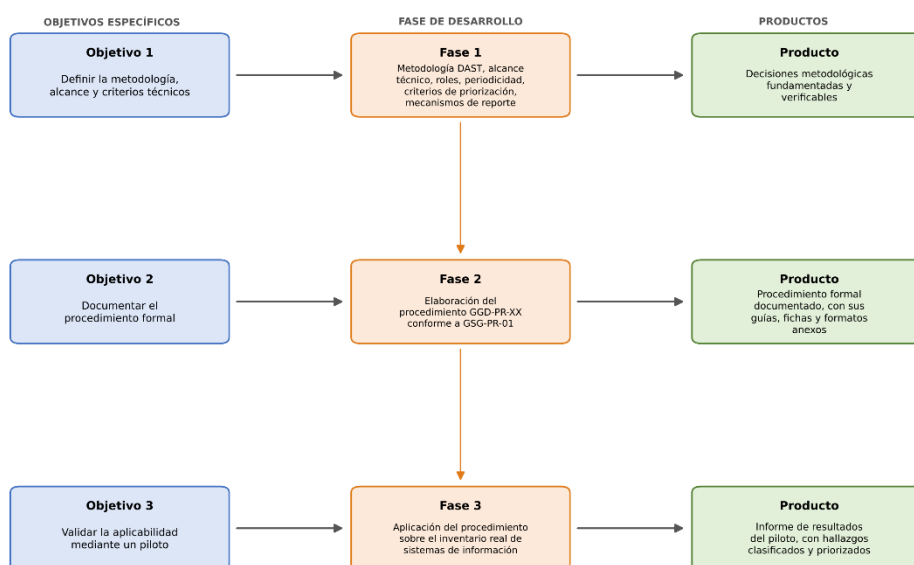
El presente proyecto se enmarca en la investigación aplicada, definida como aquella que busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector productivo, apoyándose en los hallazgos tecnológicos de la investigación básica para el enlace entre la teoría y el producto (Lozada, 2014).

Desarrollo del Proyecto

El desarrollo del proyecto se estructura en tres fases, cada una correspondiente a uno de los objetivos específicos definidos. En cada fase se describen las actividades ejecutadas y los productos documentales generados como evidencia de su cumplimiento. La Figura 4 presenta la trazabilidad metodológica del proyecto, evidenciando la correspondencia entre cada objetivo específico, la fase en que fue desarrollado y el producto que esta entregó.

Figura 4

Trazabilidad metodológica: objetivos, fases y productos



Nota. Elaboración propia.

Fase 1. Definición de la metodología, alcance y criterios técnicos

Metodología de evaluación

La selección de las pruebas de seguridad dinámica (DAST) como metodología central del procedimiento responde tanto a una decisión técnica como a una limitación operativa real de la entidad. El área de Gobierno Digital y Analítica de Datos, responsable de este procedimiento, no tiene acceso al código fuente de los sistemas de información, dado que dicho código es administrado por el área de Desarrollo de Aplicaciones y Sistemas de Información, una línea funcional distinta dentro de la misma oficina. Esta separación de responsabilidades hace que un

enfoque de pruebas de seguridad estática (SAST), que exige acceso al código fuente para su ejecución, resulte inviable dentro del alcance operativo del área responsable (**Qadir et al., 2025**).

Frente a esta limitación, el enfoque DAST resulta metodológicamente apropiado: al tratarse de una técnica de caja negra, evalúa la aplicación en tiempo de ejecución sin requerir acceso a su código fuente, simulando el comportamiento de un atacante externo (**Qadir et al., 2025**). La evidencia empírica reciente confirma, además, que SAST y DAST no son enfoques sustitutos sino complementarios: mientras SAST resulta indispensable para la detección de hallazgos de severidad alta mediante análisis detallado del código, DAST demuestra un desempeño superior en la identificación de determinadas categorías de vulnerabilidades explotables desde una perspectiva externa (**Qadir et al., 2025**). Que DAST no sustituya un análisis de código fuente es una limitación reconocida y resulta consistente con el hecho de que la ampliación a pruebas autenticadas y a otros enfoques de evaluación se plantee como línea de trabajo para ciclos posteriores del procedimiento.

La modalidad específicamente no autenticada del piloto se fundamenta en el mismo principio: la Web Security Testing Guide de OWASP plantea que las pruebas de seguridad web deben poder ejecutarse simulando de manera realista los distintos niveles de acceso con los que un atacante podría interactuar con la aplicación (**OWASP, 2020**). Al evaluar los sistemas de información de la CAR en modalidad no autenticada, el procedimiento reproduce precisamente el escenario de mayor exposición real: el de un atacante externo sin credenciales, actuando sobre la superficie de los sistemas expuestos directamente a Internet.

Alcance técnico

La separación de responsabilidades entre las áreas de Gobierno Digital y Analítica de Datos, y de Desarrollo de Aplicaciones y Sistemas de Información, determina el alcance técnico del procedimiento. Este se delimita a cuatro de las seis etapas típicas del ciclo de gestión de vulnerabilidades técnicas: identificar, evaluar, priorizar y reportar, excluyendo de manera intencional las etapas de remediación y verificación, dado que el área responsable de este procedimiento no ejecuta cambios sobre el código o la configuración de los sistemas de información, actividad que corresponde de manera exclusiva al área de Desarrollo.

Esta segregación de responsabilidades por etapa del ciclo no ocurre, entre dos dependencias distintas de la CAR, sino entre dos áreas internas de una misma oficina, lo cual permite que el procedimiento entregue como producto final un informe completo con hallazgos clasificados y recomendaciones de remediación priorizadas, sin necesidad de que el área de Gobierno Digital y Analítica de Datos ejecute directamente dichas recomendaciones.

El cierre efectivo del ciclo, correspondiente a la remediación y la verificación posterior de los hallazgos, queda así bajo la responsabilidad del área de Desarrollo, a partir del informe generado por este procedimiento.

Dado que el área de Gobierno Digital y Analítica de Datos entrega el informe sin ejecutar ni verificar directamente la remediación, el procedimiento incorpora un mecanismo de seguimiento semestral al avance del área de Desarrollo, ubicado al cierre del ciclo de ejecución. Esta decisión de diseño no responde únicamente al requisito formal de la entidad de incluir al menos un Punto de Control, sino que constituye una aplicación directa del concepto de actividades de control del Internal Control – Integrated Framework del Committee of Sponsoring Organizations of the Treadway Commission, marco de referencia internacional en el diseño de

controles organizacionales, según el cual las actividades de control son las acciones establecidas mediante políticas y procedimientos que ayudan a asegurar que las respuestas al riesgo se ejecuten de manera efectiva (COSO, 2013). Su ubicación al final del ciclo, y no en una etapa intermedia, responde a que el riesgo que se busca controlar no es la calidad de la información generada por el área de Gobierno Digital y Analítica de Datos, sino la ejecución efectiva de la remediación por parte del área de Desarrollo de Aplicaciones y Sistemas de Información: aun cuando ambas áreas pertenecen a la misma oficina (OGDAD), la ejecución de la remediación queda fuera del alcance directo del rol responsable de este procedimiento, lo que justifica el mecanismo de seguimiento como control compensatorio.

Los cuatro verbos que delimitan el alcance (identificar, evaluar, priorizar y reportar) se corresponden, a su vez, con una estructura secuencial de tres momentos: el inicio con la identificación de los sistemas de información objeto de evaluación, el desarrollo mediante la ejecución de las pruebas DAST, la evaluación y la priorización de las vulnerabilidades identificadas, y el cierre con la elaboración y entrega del informe de resultados. Esta correspondencia entre los verbos y la estructura secuencial del alcance garantiza la coherencia interna del procedimiento, evitando que se defina una acción que no tenga una etapa equivalente en su ejecución real.

Roles

Definido el alcance de lo que el procedimiento cubre y de lo que excluye, es necesario precisar quién es responsable de ejecutarlo. Esta responsabilidad se asignó a un rol específico, el Profesional Especializado en Seguridad de la Información de la Oficina de Gobernanza Digital y

Analítica de Datos (OGDAD), y no a la dependencia en su conjunto. Esta decisión se fundamenta en el control 5.2 (Roles y responsabilidades de seguridad de la información) de la norma ISO/IEC 27002:2022, el cual establece que los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización (ISO/IEC, 2022b).

Dado que las actividades del procedimiento (identificar, evaluar, priorizar y reportar vulnerabilidades técnicas) son de naturaleza eminentemente operativa y especializada, y no de carácter directivo, resulta coherente que la responsabilidad recaiga sobre el rol técnico específico encargado de ejecutarlas, y no sobre la dependencia en su totalidad. Esta asignación puntual, además, facilita la trazabilidad de cada ciclo de ejecución del procedimiento y evita la ambigüedad que resultaría de responsabilizar a una oficina completa por actividades técnicas que, en la práctica, ejecuta una sola persona con un perfil definido.

Periodicidad

Con el responsable ya definido, la siguiente decisión es con qué frecuencia debe ejecutarse el procedimiento. La ejecución anual se estableció como una decisión institucional propia, fundamentada en la disponibilidad real del licenciamiento de la herramienta Tenable Web Application Scanning (WAS) con la que cuenta la CAR. Esta decisión es consistente con el control RA-5 (Vulnerability Monitoring and Scanning) de la publicación NIST Special Publication 800-53 Revisión 5, el cual no impone una frecuencia fija de escaneo, sino que exige que esta sea definida por cada organización de acuerdo con la categorización de seguridad de sus sistemas y su nivel de riesgo (National Institute of Standards and Technology [NIST], 2020).

Bajo este criterio, la periodicidad anual constituye la frecuencia mínima operativamente viable para la entidad en el ciclo actual, sin que ello implique que dicho intervalo sea inamovible: el propio diseño del procedimiento contempla la ampliación de su cobertura y frecuencia en ciclos posteriores, conforme evolucionen las condiciones de licenciamiento y capacidad técnica de la Oficina de Gobernanza Digital y Analítica de Datos.

Criterios de priorización

Establecida la periodicidad, resta definir cómo se seleccionan los sistemas a evaluar en cada ciclo cuando no es posible cubrir la totalidad del inventario. Este criterio se diseñó combinando dos dimensiones de análisis: el nivel de criticidad del activo y su exposición real al riesgo. Para la primera dimensión, se adoptó la metodología de valoración de activos de información establecida en la Guía No. 5, Gestión y Clasificación de Activos de Información, de MinTIC, la cual califica cada sistema según sus atributos de Confidencialidad, Integridad y Disponibilidad, asignando a cada uno un nivel de Alta, Media o Baja para determinar su criticidad global (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2016). Esta valoración cualitativa por niveles es consistente con los métodos de valoración de riesgo reconocidos por la norma ISO/IEC 27005:2022, la cual admite enfoques cualitativos, cuantitativos y semicuantitativos para la estimación de las consecuencias y la probabilidad asociadas a los riesgos de seguridad de la información (ISO/IEC, 2022c).

A esta valoración de criticidad se sumaron dos criterios adicionales, propios del diseño del presente proyecto y no derivados directamente de una fuente normativa: la exposición del sistema a Internet (Sí/No) y su volumen de usuarios (Alto/Medio/Bajo). La combinación semicuantitativa de estas tres variables (criticidad, exposición y volumen de usuarios) genera un

puntaje de priorización que ordena los sistemas de mayor a menor prioridad de evaluación, permitiendo seleccionar, en estricto orden descendente, los sistemas que serán efectivamente evaluados en cada ciclo según la capacidad real disponible. Para los casos en que dos o más sistemas obtengan el mismo puntaje, la Guía de Priorización establece un criterio de desempate basado, en orden, en la exposición a Internet, el nivel de criticidad y el orden alfabético en el listado, garantizando que la selección final sea siempre objetiva y reproducible.

Este mecanismo de priorización no responde a una cifra fija de sistemas o de licenciamiento disponible, sino que se activa siempre que la totalidad de los sistemas de información de la entidad exceda la capacidad de evaluación disponible en un ciclo determinado, independientemente de la causa que genere dicha restricción. Esta formulación asegura que el procedimiento sea escalable en el tiempo, siendo igualmente aplicable si la entidad cuenta con 25, 48 o 100 sistemas de información. Este mecanismo de priorización se materializa, dentro de la secuencia del procedimiento, como una verificación previa a la ejecución de las pruebas: antes de iniciar cada ciclo, se comprueba si la totalidad de los sistemas de información puede ser evaluada o si es necesario aplicar los criterios de priorización aquí definidos.

Mecanismos de reporte

Finalmente, una vez identificados, evaluados y priorizados los sistemas y sus vulnerabilidades, el procedimiento requiere un mecanismo de reporte que traduzca los hallazgos técnicos en información útil para la toma de decisiones. Este mecanismo se diseñó combinando dos criterios técnicos de clasificación, CVSS para la severidad y OWASP Top 10 – 2021 para el tipo de riesgo, con una estructura de reporte de doble componente, gerencial y técnico, dirigida a audiencias distintas dentro de la misma cadena de remediación.

Para la severidad, los rangos de clasificación (Crítica: 9.0-10.0, Alta: 7.0-8.9, Media: 4.0-6.9, Baja: 0.1-3.9) reproducen la Tabla 14 (Qualitative Severity Rating Scale) de la especificación técnica del CVSS v3.1, publicada por el Forum of Incident Response and Security Teams (FIRST.Org, Inc., 2019). Para el tipo de vulnerabilidad, cada hallazgo se clasifica según la categoría del OWASP Top 10 – 2021 a la que corresponde, permitiendo comparar los resultados del piloto contra un esquema de riesgo reconocido internacionalmente (Open Web Application Security Project, 2021).

La decisión de estructurar el informe en dos componentes, uno gerencial, que consolida los hallazgos por sistema y nivel de severidad para la alta dirección, y uno técnico, que desagrega cada hallazgo individual con su categoría de riesgo, su puntaje CVSS y su recomendación de remediación puntual, responde a que las dos audiencias del informe requieren niveles de detalle distintos para tomar decisiones distintas: la dirección de la entidad necesita dimensionar el riesgo agregado, mientras que el equipo de Desarrollo de Aplicaciones y Sistemas de Información necesita el detalle técnico suficiente para ejecutar la remediación.

Con lo expuesto en esta fase, el procedimiento deja de plantearse como un enunciado general de gestión de vulnerabilidades técnicas y se constituye en una definición precisa de su metodología, su alcance, sus responsables, su periodicidad y sus criterios de priorización y reporte. Cada una de estas decisiones cuenta con un fundamento técnico o normativo propio; sin embargo, es su articulación conjunta la que dota al procedimiento de coherencia interna y lo diferencia de una simple adaptación genérica de los estándares internacionales de referencia a un procedimiento pertinente al contexto operativo específico de la CAR.

Fase 2. Documentación del procedimiento

El procedimiento formal de gestión de vulnerabilidades técnicas, entregable principal del presente proyecto, se elaboró siguiendo los lineamientos institucionales establecidos en el procedimiento GSG-PR-01 "Creación y Control de la Información Documentada del SIGESPU" (versión 16), documento que rige la creación de cualquier información documentada dentro del Sistema Integrado de Gestión Pública de la CAR (CAR, 2026a). Dicha decisión fue tomada debido a que el procedimiento está destinado a integrarse formalmente al SIGESPU, por lo tanto, su construcción debe estar alineada a las recomendaciones de la entidad. El documento completo del procedimiento (GGD-PR-XX), junto con sus tres anexos descritos más adelante en esta fase, se adjunta como anexo del presente proyecto, permitiendo su consulta íntegra por parte del lector.

El GSG-PR-01 clasifica los documentos por tipo, estableciendo para cada uno los elementos obligatorios, opcionales o no aplicables. El tipo documental "Procedimiento" es el único que exige la totalidad de los 16 elementos de estructura, dado su carácter operativo.

Tabla 1

Aspectos generales de presentación de los documentos

[illegible]

Tipo de documento	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Guía	✓	✓	✓	✓	✓	✓	Opc.	Opc.	Opc.	Opc.	Opc.	Opc.	Opc.	Opc.	✓	Opc.
Instructivo	✓	✓	✓	✓	✓	×	Opc.	Opc.	Opc.	Opc.	Opc.	Opc.	Opc.	✓	✓	Opc.
Listados maestros	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	×	✓	×
Manual	✓	✓	✓	✓	✓	Opc.	Opc.	Opc.	×	×	×	×	Opc.	Opc.	✓	Opc.
Matriz	✓	✓	✓	✓	✓	×	×	×	×	×	Opc.	×	×	×	✓	×
Plan	✓	✓	✓	✓	✓	Opc.	✓	✓	✓	Opc.	Opc.	Opc.	Opc.	Opc.	✓	Opc.
Políticas	✓	✓	✓	✓	✓	×	×	✓	✓	×	✓	×	×	×	✓	Opc.
Procedimiento	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Programas	✓	✓	✓	✓	✓	Opc.	✓	✓	✓	Opc.	Opc.	Opc.	Opc.	✓	✓	Opc.
Protocolo	✓	✓	✓	✓	✓	✓	Opc.	✓	✓	Opc.	Opc.	Opc.	Opc.	✓	✓	✓

1. Logo 2. Nombre del Documento 3. Versión 4. Código 5. Fecha 6. Tabla de
 Contenido 7. Páginas 8. Objetivo 9. Alcance 10. Definiciones 11. Responsable 12.
 Responsabilidades 13. Generalidades 14. Descripción 15. Control de Cambios 16. Anexos

Convenciones: ✓ = Aplica × = No aplica Opc. = Opcional

Nota. Tomado de *Creación y control de la información documentada del SIGESPU*
 (GSG-PR-01, Versión 16, p. 7), por CAR, 2026a.

Teniendo en cuenta lo anterior el procedimiento fue construido de la siguiente manera:

Código del procedimiento dentro del SIGESPU

Se utilizó el prefijo GGD (Gestión de la Gobernanza Digital), esto correspondiendo al proceso estratégico donde se ubica la Oficina de Gobernanza Digital y Analítica de Datos, esto según la tabla de codificación de procesos encontrada en el GSG-PR-01.

Tabla 2

Codificación de los procesos

NOMBRE DEL PROCESO	CÓDIGO DEL PROCESO
ESTRATÉGICOS	
Gestión Estratégica	GES
Gestión de la Gobernanza Digital	GGD
Comunicación Estratégica	CES
Gestión del SIGESPU	GSG
Gestión del Conocimiento Ambiental I+D+I-	IDI
MISIONALES	
Monitoreo y Modelamiento Ambiental	MMA
Planificación y Ordenamiento Ambiental	POA
Gestión de la Biodiversidad y Ecosistemas Estratégicos	GBE

NOMBRE DEL PROCESO	CÓDIGO DEL PROCESO
Gobernanza y Sostenibilidad Ambiental	GSA
Autoridad Ambiental	AAM
Infraestructura Ambiental	IAM
Gestión del Servicio al Ciudadano	GSC
APOYO	
Gestión Humana	GHU
Gestión Jurídica Corporativa	GJC
Gestión Administrativa	GAD
Gestión Documental y Archivo	GCT
Gestión Financiera	GFI
Gestión Disciplinaria Interna	GDI
Gestión Contractual	GCT

Nota. Tomado de *Creación y control de la información documentada del SIGESPU* (GSG-PR-01, Versión 16, pp. 10–11), por CAR, 2026a.

Luego de esto, teniendo en cuenta el tipo de documento, se usará la sigla **PR**, teniendo en cuenta la tabla de codificación por tipo de documento encontrada en el GSG-PR-01.

Tabla 3*Codificación por tipo de documentos*

TIPO DE DOCUMENTO Y DESCRIPCIÓN	CÓDIGO
	DOCUMENTO
Caracterización: Documento que describe el objetivo, alcance, responsables, actividades, recursos, indicadores, riesgos y requisitos de un proceso, mostrando sus interacciones y forma de operación. Se apoya en el ciclo PHVA para facilitar su comprensión, control y mejora continua dentro del Sistema Integrado de Gestión Pública – SIGESPU.	CP
Acuerdo de prestación del servicio: Documento que define las características, responsabilidades y condiciones para la prestación de un servicio, garantizando coordinación, calidad y cumplimiento entre la Corporación y los usuarios.	AS
Manual: Documento normativo y orientador que recopila información, conocimientos, criterios organizacionales, describe directrices, responsabilidades para la gestión de uno o varios procesos. Sirve como fuente de referencia para la creación y aplicación de procedimientos, programas, planes e instructivos, sin llegar al nivel de detalle operativo de estos.	MN
Política: Directriz de cumplimiento obligatorio que establece criterios y compromisos para orientar la toma de decisiones y la ejecución de actividades, asegurando coherencia y alineación con los objetivos estratégicos institucionales.	PL
Plan: Documento estratégico que establece los objetivos, metas, acciones, responsables, recursos y plazos necesarios para alcanzar un propósito institucional. El plan establece qué se quiere lograr y cómo se orientarán los esfuerzos hacia el cumplimiento de ese objetivo. Tiene un	PN

alcance amplio y directivo, ya que orienta y establece el marco dentro del cual se desarrollan las actividades.

Programa: Documento que agrupa y organiza un conjunto de actividades, proyectos o acciones relacionadas entre sí, orientadas a cumplir objetivos definidos dentro de una política o plan.

PG

Procedimiento: Es un conjunto de pasos ordenados y sistemáticos para realizar una actividad o proceso completo dentro de una organización o sistema. Este debe llevar una secuencia lógica y debe reflejar el cómo, dónde, cuándo, los responsables y sus interacciones.

PR

Protocolo: Es un documento que establece un conjunto de normas, directrices y pasos formales de cumplimiento obligatorio, que deben seguirse en situaciones específicas, delicadas o críticas. Define las acciones, conductas y métodos apropiados para garantizar una actuación coherente, segura y uniforme ante dichas circunstancias. Su propósito es estandarizar la respuesta institucional mediante instrucciones claras, diagramas de flujo, listas numeradas o esquemas que orienten la correcta ejecución de las acciones establecidas.

PT

Nota. Tomado de *Creación y control de la información documentada del SIGESPU* (GSG-PR-01, Versión 16, pp. 11–12), por CAR, 2026a.

Por último, el número consecutivo será asignado por la Oficina Asesora de Planeación una vez sea revisado y aprobado para publicación interna, obteniendo así el procedimiento "GGD-PR-XX - Gestión de Vulnerabilidades Técnicas para los Sistemas de Información de la CAR".

Objetivo del procedimiento

El numeral 6.1.2.4 (ítem 8) del procedimiento institucional GSG-PR-01 "Creación y Control de la Información Documentada del SIGESPU" establece que "el Objetivo del documento debe iniciar con verbo infinitivo y estar redactado en forma infinitiva" (CAR, 2026a), por cuanto el objetivo representa el propósito que se pretende cumplir con la creación del documento y debe comunicar, de manera directa y verificable, la acción central que este ejecuta.

Con base en este lineamiento, el objetivo del procedimiento se redactó de la siguiente manera:

"Establecer los lineamientos y actividades para identificar, evaluar, priorizar y reportar las vulnerabilidades técnicas presentes en los sistemas de información de la Corporación Autónoma Regional de Cundinamarca (CAR)."

La redacción parte del verbo infinitivo "Establecer", cumpliendo el requisito formal exigido por el GSG-PR-01. Su contenido sustantivo, por su parte, no se formuló de manera genérica, sino que replica de manera directa los verbos rectores del control 8.8 de ISO/IEC 27002:2022, el cual exige a las organizaciones "obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización a tales vulnerabilidades y tomar las medidas apropiadas para prevenir su explotación" (ISO/IEC, 2022b). De esta correspondencia se derivan los cuatro verbos que estructuran el objetivo: identificar, evaluar, priorizar y reportar, cuya operacionalización técnica qué se prueba, cómo, quién lo ejecuta y con qué criterios fue definida en la Fase 1.

Alcance del procedimiento

El numeral 6.1.2.4 (ítem 9) del GSG-PR-01 establece que el Alcance debe señalar el punto de partida, el desarrollo y el cierre del proceso que se documenta (CAR, 2026a). Bajo este lineamiento, y retomando la estructura secuencial de tres momentos definida en la Fase 1, el alcance del procedimiento se redactó de la siguiente manera:

"Este procedimiento inicia con la identificación de los sistemas de información objeto de evaluación, continúa con la ejecución de pruebas de seguridad dinámica (DAST), la evaluación de las vulnerabilidades técnicas identificadas, la priorización de estas vulnerabilidades, y finaliza con la elaboración y entrega del informe de resultados al área de Desarrollo de Aplicaciones y Sistemas de Información."

El inicio, el desarrollo y el cierre de esta redacción corresponden exactamente a los cuatro verbos rectores definidos en el Objetivo del procedimiento, garantizando la coherencia interna entre ambos numerales, tal como lo exige la estructura documental del GSG-PR-01.

Definiciones del procedimiento

El numeral 6.1.2.4 (ítem 10) del GSG-PR-01 establece que las definiciones deben corresponder a "todas las definiciones necesarias para la comprensión del contenido de los documentos" y que "los términos y definiciones deben estar ordenados alfabéticamente" (CAR, 2026a). Siguiendo este lineamiento, se incluyeron únicamente los diez términos técnicos indispensables para comprender el procedimiento, ordenados alfabéticamente de CVSS a Vulnerabilidad técnica, evitando definir conceptos genéricos de seguridad de la información que no son objeto directo del documento.

Cada definición se fundamentó en la fuente técnica o normativa que la respalda:

CVSS y Severidad se definieron con base en la especificación técnica del Common Vulnerability Scoring System versión 3.1, publicada por el Forum of Incident Response and Security Teams (FIRST.Org, Inc., 2019), organismo que desarrolla y mantiene oficialmente este estándar de puntuación.

DAST y OWASP WSTG se definieron con base en la OWASP Web Security Testing Guide, publicada por la fundación Open Web Application Security Project (OWASP, 2020), fuente primaria de la metodología de pruebas adoptada por el procedimiento.

MSPI se definió con base en los lineamientos del Modelo de Seguridad y Privacidad de la Información, actualizado mediante la Resolución 2277 de 2025 (Ministerio de Tecnologías de la Información y las Comunicaciones, 2025).

Vulnerabilidad técnica se definió con base en el vocabulario normalizado de seguridad de la información establecido en la norma ISO/IEC 27000:2018, la cual define una vulnerabilidad como la debilidad de un activo o control que puede ser explotada por una o más amenazas (International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2018). Esta es la definición de referencia internacional adoptada de manera consistente por toda la familia de normas ISO/IEC 27000, incluyendo la ISO/IEC 27001:2022 que fundamenta el presente procedimiento.

Hallazgo, Priorización, Nivel de criticidad de la prueba y Sistema de información son definiciones operativas construidas específicamente para efectos de este procedimiento, a partir de la terminología empleada de manera consistente en el marco teórico del proyecto (control 8.8

de ISO/IEC 27002:2022 y lineamientos de clasificación de activos del MSPI), sin corresponder a una cita textual de una fuente externa única.

Responsable

El numeral 6.1.2.4 (ítem 11) del GSG-PR-01 define este campo como la "dependencia o rol garante de la implementación y cumplimiento del documento dentro del proceso correspondiente", precisando que "en esta sección se mencionan las oficinas, direcciones o roles" (CAR, 2026a). Con base en este lineamiento, que permite designar explícitamente un rol y no exclusivamente una dependencia completa, se asignó la responsabilidad del procedimiento al Profesional Especializado en Seguridad de la Información de la Oficina de Gobernanza Digital y Analítica de Datos (OGDAD), conforme a los criterios de asignación de roles y responsabilidades ya justificados en la Fase 1.

Responsabilidades

El numeral 6.1.2.4 (ítem 12) del GSG-PR-01 exige que las responsabilidades se redacten iniciando con verbos en infinitivo (CAR, 2026a), describiendo lo que cada responsable identificado en el numeral anterior debe ejecutar. Siguiendo este lineamiento, las responsabilidades del Profesional Especializado se redactaron en un párrafo corrido, encadenando en infinitivo las acciones que se derivan directamente de las cuatro etapas definidas en el Objetivo y el Alcance del procedimiento: identificar, ejecutar (las pruebas DAST), evaluar y clasificar, y elaborar y remitir el informe, obteniendo así lo siguiente:

"Identificar los sistemas de información objeto de evaluación, ejecutar las pruebas de seguridad dinámica (DAST) sobre dichos sistemas, garantizar la adecuada configuración y

coordinación de las ventanas de escaneo, evaluar y clasificar los hallazgos identificados según su nivel de severidad y tipo de vulnerabilidad, elaborar y remitir oportunamente el informe de resultados, con el fin de contribuir a la identificación temprana de debilidades técnicas y a la protección de la confidencialidad, integridad y disponibilidad de la información institucional."

Generalidades

El numeral 6.1.2.4 (ítem 13) del GSG-PR-01 define las Generalidades como el espacio del documento destinado a "las directrices, políticas o documentos de referencia que aplican al documento", donde "se puede describir el fundamento teórico en el cual está basado el documento considerando los requisitos legales aplicables" (CAR, 2026a). Es, por tanto, el único numeral del procedimiento donde el GSG-PR-01 exige explícitamente sustentar el contenido en normativa externa, y no solo en el estándar documental institucional. Con base en este lineamiento, el numeral se estructuró en cinco bloques.

Contexto y propósito de la evaluación: el párrafo introductorio enmarca el procedimiento dentro del compromiso institucional de la CAR con la protección de sus recursos informáticos, estableciendo como propósito específico la evaluación de la superficie de exposición de los activos web institucionales, conforme a la metodología de evaluación ya justificada en la Fase 1.

Metodología OWASP: se declara la adopción del OWASP Top 10 – 2021 como marco de referencia para estructurar las pruebas (Open Web Application Security Project, 2021),

precisando su complementariedad con la OWASP Web Security Testing Guide ya citada en el Marco Teórico, conforme a los criterios de clasificación de riesgo justificados en la Fase 1.

Periodicidad y herramienta: se declara la ejecución anual del procedimiento y el uso de Tenable Web Application Scanning (WAS) en modalidad no autenticada, conforme a los criterios de periodicidad ya justificados en la Fase 1. Las nueve pruebas técnicas DAST detalladas (fingerprinting de servidor y framework, identificación de puntos de entrada, configuración y despliegue, métodos HTTP, HSTS, fijación de sesión y CSRF) se seleccionaron por representar los vectores de prueba más directamente asociados a las categorías del OWASP Top 10 – 2021 que resultan verificables mediante un escaneo dinámico no autenticado, y se presentan categorizadas en la Ilustración 2 contra dichas categorías de riesgo.

Clasificación de severidad: los rangos de severidad (Crítica: 9.0-10.0, Alta: 7.0-8.9, Media: 4.0-6.9, Baja: 0.1-3.9) reproducen la Tabla 14 (Qualitative Severity Rating Scale) del documento de especificación técnica del CVSS v3.1 (FIRST.Org, Inc., 2019, p. 19), conforme a los criterios de clasificación ya justificados en la Fase 1.

Referentes normativos y técnicos: el listado de cierre consolida las nueve fuentes que fundamentan la totalidad del procedimiento —ISO/IEC 27001:2022 (control 8.8), ISO/IEC 27002:2022, ISO/IEC 27005:2022, la OWASP Web Security Testing Guide, el OWASP Top 10 – 2021, el CVSS v3.1, las publicaciones NIST SP 800-40 Rev. 4 y NIST SP 800-53 Rev. 5, y el MSPI con su Guía No. 5 de MinTIC—, cumpliendo así, de manera explícita y verificable, la exigencia normativa del GSG-PR-01 de declarar el fundamento teórico del documento.

Descripción del procedimiento

El numeral 6.1.2.4 (ítems 14 y 15) del GSG-PR-01 exige que la descripción del procedimiento se estructure en una tabla que contenga, como mínimo, los campos Ítem, Descripción de la actividad, Área responsable y Cargo responsable, redactando cada actividad en modo infinitivo, y estableciendo como mínimo un Punto de control (P.C) dentro de la secuencia (CAR, 2026a, Nota 1).

El procedimiento se estructuró en cuatro fases. Las once actividades se agruparon en cuatro bloques:

- Identificar sistemas de información
- Realizar pruebas de seguridad dinámica (DAST)
- Clasificar resultados de pruebas
- Entregar resultados de pruebas

Replicando de manera directa la secuencia de momentos definida en el Alcance del procedimiento (inicio, desarrollo y cierre). Esta agrupación no corresponde estrictamente a la de asociar una fase por cada uno de los cuatro verbos del Objetivo (identificar, evaluar, priorizar, reportar), sino a las cuatro fases técnicas del proceso de ejecución: la fase 1 opera simultáneamente sobre "identificar" y "priorizar" (al aplicar los criterios de priorización para seleccionar los sistemas objeto de evaluación); la fase 2 materializa técnicamente la "evaluación" mediante la ejecución de las pruebas DAST; la fase 3 clasifica los hallazgos según severidad, operacionalizando nuevamente la "evaluación", esta vez sobre las vulnerabilidades y no sobre los sistemas; y la fase 4 corresponde íntegramente al "reporte". Esta distribución garantiza que, en

conjunto, las once actividades operacionalicen la totalidad de los cuatro verbos del Objetivo, aunque no exista una correspondencia lineal de una fase por verbo.

El procedimiento incorpora dos Puntos de Control, cuyo diseño y fundamento técnico ya fueron justificados en la Fase 1. El primero se ubica en la actividad **1.2**, y corresponde al mecanismo de priorización descrito en "Criterios de priorización": ante la imposibilidad de evaluar la totalidad de los sistemas de información en un ciclo determinado, este punto de control remite a la guía GGD-PR-XX-GI-01 para seleccionar los sistemas objeto de evaluación. El segundo se ubica en la actividad **4.2**, y corresponde al mecanismo de seguimiento semestral descrito en "Alcance técnico", mediante el cual se verifica el avance del área de Desarrollo de Aplicaciones y Sistemas de Información en la resolución de los hallazgos reportados.

Control de cambios

El numeral 6.1.2.4 (ítem 16) del GSG-PR-01 establece que este numeral debe garantizar "la trazabilidad de las actualizaciones realizadas a la información documentada del SIGESPU", mediante una tabla que contenga como mínimo los campos Versión, Descripción del cambio, Responsable/Memorando y Fecha (CAR, 2026a). El mismo numeral precisa que el campo "Versión" corresponde al "número consecutivo que identifica el cambio de versión del documento", que el campo "Responsable/Memorando" debe indicar "el nombre del profesional responsable que realiza la modificación y el número de memorando mediante el cual se solicita la actualización del documento", y que la "Fecha" corresponde a la de aprobación y publicación oficial del documento, siendo ambos datos registrados por el administrador del sistema documental al momento de la publicación (CAR, 2026a).

Con base en este lineamiento, se registró la versión inicial (versión 1) del procedimiento, identificando como responsable de su elaboración al Grupo de Mejora GGD, en su calidad de responsable del proceso "Gestión de la Gobernanza Digital" encargado de validar técnicamente la creación de la información documentada del proceso, conforme al numeral 5 (Responsabilidades) del propio GSG-PR-01, el cual asigna a los Grupos de Mejora la función de "revisar y validar técnicamente la creación, modificación, eliminación o transferencia de la información documentada" (CAR, 2026a). El número de memorando y la fecha de publicación quedan pendientes de asignación, dado que ambos campos son diligenciados exclusivamente por la Oficina Asesora de Planeación en el momento de la revisión y publicación oficial del documento en el repositorio institucional, y no por el autor del procedimiento.

Anexos

El numeral 6.1.2.4 (ítem 17) del GSG-PR-01 establece que en los anexos "se citan los documentos que han sido utilizados o ilustran parte del documento", precisando que "en este campo se referencian los formatos que pertenecen al procedimiento" (CAR, 2026a). Con base en este lineamiento, el procedimiento cuenta con tres anexos: dos formatos de apoyo operativo, codificados como documentos de nivel 4 (tipo "Formato", código FR), y una guía metodológica (tipo "Guía", código GI), conforme a la estructura de codificación de la Tabla 3 del GSG-PR-01.

GGD-PR-XX-GI-01 (Guía de Priorización de Sistemas de Información)

Esta guía operacionaliza los criterios de priorización justificados en la Fase 1 del presente proyecto y sustenta el Punto de Control de la actividad 1.2 del procedimiento, detallando el paso a paso de la metodología (valoración de Confidencialidad, Integridad y Disponibilidad conforme

a la Guía No. 5 de MinTIC, cálculo del Nivel de Criticidad, valoración de la Exposición a Internet y el Volumen de Usuarios, y cálculo del Puntaje de Priorización) y proporcionando la matriz en blanco para su diligenciamiento en cada ciclo de ejecución.

GGD-PR-XX-FR-01 (Ficha Técnica de Configuración de Escaneo)

Este formato operacionaliza el registro de la actividad 2.1 del procedimiento y se estructuró en seis secciones, cada una fundamentada en una fuente distinta del proyecto:

Datos generales del sistema: incluyendo el campo Nivel de criticidad, que retoma directamente la escala Alta/Media/Baja establecida en la Guía No. 5 – Gestión y Clasificación de Activos de Información (MinTIC, 2016), documento que sustenta el criterio de priorización adoptado en la actividad 1.2 del procedimiento.

Configuración del escaneo en Tenable WAS: con los parámetros técnicos (plantilla, modalidad de autenticación, límites de rendimiento, rutas excluidas) descritos en el numeral de Generalidades del procedimiento.

Pruebas técnicas DAST aplicadas: presentada como una lista de verificación (checklist) que reproduce exactamente las nueve pruebas técnicas y su categoría asociada del OWASP Top 10 – 2021, tal como fueron categorizadas en la Ilustración 2 de las Generalidades del procedimiento (Open Web Application Security Project, 2021). El formato de checklist en lugar de un campo de texto libre se seleccionó para garantizar que el registro de cada ejecución sea

comparable entre sistemas y a lo largo del tiempo, atributo consistente con el énfasis en pruebas repetibles y trazables de la OWASP Web Security Testing Guide (OWASP, 2020).

Coordinación y ejecución: registro de la evidencia de la actividad 2.2 del procedimiento (coordinación con el área de Desarrollo de Aplicaciones y Sistemas de Información).

Elaboración: registro del responsable y la fecha de diligenciamiento del formato.

Control de Cambios: exigido para todo tipo documental "Formato" conforme a la Tabla 1 (Aspectos generales de presentación de los documentos) del GSG-PR-01.

GGD-PR-XX-FR-02 (Formato de Informe de Resultados de Pruebas de Seguridad)

Este formato operacionaliza el registro de las actividades 3.2 y 4.1 del procedimiento, y se diseñó con una estructura de doble componente dentro de un mismo documento:

El componente gerencial: consolida los hallazgos por sistema según los cuatro niveles de severidad Crítica, Alta, Media, Baja, replicando la Tabla 14 (Qualitative Severity Rating Scale) del CVSS v3.1 (FIRST.Org, Inc., 2019, p. 19), y presenta las recomendaciones de remediación priorizadas dirigidas a la alta dirección.

El componente técnico: desagrega cada hallazgo individual con su categoría OWASP Top 10 – 2021, su puntaje CVSS específico y su recomendación de remediación puntual, dirigida al área de Desarrollo de Aplicaciones y Sistemas de Información para su ejecución.

La decisión de construir estos tres documentos anexos y no dejar la evidencia de las actividades sin un instrumento de registro estandarizado responde al principio de información documentada establecido en la cláusula 7.5 de la norma ISO 9001:2015, la cual exige que las organizaciones mantengan información documentada como evidencia de conformidad y de los resultados obtenidos en sus procesos (International Organization for Standardization, 2015), garantizando así la trazabilidad de cada ciclo de ejecución del procedimiento y proporcionando a las actividades que lo requieren, un soporte documental verificable ante una eventual auditoría del Sistema de Gestión de Seguridad de la Información. El procedimiento y sus tres documentos anexos: la Guía de Priorización, la Ficha Técnica y el Formato de Informe aquí descritos se incluyen al final del presente proyecto como Anexos A, B, C y D, respectivamente.

Fase 3. Validación de la aplicabilidad del procedimiento

La primera actividad de esta fase consistió en aplicar la metodología definida en la Guía de Priorización de Sistemas de Información (GGD-PR-XX-GI-01) sobre el inventario real de sistemas de información de la CAR. Dicho inventario fue solicitado al equipo de Sistemas de Información de la entidad, quienes remitieron el listado de 48 sistemas actualmente activos junto

con su Nivel de Criticidad y su Exposición a Internet, presentado en la Tabla 1. El inventario completo, tal como fue recibido, se incluye como Anexo E del presente documento.

Tabla 4

Inventario de sistemas de información de la CAR

 OFICINA DE GOBERNANZA DIGITAL Y ANALITICA DE DATOS INVENTARIO SISTEMAS DE INFORMACION DE LA CAR					
ID	Nombre de aplicación	Descripción	Prioridad	Expuesto a internet	Url acceso producción
1	PAGINA WEB 2.0	Página oficial CAR	ALTA	SI	https://www.car.gov.co
2	PAGINA WEB 1.0	Plataforma integral que facilita el acceso a recursos y servicios digitales para promover la gestión ambiental y el desarrollo sostenible en Cundinamarca. Ofrece información sobre proyectos de conservación, herramientas interactivas y fomenta la participación ciudadana en iniciativas medioambientales.	BAJA	SI	https://car1.car.gov.co/
3	ETNIAS	Página web para la etnias CAR	BAJA	SI	http://etnias.car.gov.co/
4	INTRANET 1.0	La intranet corporativa optimiza la gestión de la información interna	BAJA	SI	https://intranet.car.gov.co
5	INTRANET 2.0 (SOMOS CAR)	La intranet corporativa optimiza la gestión de la información interna	BAJA	SI	http://somos.car.gov.co/
6	ECOSISTEMA II	Aplicativo para teletrabajadores facilita el reporte, seguimiento y cargue de actividades, optimizando la gestión remota del trabajo. Permite el monitoreo de tareas, proyectos, tiempos y desempeño, mejorando la eficiencia y comunicación entre empleados y supervisores.	MEDIA	SI	https://ecosistemadigital.car.gov.co/
7	APP APLICAR 2.0	App móvil con servicios CAR	ALTA	NO	App local
8	CUMBRE AMBIENTAL INTERNACIONAL - PAGINA WEB	Página web para la cumbre ambiental	ALTA	SI	https://cumbreambiental.car.gov.co/
9	PARQUES 2.0	Página web para las aulas ambientales - parques CAR	ALTA	SI	https://aulasambientales.car.gov.co/
10	SIRPA (TAQUILLAS)	Facturación en taquillas parques	ALTA	NO	App local

11	HUELLA DE CARBONO	Página para el registro personal de huella de carbono	MEDIA	SI	https://huella-carbono.car.gov.co
12	DIGITURNO	Turnos para atención usuarios SAC	BAJA	NO	https://172.19.200.80
13	SIGCI	Sistema de Gestión de conocimiento	BAJA	SI	https://sigci.car.gov.co/
14	ELECCIONES CAR	Gestionar de forma eficiente y transparente la elección de representantes y suplentes del sector privado ante el Consejo Directivo de la CAR. Ofrece funciones como el registro en línea de candidatos y votantes, control de ingresos, gestión de candidaturas, votación electrónica segura, y reportes en tiempo real. Garantiza la seguridad, accesibilidad y cumplimiento normativo del proceso, promoviendo la transparencia y eficiencia, al mismo tiempo que optimiza tiempos y recursos. Esto fortalece la gobernanza participativa y asegura que las decisiones reflejen la voluntad del sector privado.	ALTA	SI	https://eleccionescorporacion.car.gov.co/
15	LUPPE	Link Único de Procesos y Procedimientos de la Entidad - LUPPE. Es una plataforma digital implementada por la Corporación Autónoma Regional de Cundinamarca - CAR, cuyo propósito es centralizar, administrar y permitir la consulta transparente de todo el Listado Maestro de Documentos, así como la estructura que conforma el Sistema Integrado de Planeación y Gestión de la Entidad.	ALTA	SI	https://luppe.car.gov.co/
16	NEGOCIOS VERDES	La plataforma promueve actividades económicas sostenibles que equilibran el crecimiento económico con la protección ambiental, fomentando buenas prácticas sociales, laborales y económicas. Busca reducir el impacto ambiental, generar empleo sostenible y fortalecer las economías locales a través de acciones inclusivas y responsables.	ALTA	SI	https://negociosverdes.car.gov.co
17	SIRIO BOGOTA (CON ORARBO)	Sistema de monitoreo continuo del Río Bogotá, enfocado en proteger su ecosistema y prevenir amenazas ambientales. Detecta actividades ilícitas como vertimientos ilegales, incendios forestales y tala ilegal, además de promover la educación ambiental. Utiliza tecnologías avanzadas como cámaras y sensores para monitorear y responder rápidamente	MEDIA	NO	http://siriobogota.car.gov.co

18	SIDCAR - AMBIENTAL	Gestión y seguimiento de proyectos ambientales sin expediente formal. Permite organizar, monitorear el progreso en tiempo real, RESPEL, RUA MINERIA, otros	MEDIA	SI	https://sidcarambiental.car.gov.co/
19	SIDCAR - COLAB	Reemplaza SIDCAR AMBIENTAL e incluye liquidación de permisos	ALTA	SI	https://sidcar-colab.car.gov.co/
20	PORTAL USUARIOS	Portal para tramites usuarios externos CAR	ALTA	SI	https://portalusuarios.car.gov.co/
21	SIDCAR	Sistema de Gestión Documental	ALTA	SI	https://sidcar.car.gov.co
22	SIGU	El Sistema de Información de Gestión de Usuarios de la CAR optimiza la administración de datos y actividades de los usuarios internos y externos. Facilita el registro, control de accesos y permisos,	ALTA	SI	http://sigu.car.gov.co
23	SAE	Gestión de expedientes permisivos y sancionatorios en la CAR mediante digitalización, seguimiento, reduce la pérdida de datos, agiliza tiempos de respuesta e integra otros sistemas internos. Además, garantiza el cumplimiento normativo, promueve la sostenibilidad y mejora la transparencia en los procesos administrativos y ambientales.	ALTA	SI	https://sae.car.gov.co
24	SGIP	Centraliza y organiza datos sobre los predios adquiridos, incluyendo avalúos, impuestos y visitas de inspección. Permite consultas ágiles, generación de reportes en Excel y PDF, y optimiza la gestión predial,	ALTA	SI	https://sgip.car.gov.co
25	CENSO USUARIOS - PORH	Censo de Usuarios para las cuencas hídricas	MEDIA	SI	http://censousuarios.car.gov.co/
26	CDA	Monitoreo CDA	ALTA	SI	https://simaav.car.gov.co o
27	FORMULACAR	FormulaCAR es una plataforma web que organiza la información de proyectos, aplicando la metodología del Marco Lógico para evaluar su viabilidad técnica y financiera.	ALTA	SI	https://formula.car.gov.co/
28	REVISTA CIENTIFICA - ITTPA	Plataforma que difunde avances científicos en gestión ambiental, fomentando el acceso al conocimiento, la participación comunitaria y el respaldo a políticas de sostenibilidad.	MEDIA	SI	https://ittpa.car.gov.co/
29	SINGELIA	La página web de manejo de información ambiental facilita la gestión, almacenamiento y difusión de datos ambientales, brindando acceso a información actualizada sobre calidad	MEDIA	SI	https://singelia.car.gov.co o

		del aire, agua, biodiversidad y cambio climático. Sirve como referencia centralizada para autoridades, organizaciones y el público.			
30	SITDELIA - ENVISTA ARM	Sistema geográfico con resultados del Laboratorio	MEDIA	SI	https://sitedlia.car.gov.co
31	CENDOC - CENTRO DEL DOCUMENTACIÓN	Facilita el acceso a información ambiental, promoviendo el conocimiento y la educación sobre temas ambientales. Ofrece colecciones digitales, programas educativos y asesoría en investigaciones y proyectos ambientales.	BAJA	SI	https://www.car.gov.co/cendoc
32	KOHA - CATALOGO BIBLIOGRAFICO	Catalogo bibliográfico	BAJA	SI	http://catalogo.car.gov.co
33	SIE - DSPACE - BIBLIOTECA DIGITAL AMBIENTAL	Recopila, publica y preserva los recursos digitales de la corporación, promoviendo su acceso abierto y la apropiación social para fomentar la cultura ambiental. Apoya la ejecución de políticas y proyectos ambientales en la región. Para mejorar la creación, catalogación y accesibilidad de los recursos, garantizando su disponibilidad y fiabilidad.	BAJA	SI	https://sie.car.gov.co/
34	MOODLE (CONTRATISTAS - FUNCIONARIOS - SIGAM)	Moodle es un sistema de gestión de aprendizaje que facilita la capacitación continua de funcionarios y contratistas, ofreciendo acceso flexible a cursos y recursos educativos. Permite el seguimiento del progreso, evaluaciones interactivas y la certificación de los participantes, contribuyendo al desarrollo profesional y la mejora operativa de la organización.	BAJA	NO	https://cargov.sharepoint.com/b/s/CalidaddeSoftware/IQCDpXGo8GMVRZFPppestcgolAWZJcKXU1qoJmOgXzwdUack?e=YfyFbS
35	SGC	El aplicativo de gestión de contratación de la CAR centraliza y automatiza los procesos contractuales, garantizando transparencia y eficiencia. Permite la gestión de contratos de inversión y funcionamiento, control presupuestal, seguimiento de pagos y cumplimiento normativo.	ALTA	NO	http://sgc.car.gov.co/
36	SIRFAC 1.0	El Aplicativo de Información de Rentas y Facturación de la CAR optimiza la gestión de ingresos, permitiendo el control de rentas, generación de facturas, cálculos automáticos y seguimiento de pagos. Integra seguridad, reportes detallados y acceso web,	ALTA	NO	http://sapwlbogpru.car.gov.co/

37	SARA	El aplicativo de nómina de la CAR centraliza y automatiza la gestión salarial, garantizando pagos puntuales, precisión y transparencia en la administración de recursos humanos, optimizando la eficiencia y el cumplimiento normativo.	ALTA	NO	http://172.19.200.229:8080/saraweb/webcommon/acceso.jsf_VIATICOS http://172.19.200.229:8085
38	ORION	Gestión de procesos jurídicos y disciplinarios	MEDIA	SI	https://orion.car.gov.co
39	GLPI	Software de gestión de servicios tecnológicos que optimiza la atención de incidencias y solicitudes en la CAR, mejorando la administración de recursos IT. A través de GLPI, los usuarios pueden generar tickets de soporte, hacer seguimiento y gestionar activos informáticos de manera eficiente.	MEDIA	NO	https://mesadeayuda.car.gov.co/
40	BOCHICAR	Sistema de monitoreo continuo del Río Bogotá entre Chía y Soacha, operando 24/7 para prevenir amenazas ambientales y sociales. Detecta descargas ilegales, incendios, tala, robo de recursos y otras prácticas perjudiciales. Utiliza tecnología avanzada para alertar a las autoridades y fomenta la educación ambiental para la conservación del río.	MEDIA	SI	https://visorpescar.car.gov.co
41	PESCAR BI	PESCAR integra monitoreo ambiental con Power BI, permitiendo visualizar en tiempo real datos clave sobre aire, agua, fauna y minería para una gestión más eficiente y transparente.	MEDIA	SI	http://pescarbi.car.gov.co/
42	PITCAR -PLATAFORMA DE INNOVACIÓN TERRITORIAL 1.0	Página del DLIA	MEDIA	SI	https://car1.car.gov.co/laboratorio/inicio
43	PESCAR II	Plataforma de monitoreo ambiental Pescar, implementada por la CAR Cundinamarca, permite supervisar en tiempo real factores clave como aire, agua, fauna y minería, facilitando la toma de decisiones para la protección ambiental.	MEDIA	SI	https://pescar.car.gov.co/
44	CONDOR	Plataforma web que permite registrar, monitorear y gestionar en tiempo real los proyectos, contratos y convenios de la CAR .- OBRAS. Ofrece un mapa georreferenciado, reportes automatizados, control de cumplimiento y acceso a documentación contractual. Además, promueve la	MEDIA	SI	https://condor.car.gov.co/

		transparencia mediante la interacción con la ciudadanía.			
45	GEOURBANA	Sin Info	MEDIA	SI	https://geourbana.car.gov.co/
46	SICLICA - ZIPA	Sistema de información climatológica e hidrológica (SICLICA)	MEDIA	NO	https://zipa.car.gov.co
47	GEOAMBIENTAL	Sistema Información Geográfico, cargada toda la informa ambiental CATASTRO -IGAC- RHIDRICO, POMCAS, AREAS PROTEGIDAS. PERMISOS	ALTA	SI	https://geoambiental.car.gov.co
48	SICOF (CONTABILIDAD - PRESUPUESTO - TESORERIA - RENTAS)	El Sistema Integrado de Gestión Administrativa y Financiera optimiza los procesos administrativos y financieros,	ALTA	NO	http://172.19.200.25:8080

Nota. Elaboración propia, con base en el inventario de sistemas de información suministrado por el equipo de Sistemas de Información de la CAR (2026) y en la valoración independiente del criterio de Volumen de Usuarios.

El criterio de Volumen de Usuarios no fue entregado como un dato consolidado, dado que el equipo de Sistemas de Información no cuenta con esa información sistematizada; por tanto, se valoró de manera independiente, a partir de la descripción funcional de cada sistema incluida en el mismo inventario recibido, aplicando el siguiente criterio: Alto: cuando el sistema es de uso masivo por parte de la ciudadanía o de toda la entidad, Medio: cuando su uso corresponde a un grupo amplio pero acotado, como un segmento específico de la ciudadanía o varias dependencias de la CAR, Bajo: cuando su uso es interno, limitado a una sola dependencia o a un grupo reducido de usuarios.

El cálculo del Puntaje de Priorización se realiza sumando el valor numérico asignado a cada nivel cualitativo, conforme a la escala de valoración de la Tabla 1 de la Guía de Priorización: (Nivel de Criticidad: Alta = 3, Media = 2, Baja = 1; Exposición a Internet: Sí = 2, No = 1; Volumen de Usuarios: Alto = 3, Medio = 2, Bajo = 1). A modo de ejemplo, el sistema LUPPE, con Nivel de Criticidad Alta, Exposición a Internet Sí y Volumen de Usuarios Alto, obtiene un Puntaje de Priorización de $3 + 2 + 3 = 8$, el máximo posible dentro de la escala.

Es importante precisar que este cálculo, tal como lo establece la Guía, se aplica sobre la totalidad del inventario, sin presuponer una modalidad de prueba en particular, dado que la Guía está diseñada como una herramienta reutilizable en cualquier ciclo futuro de ejecución del procedimiento, sea este autenticado o no autenticado. Sin embargo, dado que el presente proyecto decidió por facilidad operativa, según lo justificado en la Fase 1 ejecutar el piloto en modalidad no autenticada, el universo de sistemas efectivamente evaluables en esta ejecución específica se limita a aquellos con Exposición a Internet igual a Sí, ya que un sistema no expuesto no es alcanzable mediante pruebas no autenticadas desde el exterior de la red de la CAR, de los 48 sistemas del inventario, 37 cumplen esta condición de elegibilidad.

Sobre estos 37 sistemas elegibles se aplicó nuevamente el Puntaje de Priorización, ordenándolos de mayor a menor conforme al listado de la Tabla 5. Los primeros 21 lugares quedaron ocupados sin ambigüedad por sistemas con puntaje igual o superior a 6; el puesto 25 coincidió con un grupo de 14 sistemas empatados en un puntaje de 5, lo que activó el criterio de desempate establecido en la Guía (nivel de criticidad y, en última instancia, orden alfabético, dado que la Exposición a Internet ya no discrimina dentro de este subconjunto, al ser un valor

constante en los 37 sistemas elegibles). La aplicación de este criterio determinó que el sistema GEOURBANA ocupara el vigesimoquinto y último lugar de la selección.

Tabla 5

Matriz de priorización aplicada a los sistemas elegibles para el piloto (Exposición a Internet = Sí)

Matriz de priorización aplicada a los sistemas elegibles (Exposición a Internet = Sí)					
Nº	Sistema	Nivel de Criticidad	Volumen de Usuarios	Puntaje	Seleccionado
1	LUPPE	ALTA	ALTA	8	Sí
2	PAGINA WEB 2.0	ALTA	ALTA	8	Sí
3	PORTAL USUARIOS	ALTA	ALTA	8	Sí
4	SAE	ALTA	ALTA	8	Sí
5	SIDCAR	ALTA	ALTA	8	Sí
6	CUMBRE AMBIENTAL INTERNACIONAL - PAGINA WEB	ALTA	MEDIA	7	Sí
7	ELECCIONES CAR	ALTA	MEDIA	7	Sí
8	FORMULACAR	ALTA	MEDIA	7	Sí
9	GEOAMBIENTAL	ALTA	MEDIA	7	Sí
10	NEGOCIOS VERDES	ALTA	MEDIA	7	Sí
11	PARQUES 2.0	ALTA	MEDIA	7	Sí
12	SGIP	ALTA	MEDIA	7	Sí
13	SIDCAR - COLAB	ALTA	MEDIA	7	Sí
14	SIGU	ALTA	MEDIA	7	Sí
15	SINGELIA	MEDIA	ALTA	7	Sí
16	CDA	ALTA	BAJA	6	Sí
17	CONDOR	MEDIA	MEDIA	6	Sí
18	HUELLA DE CARBONO	MEDIA	MEDIA	6	Sí
19	PESCAR II	MEDIA	MEDIA	6	Sí
20	SIDCAR - AMBIENTAL	MEDIA	MEDIA	6	Sí

21	PAGINA WEB 1.0	BAJA	ALTA	6	Sí
22	BOCHICAR	MEDIA	BAJA	5	Sí
23	CENSO USUARIOS - PORH	MEDIA	BAJA	5	Sí
24	ECOSISTEMA II	MEDIA	BAJA	5	Sí
25	GEOURBANA	MEDIA	BAJA	5	Sí
26	ORION	MEDIA	BAJA	5	No
27	PESCAR BI	MEDIA	BAJA	5	No
28	PITCAR -PLATAFORMA DE INNOVACIÓN TERRITORAL 1.0	MEDIA	BAJA	5	No
29	REVISTA CIENTIFICA ITTPA	MEDIA	BAJA	5	No
30	SITDELIA - ENVISTA ARM	MEDIA	BAJA	5	No
31	CENDOC - CENTRO DEL DOCUMENTACIÓN	BAJA	MEDIA	5	No
32	ETNIAS	BAJA	MEDIA	5	No
33	INTRANET 1.0	BAJA	MEDIA	5	No
34	INTRANET 2.0 (SOMOS CAR)	BAJA	MEDIA	5	No
35	SIE - DSPACE - BIBLIOTECA DIGITAL AMBIENTAL	BAJA	MEDIA	5	No
36	KOHA - CATALOGO BIBLIOGRAFICO	BAJA	BAJA	4	No
37	SIGCI	BAJA	BAJA	4	No

Nota. Elaboración propia, con base en la aplicación de la metodología de la Guía de Priorización de Sistemas de Información (GGD-PR-XX-GI-01, Anexo B) sobre los datos de la Tabla 4.

Como resultado, se obtuvo el Listado de Sistemas Priorizados con los 25 sistemas de información que serán objeto del piloto de pruebas DAST en modalidad no autenticada. Los 23

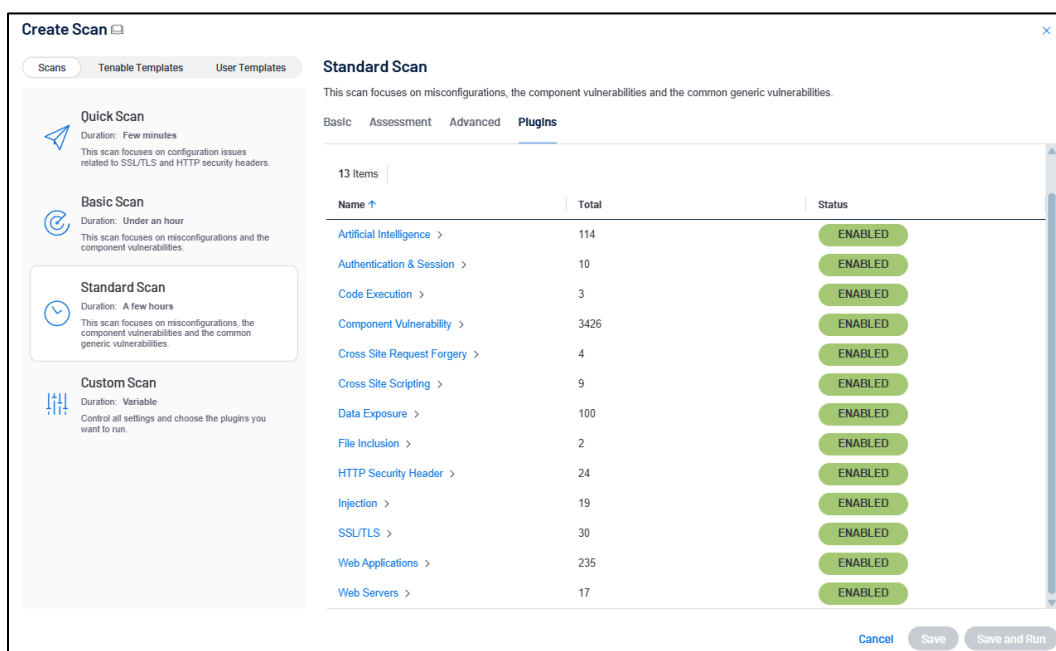
sistemas restantes, consistente con lo ya establecido en el Alcance del proyecto, quedan como línea de trabajo para ciclos posteriores del procedimiento, ya sea mediante la ampliación de cobertura entre los propios sistemas expuestos, o mediante la incorporación de pruebas autenticadas que permitan evaluar los sistemas actualmente no expuestos a Internet. Con el Listado de Sistemas Priorizados ya definido, la siguiente actividad consistió en configurar y ejecutar el piloto de pruebas DAST sobre dichos sistemas.

Configuración y ejecución del piloto DAST

Durante la configuración inicial del piloto se identificó una inconsistencia entre la plantilla de escaneo predefinida "Standard Scan" de Tenable Web Application Scanning (WAS) y las nueve pruebas técnicas DAST descritas en el procedimiento y en la Ficha Técnica de Configuración de Escaneos, dado que dicha plantilla habilita por defecto trece familias completas de plugins incluyendo, entre otras, Component Vulnerability (3.426 verificaciones) e Injection, excediendo ampliamente el alcance técnico documentado.

Figura 5

Familias de plugins habilitadas por defecto en la plantilla Standard Scan de Tenable WAS



Nota. Captura de pantalla de la interfaz de configuración de Tenable Web Application Scanning, tomada por el autor.

Para corregir esta inconsistencia, la ejecución del piloto se realizó mediante la opción **Custom Scan** de Tenable WAS, la cual permite seleccionar de manera individual las familias de plugins a ejecutar, garantizando así la trazabilidad exacta entre lo documentado y lo efectivamente escaneado.

Con base en la documentación oficial de Tenable sobre las familias de plugins de WAS, se estableció la siguiente correspondencia entre las nueve pruebas técnicas del procedimiento y las familias de plugins de la herramienta:

Tabla 6

Correspondencia entre las pruebas técnicas del procedimiento y las familias de plugins de Tenable WAS

N.º	Prueba técnica	Familia de plugins Tenable WAS
1	Fingerprint del servidor web	Web Servers
2	Identificación de puntos de entrada de las aplicaciones	No corresponde a una familia de plugins; es una función del rastreador (crawler) de WAS, configurada en los parámetros de rastreo de la pestaña Advanced
3	Fingerprint del framework de la aplicación	Web Applications
4	Pruebas de configuración y gestión de implementación	Web Servers
5	Pruebas sobre la configuración de la plataforma de la aplicación	Web Servers / HTTP Security Header
6	Pruebas de métodos HTTP	Web Servers (plugin <i>HTTP TRACE Allowed</i>)
7	Prueba de HTTP Strict Transport Security (HSTS)	HTTP Security Header (plugins <i>Missing HTTP Strict Transport Security Policy</i> , <i>HTTP Strict Transport Security Policy Detected</i> , <i>Permissive HTTP Strict Transport Security Policy Detected</i>)
8	Pruebas de fijación de sesión (Session Fixation)	Authentication & Session (plugin <i>Session Fixation</i>)
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	Cross Site Request Forgery

Nota. Elaboración propia, con base en la documentación oficial de familias de plugins de Tenable Web App Scanning (Tenable, Inc., s.f.-a, s.f.-b, s.f.-c, s.f.-d).

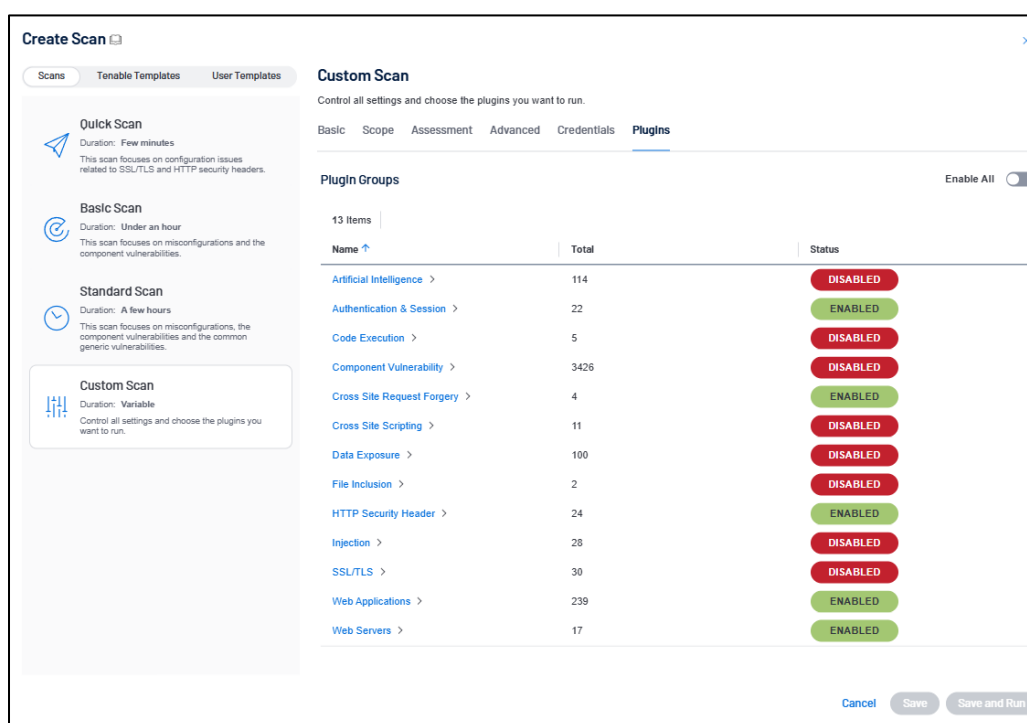
En consecuencia, en la pestaña Plugins del Custom Scan se habilitaron únicamente las cinco familias resultantes de esta correspondencia Web Servers, Web Applications, HTTP Security Header, Authentication & Session y Cross Site Request Forgery, dejando deshabilitadas las ocho familias restantes (Artificial Intelligence, Code Execution, Component Vulnerability,

Cross Site Scripting, Data Exposure, File Inclusion, Injection y SSL/TLS), por no corresponder a ninguna de las nueve pruebas documentadas.

Figura 6

Familias de plugins habilitadas en el Custom Scan, conforme a la correspondencia de la

Tabla 6



Nota. Captura de pantalla de la interfaz de configuración de Tenable Web Application Scanning, tomada por el autor.

La modalidad no autenticada del piloto se garantizó dejando vacía la pestaña Credentials del escaneo, sin registrar ningún conjunto de credenciales de acceso. Adicionalmente, dado que el escaneo se ejecutó mediante el Cloud WAS Scanner de Tenable (US Cloud Scanner), el tráfico de las pruebas se originó desde la infraestructura en la nube de Tenable, es decir, desde fuera de

la red de la CAR, reproduciendo de manera efectiva el escenario de un atacante externo sin credenciales ni acceso privilegiado a la red interna de la entidad, tal como se planteó en la Fase 1.

Figura 7

Configuración del tipo de escáner (Cloud WAS Scanner) utilizado para la ejecución del piloto

The screenshot displays the 'Create Scan' window in Tenable's interface. On the left, there are four scan templates: Quick Scan (few minutes, configuration issues), Basic Scan (under an hour, misconfigurations), Standard Scan (a few hours, misconfigurations and vulnerabilities), and Custom Scan (variable duration, all settings). The 'Custom Scan' template is selected. The main area is titled 'Custom Scan' and includes tabs for Basic, Scope, Assessment, Advanced, Credentials, and Plugins. The 'Basic' tab is active, showing fields for Folder (set to 'Proyecto'), Scanner Type (set to 'Cloud WAS Scanner'), Scanner (set to 'US Cloud Scanner'), and Tags (set to 'Select Tags'). Below these is the 'Targets' section with an 'Import Target File' button, a 'Select Application or Enter target' dropdown (showing 'Example: http://www.example.com'), an 'Add Application' button, and an 'Add to Targets List' button. A search bar is also present. At the bottom, there is a table with columns 'Targets' and 'Application ID', showing 1 target. Navigation buttons 'Cancel', 'Save', and 'Save and Run' are at the bottom right.

Nota. Captura de pantalla de la interfaz de configuración de Tenable Web Application Scanning, tomada por el autor.

La configuración de límites de rastreo se estableció en 10.000 URLs a rastrear y explorar, con una profundidad de directorio de 10 niveles, un tamaño máximo de respuesta de 5.000.000 bytes, un tiempo máximo de escaneo de 03:00:00 (HH:MM:SS) y un tiempo máximo de cola de 08:00:00, manteniendo activada la opción de reducir la velocidad del escaneo ante congestión de

red, con el fin de priorizar la estabilidad de los sistemas de información de la CAR durante la ejecución del piloto sobre su disponibilidad de respuesta inmediata.

Figura 8

Configuración general de tiempos máximos de escaneo y de cola en la pestaña Advanced

The screenshot displays the 'Create Scan' window in Tenable Web Application Scanning. The 'Advanced' tab is selected, showing the following configuration options:

- Quick Scan:** Duration: Few minutes. This scan focuses on configuration issues related to SSL/TLS and HTTP security headers.
- Basic Scan:** Duration: Under an hour. This scan focuses on misconfigurations and the component vulnerabilities.
- Standard Scan:** Duration: A few hours. This scan focuses on misconfigurations, the component vulnerabilities and the common generic vulnerabilities.
- Custom Scan:** Duration: Variable. Control all settings and choose the plugins you want to run.

The 'Custom Scan' configuration includes the following fields and options:

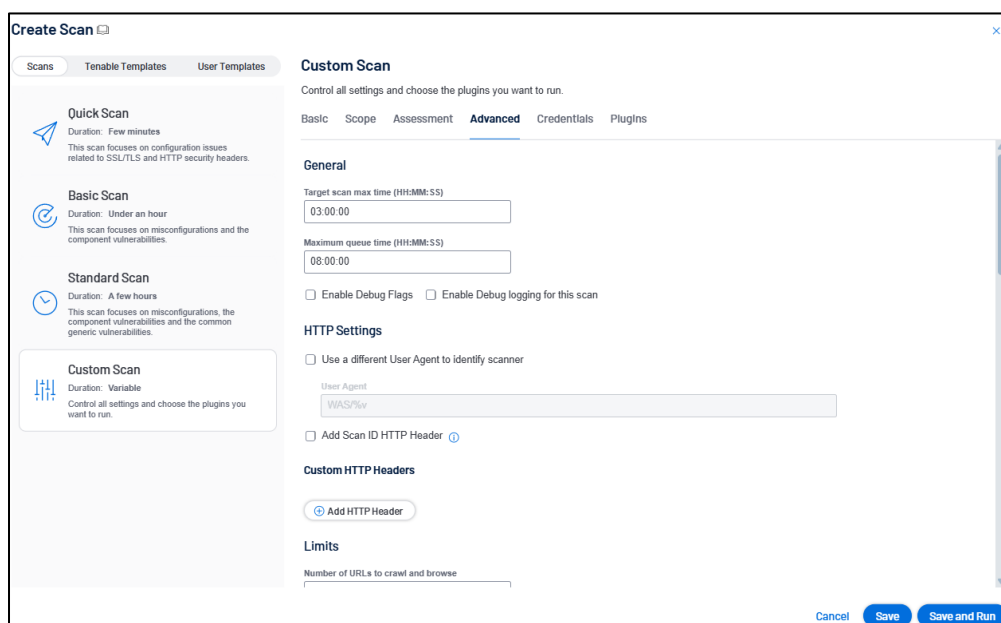
- User Agent:** WAS/vw
- Add Scan ID HTTP Header:** ☐
- Custom HTTP Headers:**
- Limits:**
 - Number of URLs to crawl and browse:** 10000
 - Max response size (Bytes):** 5000000
 - Path directory depth:** 10
 - Request redirect limit:** 3
 - Page DOM Element depth:** 5

At the bottom right, there are buttons for 'Cancel', 'Save', and 'Save and Run'.

Nota. Captura de pantalla de la interfaz de configuración de Tenable Web Application Scanning, tomada por el autor.

Figura 9

Configuración de límites de rastreo en la pestaña Advanced

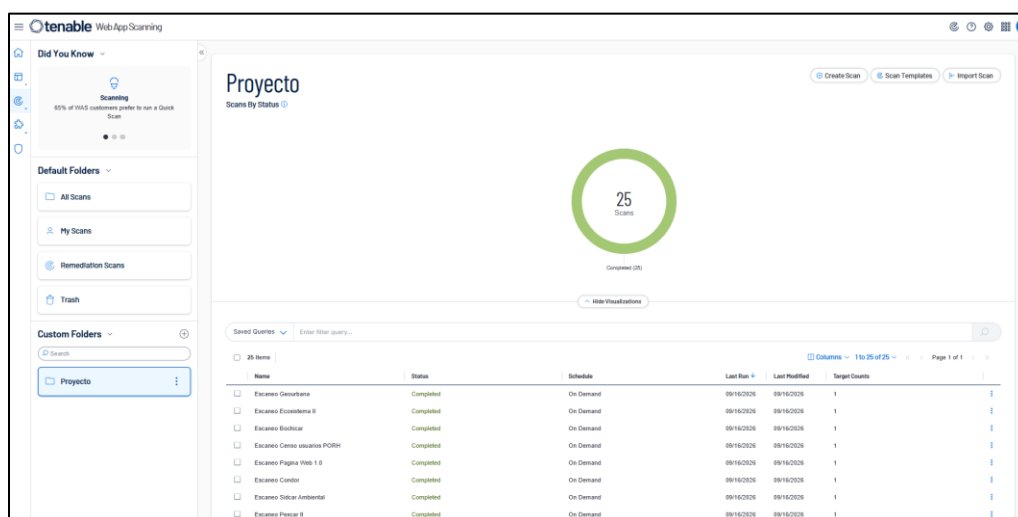


Nota. Captura de pantalla de la interfaz de configuración de Tenable Web Application Scanning, tomada por el autor.

Esta misma configuración target, modalidad no autenticada, Cloud WAS Scanner y las cinco familias de plugins habilitadas se replicó de manera idéntica sobre los 25 sistemas de información seleccionados en la Tabla 5, registrando cada configuración individual en la Ficha Técnica de Configuración de Escaneos (GGD-PR-XX-FR-01) correspondiente a cada sistema, conforme a la actividad 2.1 del procedimiento. Las 25 fichas técnicas diligenciadas se incluyen como anexo del presente documento. Como evidencia de la ejecución efectiva del piloto, la Figura 10 presenta el listado de los 25 escaneos configurados en Tenable WAS sobre los sistemas de información seleccionados, mostrando su estado de ejecución al momento del corte: 10 escaneos completados, 14 en ejecución y 1 pendiente de inicio.

Figura 10

Listado de escaneos ejecutados en Tenable WAS sobre los sistemas de información seleccionados



Nota. Captura de pantalla de la interfaz de Tenable Web Application Scanning, tomada por el autor.

Clasificación y consolidación de resultados

La ejecución del piloto sobre los 25 sistemas de información priorizados en la Tabla 2 produjo un total de **161 hallazgos**, correspondientes a **20 tipos distintos de vulnerabilidad** que se repiten con distinta frecuencia entre los sistemas evaluados. Para su consolidación, se exportó el reporte de hallazgos de cada uno de los 25 escaneos desde Tenable Web Application Scanning, y se procesó dicha información para construir tres tablas: un consolidado de hallazgos por sistema (Tabla 7), un catálogo de los tipos de hallazgo distintos identificados en todo el piloto (Tabla 8), y un detalle completo de los 161 registros individuales con su sistema, severidad, puntaje CVSS y categoría OWASP asociada (Tabla 9, incluida como anexo del presente

documento dada su extensión). Ningún sistema presentó hallazgos de severidad Crítica o Alta; la totalidad de los resultados se concentró en las severidades Media (17 hallazgos) y Baja (144 hallazgos), conforme a la clasificación de la Tabla 14 (Qualitative Severity Rating Scale) del CVSS v3.1 ya adoptada en el procedimiento (FIRST.Org, Inc., 2019).

Tabla 7

Consolidado de hallazgos por sistema

Sistema	URL	Crítica	Alta	Media	Baja	Total
Luppe	https://luppe.car.gov.co	0	0	2	8	10
Singelia	https://singelia.car.gov.co	0	0	2	6	8
Página Web 1 0	https://car1.car.gov.co/	0	0	1	8	9
Elecciones	https://eleccionescorporacion.car.gov.co/	0	0	1	7	8
Negocios	https://negociosverdes.car.gov.co	0	0	1	7	8
Verdes						
Cumbre	https://cumbreambiental.car.gov.co/	0	0	1	7	8
Ambiental						
Huella de	https://huella-carbono.car.gov.co	0	0	1	7	8
Carbono						
Geoambiental	https://geoambiental.car.gov.co	0	0	1	6	7
Portal usuarios	https://portalusuarios.car.gov.co/	0	0	1	6	7
Condor	https://orion.car.gov.co	0	0	1	6	7
Bochicar	https://ittpa.car.gov.co/	0	0	1	6	7
Geourbana	https://geourbana.car.gov.co/	0	0	1	6	7
Ecosistema II	https://ecosistemadigital.car.gov.co/	0	0	1	5	6
Pescar II	https://pescar.car.gov.co/	0	0	1	4	5

Sidcar Colab	https://sidcar-colab.car.gov.co/	0	0	1	3	4
Parques 2 0	https://aulasambientales.car.gov.co/	0	0	0	8	8
SGIP	https://sgip.car.gov.co	0	0	0	8	8
Página Web 2 0	https://www.car.gov.co	0	0	0	6	6
SIGU	https://sigu.car.gov.co	0	0	0	6	6
Sidcar Ambiental	https://sidcarambiental.car.gov.co/	0	0	0	6	6
Censo usuarios	https://censousuarios.car.gov.co/	0	0	0	5	5
PORH						
SAE	https://sae.car.gov.co	0	0	0	4	4
Sidcar	https://sidcar.car.gov.co	0	0	0	4	4
CDA	https://simaav.car.gov.co	0	0	0	3	3
Formulacar	https://formula.car.gov.co/	0	0	0	2	2
TOTAL		0	0	17	144	161

Nota. Elaboración propia, con base en los resultados del piloto de pruebas DAST ejecutado en Tenable Web Application Scanning sobre los 25 sistemas seleccionados.

El sistema LUPPE, que había obtenido el puntaje máximo de priorización en la Tabla 2, registró el mayor número de hallazgos (10), seguido de Singelia (8). En el extremo opuesto, Formulacar registró únicamente 2 hallazgos, ambos de severidad Baja. Esta distribución no guarda una relación directa con el Puntaje de Priorización de cada sistema, dado que dicho puntaje refleja la criticidad institucional, la exposición y el volumen de usuarios del sistema, es decir, el impacto potencial de una vulnerabilidad, y no la cantidad de debilidades técnicas efectivamente presentes en su implementación.

Clasificación por severidad

De los 20 tipos de hallazgo identificados, 8 corresponden a severidad Media (con puntajes CVSS entre 4.3 y 6.8) y 12 a severidad Baja (todos con puntaje CVSS de 2.6), conforme al catálogo consolidado en la Tabla 8. El hallazgo de mayor severidad del piloto fue **"OpenAPI Permissive Input Validation"** (CVSS 6.8, Media), identificado en un sistema que expone documentación de API sin restricciones adecuadas de validación de entrada. Los hallazgos de severidad Baja correspondieron mayoritariamente a debilidades de configuración de cabeceras HTTP de seguridad, ausencia o configuración permisiva de Content Security Policy, Cache-Control, X-Frame-Options y X-Content-Type-Options, y cookies configuradas sin los atributos Secure, HttpOnly o SameSite, siendo **"Cookie Without SameSite Flag Detected"** el hallazgo más recurrente, presente en 23 de los 25 sistemas evaluados.

Tabla 8

Catálogo de tipos de hallazgo distintos identificados en el piloto

Hallazgo	Severidad	CVSS	Familia Tenable WAS	Categoría OWASP Top 10:2021	N.º de sistemas donde aparece
Insecure 'Access-Control-Allow-Origin' Header	Low	2,6	HTTP Security Header	A05 - Security Misconfiguration	6

Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header	A05 - Security Misconfiguration	8
Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header	A05 - Security Misconfiguration	22
Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header	A04 - Insecure Design	20
Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header	A04 - Insecure Design	11
Content Security Policy Missing 'Report-To'	Low	2,6	HTTP Security Header	A04 - Insecure Design	7
Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header	A01 - Broken Access Control	23
Missing Content Security Policy	Low	2,6	HTTP Security Header	A04 - Insecure Design	14
Missing 'X-Frame- Options' Header	Low	2,6	HTTP Security Header	A04 - Insecure Design	8
Missing 'X-Content-Type- Options' Header	Low	2,6	HTTP Security Header		8

Password Field With Auto-Complete	Low	2,6	Authentication & Session	A05 - Security Misconfiguration	8
Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery	A01 - Broken Access Control	9
OpenAPI Permissive Input Validation	Medium	6,8	Web Applications	A03 - Injection	1
Permissive HTTP Strict Transport Security Policy Detected	Medium	5,8	HTTP Security Header	A02 - Cryptographic Failures	5
Missing HTTP Strict Transport Security Policy	Medium	5,8	HTTP Security Header	A02 - Cryptographic Failures	6
Mixed Resource Detection	Medium	5,8	Web Applications	A02 - Cryptographic Failures	1
Access Restriction Bypass Via Origin Spoof	Medium	5	Authentication & Session	A07 - Identification and Authentication Failures	1
Password Submitted Using GET Method	Medium	5	Web Applications	A04 - Insecure Design	1
PHPinfo Information Disclosure	Medium	5	Web Applications	A01 - Broken Access Control	1
Insecure Cross-Origin Resource Sharing Configuration	Medium	4,3	HTTP Security Header	A07 - Identification and Authentication Failures	1

Nota. Elaboración propia, con base en los resultados del piloto de pruebas DAST ejecutado en Tenable Web Application Scanning.

Clasificación por tipo (OWASP Top 10:2021)

Cada hallazgo fue clasificado por Tenable WAS según su categoría del OWASP Top 10:2021, de manera automática y consistente con el marco de referencia adoptado en el procedimiento (Open Web Application Security Project, 2021). La Tabla 9 presenta la distribución de los 20 tipos de hallazgo según esta clasificación.

Tabla 9

Distribución de tipos de hallazgo según categoría OWASP Top 10:2021

CATEGORÍA OWASP TOP 10:2021	TIPOS DE HALLAZGO
A01 – BROKEN ACCESS CONTROL	3
A02 – CRYPTOGRAPHIC FAILURES	3
A03 – INJECTION	1
A04 – INSECURE DESIGN	6
A05 – SECURITY MISCONFIGURATION	3
A07 – IDENTIFICATION AND AUTHENTICATION FAILURES	2

SIN CATEGORÍA OWASP ASIGNADA	1
-------------------------------------	----------

Nota. Elaboración propia, con base en la categorización OWASP Top 10:2021 asignada automáticamente por Tenable Web Application Scanning a cada hallazgo. Un hallazgo ("Missing 'X-Content-Type-Options' Header") no cuenta con categoría OWASP 2021 asignada por la herramienta.

La categoría **A04 – Insecure Design** concentró la mayor cantidad de tipos de hallazgo distintos (6 de 20), seguida de **A01 – Broken Access Control** y **A05 – Security Misconfiguration** (3 cada una). No se identificaron hallazgos en las categorías A06, A08, A09 ni A10, lo cual es consistente con el alcance técnico del piloto: al tratarse de un escaneo no autenticado limitado a cinco familias de plugins específicas (Tabla 6), el piloto no cubre categorías de riesgo como componentes desactualizados (A06) o fallas de integridad de software (A08), que requieren un análisis de composición de dependencias o de la cadena de suministro de software, fuera del alcance definido en la Fase 1.

Consolidación en el Formato de Informe

Los resultados del piloto se consolidaron en un único Formato de Informe de Resultados de Pruebas de Seguridad (GGD-PR-XX-FR-02), conforme a la estructura de doble componente definida en la Fase 1 y documentada en la Fase 2. El componente gerencial del informe consolidó los hallazgos de los 25 sistemas según los cuatro niveles de severidad de la Tabla 7, mientras que el componente técnico desagregó cada hallazgo individual con su sistema, categoría OWASP Top 10:2021, puntaje CVSS y recomendación de remediación, dirigida al área de

Desarrollo de Aplicaciones y Sistemas de Información para su ejecución. El Formato de Informe diligenciado se incluye como **Anexo H** del presente documento.

Con lo desarrollado en esta fase, el procedimiento diseñado en la Fase 1 y documentado en la Fase 2 deja de ser una propuesta metodológica y pasa a contar con evidencia real de su aplicabilidad: la Guía de Priorización seleccionó de manera objetiva y reproducible los 25 sistemas evaluados a partir del inventario institucional; el piloto se ejecutó bajo una configuración técnica verificable y trazable frente a las nueve pruebas definidas; y los 161 hallazgos resultantes se clasificaron y consolidaron conforme a los criterios de severidad y tipo establecidos desde el diseño del procedimiento.

La ausencia de hallazgos de severidad Crítica o Alta no invalida la utilidad del piloto como mecanismo de validación: por el contrario, confirma que el procedimiento es capaz de operar y producir resultados consistentes incluso cuando el universo evaluado presenta un perfil de riesgo predominantemente bajo, sin que ello dependa de la gravedad de lo encontrado. Con esto, el objetivo específico de validar la aplicabilidad del procedimiento mediante un piloto real queda cumplido, cerrando el ciclo completo del proyecto: de la definición metodológica (Fase 1), a su formalización documental (Fase 2), y finalmente a su ejecución y comprobación práctica (Fase 3).

Resultados

El presente proyecto se desarrolló en tres fases, cada una asociada a uno de los objetivos específicos definidos: la Fase 1 definió la metodología, el alcance y los criterios técnicos del procedimiento; la Fase 2 documentó formalmente dicho procedimiento conforme a los lineamientos institucionales del SIGESPU; y la Fase 3 validó su aplicabilidad mediante la ejecución de un piloto real sobre los sistemas de información de la CAR. A continuación, se contrasta lo propuesto en cada objetivo específico con los resultados efectivamente obtenidos.

Tabla 10

Comparación entre los objetivos específicos propuestos y los resultados obtenidos

Objetivo específico	Propuesto	Resultado obtenido
<i>1. Definir la metodología, alcance y criterios técnicos</i>	Definir metodología DAST, alcance técnico, roles, periodicidad, criterios de priorización y mecanismos de reporte, con base en el control 8.8 de ISO/IEC 27001:2022 y buenas prácticas técnicas	Se definieron los 6 criterios técnicos completos (metodología, alcance, roles, periodicidad, priorización, reporte), fundamentados en 9 referentes normativos y técnicos (Fase 1)
<i>2. Documentar el procedimiento formal</i>	Consolidar el procedimiento en un documento institucional, conforme a los lineamientos del SIGESPU	Se elaboró el procedimiento GGD-PR-XX, cumpliendo los 16 elementos exigidos por el GSG-PR-01 para el tipo documental "Procedimiento",

		junto con 3 documentos anexos (Guía de Priorización, Ficha Técnica, Formato de Informe) (Fase 2)
3. Validar la aplicabilidad mediante un piloto	Ejecutar un piloto DAST sobre 25 sistemas seleccionados, clasificar hallazgos por severidad y tipo, y consolidarlos en un informe	Se aplicó la Guía de Priorización sobre 48 sistemas reales, se ejecutó el piloto sobre los 25 seleccionados (161 hallazgos, 20 tipos distintos), y se consolidaron en el Formato de Informe diligenciado (Fase 3)

Nota. Elaboración propia, con base en el desarrollo de las Fases 1, 2 y 3 del presente proyecto.

Resultados por objetivo específico

Objetivo 1 Definición de la metodología, alcance y criterios técnicos.

Este objetivo se cumplió en su totalidad mediante el desarrollo de la Fase 1, en la cual se definieron de manera articulada los seis criterios exigidos: la metodología de evaluación (DAST no autenticado, justificada frente al enfoque SAST por la separación organizacional entre las áreas de Gobierno Digital y Desarrollo de Aplicaciones), el alcance técnico (cuatro de las seis etapas del ciclo de gestión de vulnerabilidades del NIST SP 800-40 Rev. 4), los roles (asignados a un rol técnico específico y no a la dependencia en su conjunto, conforme al control 5.2 de ISO/IEC 27002:2022), la periodicidad (anual, conforme al control RA-5 de NIST SP 800-53 Rev. 5), los criterios de priorización (metodología semicuantitativa basada en la Guía No. 5 de

MinTIC y en ISO/IEC 27005:2022) y los mecanismos de reporte (CVSS v3.1 para severidad, OWASP Top 10 – 2021 para tipo de riesgo). Cada una de estas seis decisiones quedó fundamentada en un referente técnico o normativo verificable, cumpliendo así con la exigencia del objetivo de tomar como referencia el control 8.8 de ISO/IEC 27001:2022 y las buenas prácticas de la industria.

Objetivo 2 Documentación del procedimiento formal

Este objetivo se cumplió mediante la elaboración del procedimiento GGD-PR-XX "Gestión de Vulnerabilidades Técnicas para los Sistemas de Información de la CAR", construido siguiendo estrictamente los lineamientos del procedimiento institucional GSG-PR-01, incluyendo la totalidad de los 16 elementos de estructura exigidos para el tipo documental "Procedimiento" (Tabla 1 del GSG-PR-01), su codificación conforme a la Tabla 3 de dicho documento, y sus 17 numerales de contenido. El procedimiento se complementó con tres documentos anexos la Guía de Priorización de Sistemas de Información (GGD-PR-XX-GI-01), la Ficha Técnica de Configuración de Escaneos (GGD-PR-XX-FR-01) y el Formato de Informe de Resultados de Pruebas de Seguridad (GGD-PR-XX-FR-02), consolidando así las fuentes, guías y el paso a paso definido para su aplicación, tal como lo exigía el objetivo.

Objetivo 3 Validación de la aplicabilidad mediante un piloto

Este objetivo se cumplió mediante la ejecución real del procedimiento diseñado. Se aplicó la Guía de Priorización sobre el inventario real de 48 sistemas de información de la CAR, seleccionando los 25 sistemas de mayor puntaje entre los 37 elegibles para la modalidad no

autenticada. Sobre estos 25 sistemas se ejecutó el piloto de pruebas DAST mediante Tenable Web Application Scanning, con una configuración Custom Scan verificada contra las nueve pruebas técnicas documentadas. El piloto identificó 161 hallazgos, correspondientes a 20 tipos distintos de vulnerabilidad, clasificados por severidad (CVSS) y por categoría de riesgo (OWASP Top 10:2021), y consolidados en un único Formato de Informe con su componente gerencial y técnico, con recomendaciones de remediación priorizadas dirigidas al área de Desarrollo de Aplicaciones y Sistemas de Información.

Contraste con la hipótesis

La hipótesis de investigación planteada al inicio del proyecto establecía que *"el diseño de un procedimiento formal de gestión de vulnerabilidades técnicas, alineado al control 8.8 de la norma ISO/IEC 27001:2022, permitirá a la CAR identificar, evaluar, priorizar y reportar de manera sistemática las vulnerabilidades presentes en sus sistemas de información"*, frente a la hipótesis nula, que planteaba lo contrario.

Los resultados obtenidos en la Fase 3 respaldan la hipótesis de investigación: el procedimiento diseñado permitió **identificar** sistemáticamente los sistemas de información mediante un inventario institucional y una metodología de priorización objetiva; **evaluar** dichos sistemas mediante la ejecución real de un piloto DAST verificable y trazable frente a lo documentado, **priorizar** tanto los sistemas evaluados (mediante el Puntaje de Priorización) como los hallazgos identificados (mediante su clasificación por severidad CVSS) y **reportar** de manera sistemática los resultados en un formato institucional estandarizado, con recomendaciones de remediación priorizadas. Dado que las cuatro capacidades planteadas en la hipótesis se verificaron con evidencia concreta y reproducible, se acepta la hipótesis de

investigación y se rechaza la hipótesis nula. Es importante precisar que esta aceptación no corresponde a una prueba estadística de significancia dado el carácter de proyecto, sino a la comprobación de que el procedimiento, al ser ejecutado, cumple efectivamente las cuatro funciones para las que fue diseñado.

Cumplimiento del objetivo general

El objetivo general del proyecto planteaba diseñar un procedimiento formal de gestión de vulnerabilidades técnicas para los sistemas de información de la CAR, alineado al control 8.8 de ISO/IEC 27001:2022, que permitiera a la entidad identificar, evaluar, priorizar y reportar de manera sistemática dichas vulnerabilidades. El cumplimiento de los tres objetivos específicos la definición metodológica (Fase 1), la documentación formal (Fase 2) y la validación práctica (Fase 3) da cumplimiento integral a este objetivo general: el procedimiento no solo quedó diseñado conceptualmente, sino formalizado conforme al sistema de gestión documental de la entidad y comprobado mediante su ejecución real sobre 25 sistemas de información de la CAR, evidenciando que la entidad cuenta, a partir del presente proyecto, con una herramienta operativa, verificable y alineada al control 8.8 de ISO/IEC 27001:2022 para la gestión sistemática de sus vulnerabilidades técnicas.

Conclusiones y Recomendación

El presente proyecto diseñó, documentó y validó un procedimiento formal de gestión de vulnerabilidades técnicas para los sistemas de información de la CAR, alineado al control 8.8 de ISO/IEC 27001:2022, dando respuesta a la ausencia de un proceso institucionalizado que se había identificado en el planteamiento del problema. A diferencia de una adaptación genérica de estándares internacionales, el procedimiento se construyó a partir de las condiciones reales de la entidad la separación organizacional entre las áreas de Gobierno Digital y Desarrollo de Aplicaciones, la disponibilidad real de licenciamiento de Tenable WAS, y la ausencia de datos consolidados como el volumen de usuarios por sistema, resolviendo cada una de estas limitaciones con una decisión técnica fundamentada y documentada, en lugar de omitirlas.

La ejecución del piloto sobre 25 sistemas de información reales confirmó que el procedimiento es operativamente aplicable: permitió priorizar de manera objetiva y reproducible un universo de 48 sistemas, ejecutar pruebas de seguridad dinámica bajo una configuración técnica verificable frente a lo documentado, y clasificar y consolidar 161 hallazgos en un formato institucional estandarizado. La ausencia de hallazgos de severidad Crítica o Alta en el piloto no resta valor a esta validación, dado que el objetivo del proyecto era comprobar la aplicabilidad del procedimiento como instrumento de gestión, no producir un resultado de severidad predeterminado.

Finalmente, el proyecto demuestra que es posible construir un procedimiento de seguridad de la información técnicamente riguroso y, al mismo tiempo, plenamente conforme con el sistema de gestión documental institucional de una entidad pública colombiana el SIGESPU, sin que ambas exigencias resulten contradictorias entre sí. Esto convierte al

procedimiento en un entregable con potencial de adopción real por parte de la CAR, y no únicamente en un ejercicio académico, para la entidad, se recomienda:

- a) Surtir el proceso formal de revisión y aprobación del procedimiento GGD-PR-XX ante la Oficina Asesora de Planeación, con el fin de que se integre oficialmente al SIGESPU.
- b) Priorizar la remediación de los ocho tipos de hallazgo de severidad Media identificados en el piloto, iniciando por "OpenAPI Permissive Input Validation" (CVSS 6.8).
- c) Dada la alta recurrencia de hallazgos relacionados con cabeceras HTTP de seguridad y atributos de cookies presentes en prácticamente la totalidad de los 25 sistemas evaluados, evaluar la definición de una configuración base de seguridad HTTP aplicable de manera estandarizada a todos los sistemas de información de la entidad, en lugar de remediar cada hallazgo de forma aislada por sistema.
- d) Institucionalizar la actualización periódica del criterio de Volumen de Usuarios en el inventario de sistemas de información, de manera que en ciclos futuros este dato esté disponible como una métrica consolidada y no dependa de una valoración cualitativa ad hoc como la realizada en el presente proyecto.

Para futuros ciclos de ejecución del procedimiento, se recomienda:

- a) Ampliar la cobertura del piloto a los 23 sistemas de información restantes, priorizados según el mismo criterio de la Guía de Priorización

- b) Incorporar pruebas en modalidad autenticada, lo cual permitiría evaluar tanto los sistemas actualmente no expuestos a Internet como las vulnerabilidades específicamente asociadas a flujos internos de la aplicación, no alcanzables mediante el enfoque no autenticado adoptado en el presente proyecto.

Para futuras líneas de investigación relacionadas, se recomienda explorar la incorporación complementaria de pruebas de seguridad estática (SAST) al procedimiento, dado que la literatura consultada en el presente proyecto (Qadir et al., 2025) confirma que este enfoque resulta particularmente efectivo para la detección de hallazgos de severidad alta mediante el análisis del código fuente, una capacidad que actualmente excede el alcance organizacional del área responsable de este procedimiento, pero que podría desarrollarse en coordinación con el área de Desarrollo de Aplicaciones y Sistemas de Información en un proyecto futuro.

Referencias

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (2013). *Internal control — Integrated framework*.

Congreso de Colombia. (1993, 22 de diciembre). *Ley 99 de 1993, por la cual se crea el Ministerio del Medio Ambiente, se reordena el Sector Público encargado de la gestión y conservación del medio ambiente y los recursos naturales renovables, se organiza el Sistema Nacional Ambiental, SINA*. Diario Oficial No. 41.146.

Consejo Directivo CAR. (2025). *Acuerdo No. 27 de 2025, por el cual se determina la estructura interna de la Corporación Autónoma Regional de Cundinamarca – CAR, se establecen las funciones y responsabilidades de las dependencias que la conforman y se dictan otras disposiciones*. <https://www.car.gov.co/transparencia-y-acceso-a-la-informacion-publica/normatividad/acuerdos/yevuffff59q0ek0dx69bccpn>

Corporación Autónoma Regional de Cundinamarca. (2026a). *Creación y control de la información documentada del SIGESPU* (GSG-PR-01, Versión 16).

Corporación Autónoma Regional de Cundinamarca. (2026b). *Plan Anual de Vacantes 2026*. <https://car1.car.gov.co/vercontenido/5680>

Corporación Autónoma Regional de Cundinamarca. (2026c). *Sistema Integrado de Gestión Pública* [Mapa de procesos]. <https://www.car.gov.co/vercontenido/6>

Corporación Autónoma Regional de Cundinamarca [CAR]. (s.f.-a). *Nosotros*. <https://www.car.gov.co/nosotros>

- Corporación Autónoma Regional de Cundinamarca [CAR]. (s.f.-b). *Misión y visión*.
<https://www.car.gov.co/vercontenido/3>
- FIRST.Org, Inc. (2019). *Common Vulnerability Scoring System version 3.1: Specification document*. https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf
- Instituto Nacional de Ciberseguridad [INCIBE]. (2019). *Midiendo la severidad de las vulnerabilidades: Cambios en CVSS 3.1*. INCIBE-CERT. <https://www.incibe.es/incibe-cert/blog/midiendo-severidad-las-vulnerabilidades-cambios-cvss-31>
- International Organization for Standardization. (2015). *ISO 9001:2015 — Quality management systems — Requirements*.
- International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2018). *ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary*.
- International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2022a). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
- International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2022b). *ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls*.

International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2022c). *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.

Lozada, J. (2014). Investigación aplicada: Definición, propiedad intelectual e industria. *CienciAmérica*, 3(1), 47–50.

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2016). *Guía para la gestión y clasificación de activos de información* (Guía No. 5).

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2025). *Resolución 2277 de 2025, por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia*.

National Institute of Standards and Technology [NIST]. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-53r5>

National Institute of Standards and Technology [NIST]. (2022). *Guide to enterprise patch management planning: Preventive maintenance for technology* (NIST Special Publication 800-40 Rev. 4). <https://doi.org/10.6028/NIST.SP.800-40r4>

Open Web Application Security Project [OWASP]. (2020). *OWASP Web Security Testing Guide* (v4.2). <https://owasp.org/www-project-web-security-testing-guide/>

Open Web Application Security Project [OWASP]. (2021). *OWASP Top 10:2021*. <https://owasp.org/Top10/>

Qadir, S., Waheed, E., Khanum, A., & Jehan, S. (2025). Comparative evaluation of approaches & tools for effective security testing of Web applications. *PeerJ Computer Science*, 11, Artículo e2821. <https://doi.org/10.7717/peerj-cs.2821>

Tenable, Inc. (s.f.-a). *Authentication & Session Plugins*. Tenable.
<https://www.tenable.com/plugins/was/families/Authentication%20&%20Session>

Tenable, Inc. (s.f.-b). *Cross Site Request Forgery Plugins*. Tenable.
<https://www.tenable.com/plugins/was/families/Cross%20Site%20Request%20Forgery>

Tenable, Inc. (s.f.-c). *HTTP Security Header Plugins*. Tenable.
<https://www.tenable.com/plugins/was/families/HTTP%20Security%20Header>

Tenable, Inc. (s.f.-d). *Web Servers Plugins*. Tenable.
<https://www.tenable.com/plugins/was/families/Web%20Servers>

Anexos

Anexo A

Procedimiento GGD-PR-XX — Gestión de Vulnerabilidades Técnicas para los Sistemas de Información de la CAR

	GESTIÓN DE VULNERABILIDADES TÉCNICAS PARA LOS SISTEMAS DE INFORMACIÓN			GGD-PR-XX
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: XX-XXXX-2026	Página 1 de 6

TABLA DE CONTENIDO

Contenido

1. OBJETIVO.....	2
2. ALCANCE.....	2
3. DEFINICIONES.....	2
4. RESPONSABLES	4
5. RESPONSABILIDADES	4
6. GENERALIDADES.....	4
7. DESCRIPCIÓN DEL PROCEDIMIENTO.....	4
8. CONTROL DE CAMBIOS	7
9. ANEXOS.....	8

Elaborado por: Grupo de Mejora GGD	Revisado por: Administrador del Sistema	Aprobado Por Jefe Oficina de Gobernanza Digital y analítica de datos
--	---	--

1. OBJETIVO

Establecer los lineamientos y actividades para identificar, evaluar, priorizar y reportar las vulnerabilidades técnicas presentes en los sistemas de información de la Corporación Autónoma Regional de Cundinamarca (CAR).

2. ALCANCE

Este procedimiento inicia con la identificación de los sistemas de información objeto de evaluación, continúa con la ejecución de pruebas de seguridad dinámica (DAST), la evaluación de las vulnerabilidades técnicas identificadas, la priorización de estas vulnerabilidades, y finaliza con la elaboración y entrega del informe de resultados al área de Desarrollo de Aplicaciones y Sistemas de Información.

Este procedimiento no incluye las actividades de remediación ni de verificación de las vulnerabilidades técnicas identificadas, las cuales son responsabilidad del equipo de Desarrollo de Aplicaciones y Sistemas de Información, con base en las recomendaciones entregadas por la Oficina de Gobernanza Digital y Analítica de Datos.

3. DEFINICIONES

- **CVSS (Common Vulnerability Scoring System):** marco abierto que proporciona una metodología estandarizada de puntuación de la severidad de las vulnerabilidades, mediante métricas Base, Temporal y Ambiental.
- **DAST (Dynamic Application Security Testing):** pruebas de seguridad dinámica que evalúan una aplicación en tiempo de ejecución, sin acceso a su código fuente, simulando el comportamiento de un atacante externo.
- **Hallazgo:** vulnerabilidad técnica identificada durante la ejecución de una prueba de seguridad sobre un sistema de información.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información, habilitador de la Política de Gobierno Digital para las entidades públicas colombianas.
- **Nivel de criticidad de la prueba:** valoración asignada a cada prueba técnica DAST según la probabilidad y el impacto potencial del riesgo que evalúa, utilizada para priorizar la ejecución y el análisis de los resultados de las pruebas técnicas aplicadas sobre los sistemas de información.
- **OWASP WSTG:** Web Security Testing Guide de la fundación Open Web Application Security Project, marco de referencia metodológico para pruebas de seguridad en aplicaciones web.
- **Priorización:** proceso de ordenar los sistemas de información o los hallazgos identificados según su nivel de criticidad, exposición o severidad.
- **Severidad:** medida de la gravedad técnica de una vulnerabilidad, determinada mediante el sistema de puntuación CVSS.
- **Sistema de información:** conjunto organizado de recursos tecnológicos que permite el almacenamiento, procesamiento y transmisión de información institucional.

- **Vulnerabilidad técnica:** debilidad de un activo o control que puede ser explotada por una o más amenazas, comprometiendo la confidencialidad, integridad o disponibilidad de la información.

4. RESPONSABLES

Profesional Especializado en Seguridad de la Información de la Oficina de Gobernanza Digital y Analítica de Datos (OGDAD)

5. RESPONSABILIDADES

Identificar los sistemas de información objeto de evaluación, ejecutar las pruebas de seguridad dinámica (DAST) sobre dichos sistemas, garantizar la adecuada configuración y coordinación de las ventanas de escaneo, evaluar y clasificar los hallazgos identificados según su nivel de severidad y tipo de vulnerabilidad, elaborar y remitir oportunamente el informe de resultados, con el fin de contribuir a la identificación temprana de debilidades técnicas y a la protección de la confidencialidad, integridad y disponibilidad de la información institucional.

6. GENERALIDADES

La Corporación Autónoma Regional de Cundinamarca (CAR), en cumplimiento de su compromiso institucional con la protección de los recursos informáticos y la consolidación de una gestión ambiental apoyada en el uso estratégico de la tecnología, ha diseñado este procedimiento enfocado en identificar, analizar y reportar las vulnerabilidades presentes en sus activos tecnológicos expuestos a internet.

El desarrollo del procedimiento tiene como objetivo principal la evaluación de la superficie de exposición de los activos web institucionales, permitiendo identificar de manera temprana vulnerabilidades asociadas a los aplicativos web de la Corporación, a partir de esta identificación temprana se busca priorizar acciones de remediación y fortalecer los controles de seguridad orientados a preservar la disponibilidad, integridad y confidencialidad de la información administrada por la entidad.

La metodología adoptada para este ejercicio de verificación de vulnerabilidades se fundamenta en las directrices y buenas prácticas establecidas por el OWASP (Open Web Application Security Project), reconocidas a nivel mundial como referencia para la identificación, evaluación y mitigación de riesgos de seguridad en aplicaciones web. En particular, se tomarán como marco de referencia las vulnerabilidades descritas en el OWASP Top 10 – 2021, lo cual permitirá estructurar un enfoque integral y actualizado frente a los riesgos más críticos que enfrentan las aplicaciones modernas. A continuación, se presenta la representación gráfica del OWASP Top 10 – 2021, que servirá como base para el análisis técnico de las vulnerabilidades encontradas:

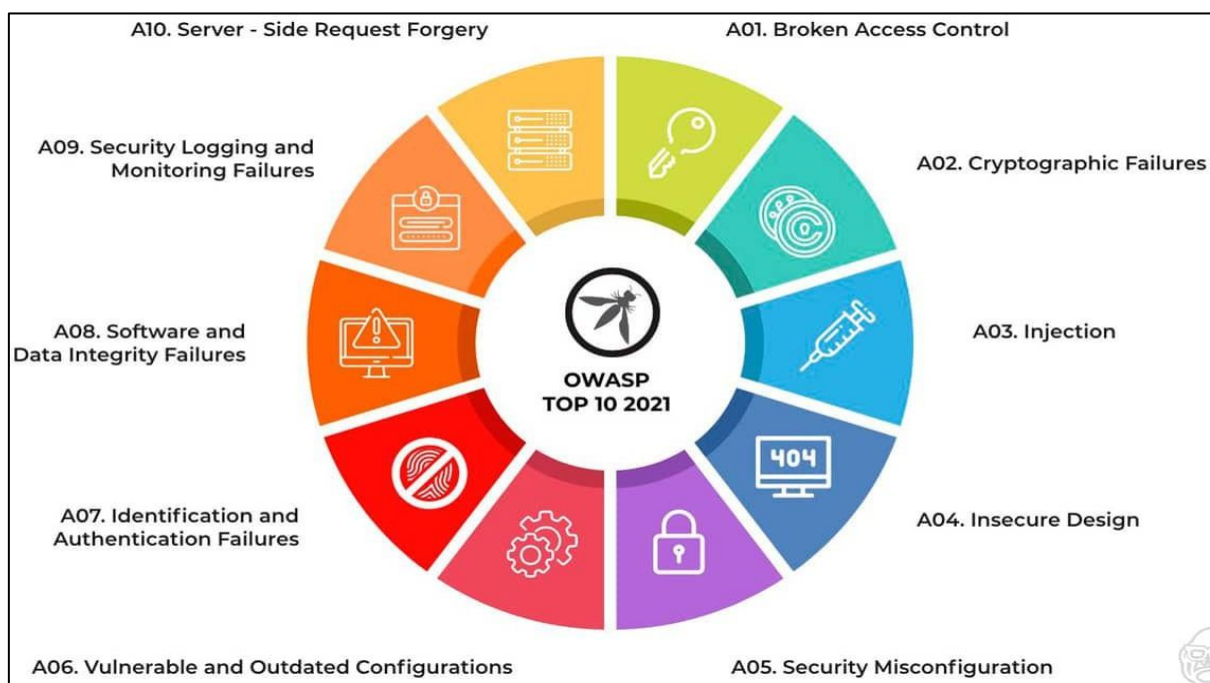


Ilustración 1 - Open Web Application Security Project. <https://owasp.org/Top10/>

Las pruebas del presente procedimiento se ejecutarán con una periodicidad anual, pudiendo ajustarse su frecuencia según la criticidad de los sistemas de información o por requerimiento de la Oficina de Gobernanza Digital y Analítica de Datos.

Las pruebas de seguridad dinámica (DAST) se ejecutarán mediante la herramienta Tenable Web Application Scanning (WAS) licenciada en la Corporación, en modalidad no autenticada, es decir sobre la superficie de los sistemas de información expuestos a Internet, a continuación, se detallan las pruebas de análisis dinámico de seguridad (DAST) que se deben ejecutar sobre los sistemas de información de la Corporación:

- **Fingerprint del servidor web:** Identificación de tecnologías, versiones de servidor y cabeceras de respuesta, con el fin de detectar posibles exposiciones por configuraciones predeterminadas o desactualizadas.
- **Identificación de puntos de entrada de las aplicaciones:** Mapeo de formularios, parámetros y endpoints accesibles desde el cliente, que puedan representar vectores de entrada para validaciones posteriores.
- **Fingerprint del framework de la aplicación:** Detección de frameworks, librerías y estructuras tecnológicas utilizadas (por ejemplo, Laravel, Django, React), con el objetivo de identificar riesgos asociados a versiones vulnerables.
- **Pruebas de configuración y gestión de implementación:** Evaluación de configuraciones inseguras, cabeceras HTTP faltantes o

mal implementadas, y errores comunes de despliegue que puedan exponer información crítica.

•**Pruebas sobre la configuración de la plataforma de la aplicación:** Análisis de aspectos como la revelación de errores internos, trazas de debug activadas o mensajes del servidor que comprometan la seguridad.

•**Pruebas de métodos HTTP:** Verificación de métodos habilitados (GET, POST, PUT, DELETE, TRACE, OPTIONS), identificando aquellos innecesarios o inseguros que puedan facilitar ataques.

•**Prueba de Strict Transport Security (HSTS):** Comprobación del uso correcto de cabeceras de seguridad que fuerzan la navegación por HTTPS y previenen ataques de downgrade o man-in-the-middle.

•**Pruebas de fijación de sesión (Session Fixation):** Evaluación de posibles debilidades en el manejo de tokens de sesión y su regeneración durante el ciclo de autenticación.

•**Pruebas de falsificación de solicitudes entre sitios (CSRF):** Verificación de mecanismos de protección contra ataques que intentan realizar acciones no autorizadas desde navegadores autenticados.

A continuación, se detalla la tabla de categorización respecto a OWASP Top 10 - 2021 de las pruebas a realizar:

Nº	Prueba Técnica	Categoría OWASP Top 10 – 2021	Objetivo de la Prueba	Nivel de Criticidad
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	Identificar versiones y tecnologías expuestas susceptibles a vulnerabilidades conocidas.	Media
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	Detectar vectores de entrada que puedan ser utilizados en ataques si no están debidamente controlados.	Alta
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	Detectar frameworks desactualizados o vulnerables utilizados por las aplicaciones.	Alta

4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	Evaluar configuraciones erróneas o inseguras que aumenten la superficie de exposición.	Alta
----------	--	---------------------------------	--	------

Nº	Prueba Técnica	Categoría OWASP Top 10 – 2021	Objetivo de la Prueba	Nivel de Criticidad
5	Prueba de la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	Verificar posibles errores de diseño o configuraciones que revelen información crítica.	Media
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	Verificar qué métodos HTTP están habilitados y si representan un riesgo.	Alta
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	Comprobar que se aplique correctamente la política de navegación segura mediante HTTPS.	Alta
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	Evaluar el manejo adecuado de tokens de sesión para evitar secuestro o reutilización.	Alta
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	Verificar si existen mecanismos de protección contra acciones no autorizadas iniciadas externamente.	Alta

Ilustración 2 - Categorización pruebas técnicas respecto a OWASP Top 10 -2021.

Para la evaluación y clasificación de las vulnerabilidades detectadas durante las pruebas será realizada con base en el Common Vulnerability Scoring System (CVSS) versión 3, estándar internacional publicado por el Forum of Incident Response and Security Teams (FIRST).

Clasificación de severidad según CVSS v3:

Nivel de Severidad	Rango de Puntuación CVSS
Crítica	9.0 – 10.0

Alta	7.0 – 8.9
Media	4.0 – 6.9
Baja	0.1 – 3.9

Ilustración 3 - Clasificación de Common Vulnerability Scoring System CVSS.

La siguiente imagen ilustra los criterios operativos utilizados para la valoración de severidad, facilitando su interpretación:

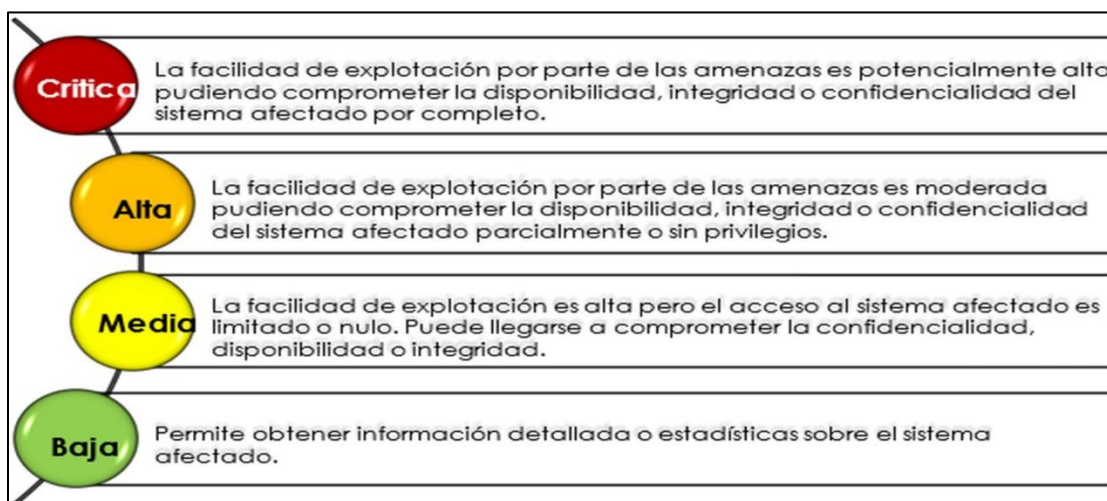


Ilustración 4 - Adaptado de Common Vulnerability Scoring System version 3.1: Specification document, por FIRST.Org, Inc., 2019 (https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf).

Este procedimiento se fundamenta en los siguientes referentes normativos y técnicos:

- ISO/IEC 27001:2022, control 8.8 – Gestión de vulnerabilidades técnicas.
- ISO/IEC 27002:2022 – Controles de seguridad de la información.
- OWASP Web Security Testing Guide (WSTG) v4.2.
- Common Vulnerability Scoring System (CVSS) v3.1 – FIRST.Org, Inc.
- NIST Special Publication 800-40, Rev. 4 – Guide to Enterprise Patch Management Planning.
- Modelo de Seguridad y Privacidad de la Información (MSPI), actualizado mediante Resolución 2277 de 2025 de MinTIC.

7. DESCRIPCIÓN DEL PROCEDIMIENTO

ITEM	ACTIVIDAD DEL PROCEDIMIENTO	AREA RESPONSABLE	CARGO RESPONSABLE
1	Identificar sistemas de Información		
1.1	Identificar y mantener actualizado el inventario de los sistemas de información de la CAR.	Oficina de Gobernanza Digital y Analítica de Datos (OGDAD)	Profesional Especializado
1.2	Generar listado de sistemas de información priorizados para evaluación. PC. En caso de que por algún motivo no se pueda realizar pruebas a la totalidad de los sistemas de información, se debe elegir la cantidad que se pueda basándose en la guía GGD-PR-XX-GI-01 Guía Priorización Sistemas de Información		
2	Realizar pruebas de seguridad dinámica (DAST)		
2.1	Configurar en la herramienta que se realizarán las pruebas los parámetros de escaneo para los sistemas de información priorizados para evaluación, registrando dicha configuración en el formato GGD-PR-XX-FR-01 (Ficha Técnica de Configuración de Escaneo).	Oficina de Gobernanza Digital y Analítica de Datos (OGDAD)	Profesional Especializado
2.2	Coordinar con equipo de desarrollo de Sistemas de Información las ventanas de ejecución de las pruebas de los sistemas de información.		
2.3	Ejecutar las pruebas de seguridad dinámica (DAST) sobre los sistemas de información priorizados, en modalidad no autenticada.		
3	Clasificar resultados de pruebas		
3.1	Evaluar y clasificar los hallazgos identificados según severidad usando como referencia el estándar CVSS v3.1.	Oficina de Gobernanza Digital y Analítica de Datos (OGDAD)	Profesional Especializado
3.2	Elaborar, mediante el formato GGD-PR-XX-FR-02 (Formato de Informe de Resultados de Pruebas de Seguridad), el informe que consolide los hallazgos identificados y las recomendaciones de remediación priorizadas.		
4	Entregar resultados de pruebas		
4.1	Remitir los informes diligenciados al área de Desarrollo de Aplicaciones y Sistemas de Información,	Oficina de Gobernanza Digital y Analítica de	Profesional Especializado

	para la remediación y verificación de los hallazgos reportados.	Datos (OGDAD)	
4.2	Realizar seguimiento semestral al equipo de Desarrollo de sistemas de información respecto al avance en la resolución de los hallazgos reportados a partir de la ejecución del procedimiento. PC. Solicitud avances al respecto de las labores realizadas relacionadas con la resolución de los hallazgos reportados.		

8. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCION DEL CAMBIO	RESPONSABLE / MEMORANDO	FECHA
1	Versión inicial	Grupo de mejora GGD	

9. ANEXOS

- GGD-PR-XX-FR-01 - Ficha Técnica de Configuración de Escaneo.

10. GGD-PR-XX-FR-02 - Formato de Informe de Resultados de Pruebas de Seguridad.

- GGD-PR-XX-GI-01 Guía Priorización Sistemas de Información

Anexo B

Guía de Priorización de Sistemas de Información (GGD-PR-XX-GI-01)

	GUÍA PARA LA PRIORIZACIÓN DE SISTEMAS DE INFORMACIÓN EN LA EJECUCIÓN DE PRUEBAS DE SEGURIDAD			GGD-PR-XX-GI-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: XX-XXXX-2026	Página 1 de 4

TABLA DE CONTENIDO

1.OBJETIVO	100
2.ALCANCE.....	101
3.METODOLOGÍA DE PRIORIZACIÓN	101
4.ESCALA DE VALORACIÓN PARA EL CÁLCULO DEL PUNTAJE DE PRIORIZACIÓN	102
5.MATRIZ DE PRIORIZACIÓN.....	102

Elaborado por: Grupo de Mejora GGD	Revisado por: Administrador del Sistema	Aprobado Por Jefe Oficina de Gobernanza Digital y analítica de datos
--	---	--

1. OBJETIVO

Establecer los criterios y la metodología para priorizar los sistemas de información de la CAR objeto de evaluación mediante pruebas de seguridad dinámica (DAST), en aquellos ciclos de ejecución del procedimiento GGD-PR-XX en los que no sea posible evaluar la totalidad de los sistemas de información de la entidad.

2. ALCANCE

Esta guía aplica a todo ciclo de ejecución del procedimiento GGD-PR-XX en el cual la totalidad de los sistemas de información de la CAR exceda la capacidad de evaluación disponible en dicho ciclo, independientemente de la causa que genere dicha restricción (licenciamiento de herramientas, capacidad técnica, disponibilidad de recursos u otro factor operativo). No aplica en aquellos ciclos en los que la totalidad de los sistemas de información pueda evaluarse sin restricción alguna.

3. METODOLOGÍA DE PRIORIZACIÓN

La priorización de sistemas de información se ejecuta mediante los siguientes pasos:

- a. Levantar o actualizar el inventario de los sistemas de información de la CAR.
- b. Valorar cada sistema en los atributos de Confidencialidad, Integridad y Disponibilidad, asignando a cada uno un nivel de Alta, Media o Baja, conforme a los lineamientos de la Guía No. 5 – Gestión y Clasificación de Activos de Información de MinTIC (MinTIC, 2016).
- c. Combinar las tres valoraciones anteriores en un único Nivel de Criticidad del sistema (Alta, Media o Baja).
- d. Valorar la Exposición a Internet del sistema (Sí / No) y su Volumen de Usuarios (Alto / Medio / Bajo).
- e. Calcular el Puntaje de Priorización de cada sistema, combinando de forma semicuantitativa el Nivel de Criticidad, la Exposición a Internet y el Volumen de Usuarios, conforme a la escala de valoración establecida en la Tabla 1 de la presente guía.
- f. Ordenar los sistemas de mayor a menor Puntaje de Priorización, generando el Listado de Sistemas Priorizados. En caso de empate en el Puntaje entre dos o más sistemas, el orden entre ellos se definirá aplicando, en su orden: (a) la Exposición a Internet, dando prioridad a los sistemas expuestos; (b) el Nivel de Criticidad, dando prioridad a Alta sobre Media sobre Baja; y (c), de persistir el empate, el orden alfabético del nombre del sistema.
- g. Seleccionar, a partir de dicho listado y en estricto orden descendente de puntaje, los sistemas que serán efectivamente evaluados en el ciclo de ejecución, según la capacidad real disponible (licenciamiento, capacidad técnica o de recursos) en dicho ciclo.

El uso de una escala de valoración semicuantitativa que combina niveles cualitativos (Alta/Media/Baja) con una puntuación numérica para permitir el ordenamiento de los sistemas es un enfoque de valoración de riesgos de activos de información reconocido por la norma ISO/IEC 27005:2022, la cual admite métodos cualitativos, cuantitativos y semicuantitativos para la valoración de las consecuencias y la probabilidad asociadas a los riesgos de seguridad de la información (ISO/IEC, 2022c). Esta guía no pretende sustituir un análisis cuantitativo de riesgo, sino ofrecer un mecanismo objetivo, trazable y de fácil aplicación para ordenar sistemas de información cuando no es posible evaluarlos en su totalidad.

4. ESCALA DE VALORACIÓN PARA EL CÁLCULO DEL PUNTAJE DE PRIORIZACIÓN

El Puntaje de Priorización de cada sistema corresponde a la suma de los tres valores asignados (Nivel de Criticidad + Exposición a Internet + Volumen de Usuarios), con un rango posible de 3 (mínima prioridad) a 8 (máxima prioridad).

CRITERIO	NIVEL	VALOR ASIGNADO
Nivel de Criticidad	Alta	3
Nivel de Criticidad	Media	2
Nivel de Criticidad	Baja	1
Exposición a Internet	Si	2
Exposición a Internet	No	1
Volumen de Usuarios	Alto	3
Volumen de Usuarios	Medio	2
Volumen de Usuarios	Bajo	1

Tabla 1 - Escala de valoración para el cálculo del puntaje de priorización.

5. MATRIZ DE PRIORIZACIÓN

Plantilla en blanco para el diligenciamiento del ejercicio de priorización en cada ciclo de ejecución del procedimiento GGD-PR-XX.

SISTEMA	NIVEL DE CRITICIDAD	EXPOSICIÓN A INTERNET	VOLUMEN DE USUARIOS	PUNTAJE

Anexo C

Ficha Técnica de Configuración de Escaneos (GGD-PR-XX-FR-01) - Plantilla en blanco

 CUNDINAMARCA	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: XX-XXXX-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	
URL objetivo	
Área / responsable del sistema	
Nivel de criticidad del sistema (Alta / Media / Baja)	

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	
Modalidad de autenticación	
Límites de rendimiento (throttling)	

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Rutas / funcionalidades excluidas	

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	
Ventana de ejecución (inicio – fin)	
Fecha real de ejecución	
Incidencias durante la ejecución (si las hubo)	

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	

6. Elaboración:

Elaborado por	Fecha

Anexo D

Formato de Informe de Resultados de Pruebas de Seguridad (GGD-PR-XX-FR-02) -

Plantilla en blanco

	FORMATO INFORME DE RESULTADOS DE ESCANEOS			GGD-PR-XX-FR-02
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: XX-XXXX-2026	Página 1 de 2

Este formato consolida los resultados de las pruebas de seguridad dinámica (DAST) ejecutadas sobre los sistemas de información de la Corporación, presentando un componente técnico (dirigido al área de Desarrollo de Aplicaciones y Sistemas de Información) y un componente gerencial (dirigido a la alta dirección).

1. Datos generales del informe:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Período de evaluación	
Número de sistemas evaluados	
Fecha de elaboración del informe	
Elaborado por	

2. Resumen ejecutivo (componente gerencial)

Síntesis del estado general de seguridad de los sistemas evaluados.

SISTEMA DE INFORMACIÓN	CRÍTICA	ALTA	MEDIA	BAJA	TOTAL

SISTEMA DE INFORMACIÓN	CRÍTICA	ALTA	MEDIA	BAJA	TOTAL
TOTAL					

Recomendaciones prioritarias:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Recomendaciones	

3. Detalle técnico de hallazgos (componente técnico)

Detalle de cada hallazgo identificado.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN

4. Conclusiones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Conclusiones generales	

5. Aprobación:

Elaborado por	Aprobado por

Anexo E

Inventario de sistemas de información de la CAR

 OFICINA DE GOBERNANZA DIGITAL Y ANALITICA DE DATOS INVENTARIO SISTEMAS DE INFORMACION DE LA CAR					
ID	Nombre de aplicación	Descripción	Prioridad	Expuesto a internet	Url acceso producción
1	PAGINA WEB 2.0	Pagina oficial CAR	ALTA	SI	https://www.car.gov.co
2	PAGINA WEB 1.0	Plataforma integral que facilita el acceso a recursos y servicios digitales para promover la gestión ambiental y el desarrollo sostenible en Cundinamarca. Ofrece información sobre proyectos de conservación, herramientas interactivas y fomenta la participación ciudadana en iniciativas medioambientales.	BAJA	SI	https://car1.car.gov.co/
3	ETNIAS	Pagina web para la etnias CAR	BAJA	SI	http://etnias.car.gov.co/
4	INTRANET 1.0	La intranet corporativa optimiza la gestión de la información interna	BAJA	SI	https://intranet.car.gov.co
5	INTRANET 2.0 (SOMOS CAR)	La intranet corporativa optimiza la gestión de la información interna	BAJA	SI	http://somos.car.gov.co/
6	ECOSISTEMA II	Aplicativo para teletrabajadores facilita el reporte, seguimiento y cargue de actividades, optimizando la gestión remota del trabajo. Permite el monitoreo de tareas, proyectos, tiempos y desempeño, mejorando la eficiencia y comunicación entre empleados y supervisores.	MEDIA	SI	https://ecosistemadigital.car.gov.co/
7	APP APLICAR 2.0	App movil con servicios CAR	ALTA	NO	App local
8	CUMBRE AMBIENTAL INTERNACIONAL - PAGINA WEB	Pagina web para la cumbre ambiental	ALTA	SI	https://cumbreambiental.car.gov.co/
9	PARQUES 2.0	Pagina web para las aulas ambientales - parques CAR	ALTA	SI	https://aulasambientales.car.gov.co/
10	SIRPA (TAQUILLAS)	Facturación en taquillas parques	ALTA	NO	App local
11	HUELLA DE CARBONO	Pagina para el registro personal de huella de carbono	MEDIA	SI	https://huella-carbono.car.gov.co
12	DIGITURNO	Turnos para atención usuarios SAC	BAJA	NO	https://172.19.200.80
13	SIGCI	Sistema de Gestion de conocimiento	BAJA	SI	https://sigci.car.gov.co/
14	ELECCIONES CAR	Gestionar de forma eficiente y transparente la elección de representantes y suplentes del sector privado ante el Consejo Directivo de la CAR. Ofrece funciones como el registro en línea de candidatos y votantes, control de ingresos, gestión de candidaturas, votación electrónica segura, y reportes en tiempo real. Garantiza la seguridad, accesibilidad y cumplimiento normativo del proceso, promoviendo la transparencia y eficiencia, al mismo tiempo que optimiza tiempos y recursos. Esto fortalece la gobernanza	ALTA	SI	https://eleccionescorporacion.car.gov.co/

		participativa y asegura que las decisiones reflejen la voluntad del sector privado.			
15	LUPPE	Link Único de Procesos y Procedimientos de la Entidad - LUPPE. Es una plataforma digital implementada por la Corporación Autónoma Regional de Cundinamarca - CAR, cuyo propósito es centralizar, administrar y permitir la consulta transparente de todo el Listado Maestro de Documentos, así como la estructura que conforma el Sistema Integrado de Planeación y Gestión de la Entidad.	ALTA	SI	https://luppe.car.gov.co/
16	NEGOCIOS VERDES	La plataforma promueve actividades económicas sostenibles que equilibran el crecimiento económico con la protección ambiental, fomentando buenas prácticas sociales, laborales y económicas. Busca reducir el impacto ambiental, generar empleo sostenible y fortalecer las economías locales a través de acciones inclusivas y responsables.	ALTA	SI	https://negociosverdes.car.gov.co
17	SIRIO BOGOTA (CON ORARBO)	Sistema de monitoreo continuo del Río Bogotá, enfocado en proteger su ecosistema y prevenir amenazas ambientales. Detecta actividades ilícitas como vertimientos ilegales, incendios forestales y tala ilegal, además de promover la educación ambiental. Utiliza tecnologías avanzadas como cámaras y sensores para monitorear y responder rápidamente	MEDIA	NO	http://siribogota.car.gov.co
18	SIDCAR - AMBIENTAL	Gestión y seguimiento de proyectos ambientales sin expediente formal. Permite organizar, monitorear el progreso en tiempo real, RESPEL, RUA MINERIA, otros	MEDIA	SI	https://sidcarambiental.car.gov.co/
19	SIDCAR - COLAB	Reemplaza SIDCAR AMBIENTAL e incluye liquidación de permisos	ALTA	SI	https://sidcar-colab.car.gov.co/
20	PORTAL USUARIOS	Portal para trámites usuarios externos CAR	ALTA	SI	https://portalusuarios.car.gov.co/
21	SIDCAR	Sistema de Gestión Documental	ALTA	SI	https://sidcar.car.gov.co
22	SIGU	El Sistema de Información de Gestión de Usuarios de la CAR optimiza la administración de datos y actividades de los usuarios internos y externos. Facilita el registro, control de accesos y permisos,	ALTA	SI	http://sigu.car.gov.co
23	SAE	Gestión de expedientes permisivos y sancionatorios en la CAR mediante digitalización, seguimiento, reduce la pérdida de datos, agiliza tiempos de respuesta e integra otros sistemas internos. Además, garantiza el cumplimiento normativo, promueve la sostenibilidad y mejora la transparencia en los procesos administrativos y ambientales.	ALTA	SI	https://sae.car.gov.co
24	SGIP	Centraliza y organiza datos sobre los predios adquiridos, incluyendo avalúos, impuestos y visitas de inspección. Permite consultas ágiles, generación de reportes en Excel y PDF, y optimiza la gestión predial,	ALTA	SI	https://sgip.car.gov.co
25	CENSO USUARIOS - PORH	Censo de Usuarios para las cuencas hídricas	MEDIA	SI	http://censousuarios.car.gov.co/
26	CDA	Monitoreo CDA	ALTA	SI	https://simaav.car.gov.co
27	FORMULACAR	FormulaCAR es una plataforma web que organiza	ALTA	SI	https://formula.car.gov.co

		la información de proyectos, aplicando la metodología del Marco Lógico para evaluar su viabilidad técnica y financiera.			o/
28	REVISTA CIENTIFICA ITTPA	Plataforma que difunde avances científicos en gestión ambiental, fomentando el acceso al conocimiento, la participación comunitaria y el respaldo a políticas de sostenibilidad.	MEDIA	SI	https://ittpa.car.gov.co/
29	SINGELIA	La página web de manejo de información ambiental facilita la gestión, almacenamiento y difusión de datos ambientales, brindando acceso a información actualizada sobre calidad del aire, agua, biodiversidad y cambio climático. Sirve como referencia centralizada para autoridades, organizaciones y el público.	MEDIA	SI	https://singelia.car.gov.co
30	SITDELIA - ENVISTA ARM	Sistema geografico con resultados del Laboratorio	MEDIA	SI	https://sitedlia.car.gov.co
31	CENDOC - CENTRO DEL DOCUMENTACIÓN	Facilita el acceso a información ambiental, promoviendo el conocimiento y la educación sobre temas ambientales. Ofrece colecciones digitales, programas educativos y asesoría en investigaciones y proyectos ambientales.	BAJA	SI	https://www.car.gov.co/cendoc
32	KOHA - CATALOGO BIBLIOGRAFICO	Catalogo bibliografico	BAJA	SI	http://catalogo.car.gov.co
33	SIE - DSPACE - BIBLIOTECA DIGITAL AMBIENTAL	Recopila, publica y preserva los recursos digitales de la corporación, promoviendo su acceso abierto y la apropiación social para fomentar la cultura ambiental. Apoya la ejecución de políticas y proyectos ambientales en la región. Para mejorar la creación, catalogación y accesibilidad de los recursos, garantizando su disponibilidad y fiabilidad.	BAJA	SI	https://sie.car.gov.co/
34	MOODLE (CONTRATISTAS - FUNCIONARIOS - SIGAM)	Moodle es un sistema de gestión de aprendizaje que facilita la capacitación continua de funcionarios y contratistas, ofreciendo acceso flexible a cursos y recursos educativos. Permite el seguimiento del progreso, evaluaciones interactivas y la certificación de los participantes, contribuyendo al desarrollo profesional y la mejora operativa de la organización.	BAJA	NO	https://cargov.sharepoint.com/:b/s/CalidaddeSoftware/IQCDpXGo8GMVRZFPPpsscgoIAWZJcKXU1qoJmOgXzwdUack?e=YfyFbS
35	SGC	El aplicativo de gestión de contratación de la CAR centraliza y automatiza los procesos contractuales, garantizando transparencia y eficiencia. Permite la gestión de contratos de inversión y funcionamiento, control presupuestal, seguimiento de pagos y cumplimiento normativo.	ALTA	NO	http://sgc.car.gov.co/
36	SIRFAC 1.0	El Aplicativo de Información de Rentas y Facturación de la CAR optimiza la gestión de ingresos, permitiendo el control de rentas, generación de facturas, cálculos automáticos y seguimiento de pagos. Integra seguridad, reportes detallados y acceso web,	ALTA	NO	http://sapwlbogpru.car.gov.co/
37	SARA	El aplicativo de nómina de la CAR centraliza y automatiza la gestión salarial, garantizando pagos puntuales, precisión y transparencia en la administración de recursos humanos, optimizando la eficiencia y el cumplimiento normativo.	ALTA	NO	http://172.19.200.229:8080/saraweb/webcommoon/acceso.jsf http://172.19.200.229:8085

38	ORION	Gestión de procesos jurídicos y disciplinarios	MEDIA	SI	https://orion.car.gov.co
39	GLPI	Software de gestión de servicios tecnológicos que optimiza la atención de incidencias y solicitudes en la CAR, mejorando la administración de recursos IT. A través de GLPI, los usuarios pueden generar tickets de soporte, hacer seguimiento y gestionar activos informáticos de manera eficiente.	MEDIA	NO	https://mesadeayuda.car.gov.co/
40	BOCHICAR	Sistema de monitoreo continuo del Río Bogotá entre Chía y Soacha, operando 24/7 para prevenir amenazas ambientales y sociales. Detecta descargas ilegales, incendios, tala, robo de recursos y otras prácticas perjudiciales. Utiliza tecnología avanzada para alertar a las autoridades y fomenta la educación ambiental para la conservación del río.	MEDIA	SI	https://visorpescar.car.gov.co
41	PESCAR BI	PESCAR integra monitoreo ambiental con Power BI, permitiendo visualizar en tiempo real datos clave sobre aire, agua, fauna y minería para una gestión más eficiente y transparente.	MEDIA	SI	http://pescarbi.car.gov.co/
42	PITCAR - PLATAFORMA DE INNOVACIÓN TERRITORIAL 1.0	Pagina del DLIA	MEDIA	SI	https://car1.car.gov.co/aboratorio/inicio
43	PESCAR II	Plataforma de monitoreo ambiental Pescar, implementada por la CAR Cundinamarca, permite supervisar en tiempo real factores clave como aire, agua, fauna y minería, facilitando la toma de decisiones para la protección ambiental.	MEDIA	SI	https://pescar.car.gov.co/
44	CONDOR	Plataforma web que permite registrar, monitorear y gestionar en tiempo real los proyectos, contratos y convenios de la CAR .-OBRAS. Ofrece un mapa georreferenciado, reportes automatizados, control de cumplimiento y acceso a documentación contractual. Además, promueve la transparencia mediante la interacción con la ciudadanía.	MEDIA	SI	https://condor.car.gov.co/
45	GEOURBANA	Sin Info	MEDIA	SI	https://geourbana.car.gov.co/
46	SICLICA - ZIPA	Sistema de información climatológica e hidrológica (SICLICA)	MEDIA	NO	https://zipa.car.gov.co
47	GEOAMBIENTAL	Sistema Información Geográfica, cargada toda la información ambiental CATASTRO -IGAC-RHIDRICO, POMCAS, AREAS PROTEGIDAS. PERMISOS	ALTA	SI	https://geoambiental.car.gov.co
48	SICOF (CONTABILIDAD - PRESUPUESTO - TESORERÍA - RENTAS)	El Sistema Integrado de Gestión Administrativa y Financiera optimiza los procesos administrativos y financieros,	ALTA	NO	http://172.19.200.25:8080

Anexo F

Fichas Técnicas de Configuración de Escaneos diligenciadas (25 sistemas)

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	LUPPE
URL objetivo	https://luppe.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de

CAMPO	DESCRIPCIÓN / DILIGENCIAR
	escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidentes durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
	PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026 Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	PAGINA WEB 2.0
URL objetivo	https://luppe.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	PORTAL USUARIOS
URL objetivo	https://portalusuarios.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
	PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026
				Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	SAE
URL objetivo	https://sae.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	SIDCAR
URL objetivo	https://sidcar.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	CUMBRE AMBIENTAL
URL objetivo	https://cumbreambiental.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	ELECCIONES CAR
URL objetivo	https://eleccionescorporacion.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCAÑEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
	PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026
				Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	FORMULACAR
URL objetivo	https://formula.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	GEOAMBIENTAL
URL objetivo	https://geoambiental.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

 CUNDINAMARCA	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST	GGD-PR-XX-FR-01
---	---	------------------------

PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3
----------------	--------------------------------------	------------------	------------------------------	----------------------

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	NEGOCIOS VERDES
URL objetivo	https://negociosverdes.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	PARQUES 2.0
URL objetivo	https://aulasambientales.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	SGIP
URL objetivo	https://sgip.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	SIDCAR - COLAB
URL objetivo	https://sidcar-colab.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidentes durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	SIGU
URL objetivo	http://sigu.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de

CAMPO	DESCRIPCIÓN / DILIGENCIAR
	escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCAÑEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	SINGELIA
URL objetivo	https://singelia.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	MEDIA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	CDA
URL objetivo	https://simaav.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	ALTA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	CONDOR
URL objetivo	https://condor.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nivel de criticidad del sistema (Alta / Media / Baja)	MEDIA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
	PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026
				Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	HUELLA DE CARBONO
URL objetivo	https://huella-carbono.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	MEDIA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	PESCAR II
URL objetivo	https://pescar.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	MEDIA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCAÑEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión	Fecha: 11-09-2026	Página 1 de 3

		1		
--	--	---	--	--

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	SIDCAR - AMBIENTAL
URL objetivo	https://sidcarambiental.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	MEDIA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	PAGINA WEB 1.0
URL objetivo	https://car1.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	BAJA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	BOCHICAR
URL objetivo	https://visorpescar.car.gov.co
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	MEDIA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

	FICHA TÉCNICA DE CONFIGURACIÓN DE ESCANEOS DE PRUEBAS DAST			GGD-PR-XX-FR-01
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: 11-09-2026	Página 1 de 3

Este formato registra los parámetros técnicos de configuración de cada escaneo de seguridad dinámica (DAST) ejecutado con la herramienta de escaneo de vulnerabilidades web de la Corporación sobre un sistema de información.

1. Datos generales del sistema evaluado:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Nombre del sistema de información	CENSO USUARIOS - PORH
URL objetivo	http://censousuarios.car.gov.co/
Área / responsable del sistema	Desarrollo de aplicaciones y sistemas de información
Nivel de criticidad del sistema (Alta / Media / Baja)	MEDIA

2. Configuración de escaneo en la herramienta de realización de pruebas:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Plantilla de escaneo utilizada	Custom Scan (familias de plugins habilitadas: Web Servers, Web Applications, HTTP Security Header, Authentication & Session, Cross Site Request Forgery)
Modalidad de autenticación	No autenticada
Límites de rendimiento (throttling)	10.000 URLs a rastrear y explorar; profundidad de directorio: 10; tamaño máximo de respuesta: 5.000.000 bytes; tiempo máximo de escaneo: 03:00:00 (HH:MM:SS); tiempo máximo de cola: 08:00:00; reducción de velocidad activada ante congestión de red.
Rutas / funcionalidades excluidas	Ninguna (no se configuraron exclusiones de ruta o funcionalidad para este piloto).

3. Pruebas técnicas DAST aplicadas:

Marcar con una X las pruebas técnicas ejecutadas sobre el sistema evaluado, conforme a la categorización establecida en el numeral de Generalidades del procedimiento GGD-PR-XX.

N.º	PRUEBA TÉCNICA	CATEGORÍA OWASP TOP 10 – 2021	¿APLICADA?
1	Fingerprint del servidor web	A06 – Vulnerable and Outdated Components	X
2	Identificación de puntos de entrada de las aplicaciones	A01 – Broken Access Control / A05 – Security Misconfiguration	X
3	Fingerprint del framework de la aplicación	A08 – Software and Data Integrity Failures	X
4	Pruebas de configuración y gestión de implementación	A05 – Security Misconfiguration	X
5	Pruebas sobre la configuración de la plataforma de la aplicación	A04 – Insecure Design / A05 – Security Misconfiguration	X
6	Pruebas de métodos HTTP	A05 – Security Misconfiguration	X
7	Prueba de HTTP Strict Transport Security (HSTS)	A02 – Cryptographic Failures	X
8	Pruebas de fijación de sesión (Session Fixation)	A07 – Identification and Authentication Failures	X
9	Pruebas de falsificación de solicitudes entre sitios (CSRF)	A01 – Broken Access Control	X

4. Coordinación y ejecución:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Fecha y hora de coordinación con Desarrollo de Aplicaciones y Sistemas de Información	10/09/2026 10:00 AM
Ventana de ejecución (inicio – fin)	11/09/2026 01:00 AM – 03:00 AM
Fecha real de ejecución	11/09/2026 01:00 AM – 03:00 AM
Incidencias durante la ejecución (si las hubo)	N/A

5. Observaciones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Observaciones generales	N/A

6. Elaboración:

Elaborado por	Fecha
Diego Contreras	11/09/2026

Anexo G

Detalle completo de hallazgos del piloto DAST

<i>Sistema</i>	<i>URL</i>	<i>Hallazgo</i>	<i>Severidad</i>	<i>CVSS</i>	<i>Familia</i>
<i>Elecciones</i>	https://eleccionescorporacion.car.gov.co/	Insecure 'Access-Control-Allow-Origin' Header	Low	2,6	HTTP Security Header
<i>Elecciones</i>	https://eleccionescorporacion.car.gov.co/	Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header
<i>Elecciones</i>	https://eleccionescorporacion.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Elecciones</i>	https://eleccionescorporacion.car.gov.co/	Permissive HTTP Strict Transport Security Policy Detected	Medium	5,8	HTTP Security Header
<i>Elecciones</i>	https://eleccionescorporacion.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Elecciones</i>	https://eleccionescorporacion.car.gov.co/	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>Elecciones</i>	https://eleccionescorporacion.car.gov.co/	Content Security Policy Missing 'Report-To'	Low	2,6	HTTP Security Header
<i>Elecciones</i>	https://eleccionescorporacion.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Formulacar</i>	https://formula.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Formulacar</i>	https://formula.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Geoambiental</i>	https://geoambiental.car.gov.co	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Geoambiental</i>	https://geoambiental.car.gov.co	Missing HTTP Strict Transport Security Policy	Medium	5,8	HTTP Security Header
<i>Geoambiental</i>	https://geoambiental.car.gov.co	Missing 'X-Frame-Options' Header	Low	2,6	HTTP Security Header
<i>Geoambiental</i>	https://geoambiental.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Geoambiental</i>	https://geoambiental.car.gov.co	Missing 'X-Content-Type-Options' Header	Low	2,6	HTTP Security Header
<i>Geoambiental</i>	https://geoambiental.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header

<i>Geoambiental</i>	https://geoambiental.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Parques 20</i>	https://aulasambientales.car.gov.co/	Insecure 'Access-Control-Allow-Origin' Header	Low	2,6	HTTP Security Header
<i>Parques 20</i>	https://aulasambientales.car.gov.co/	Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header
<i>Parques 20</i>	https://aulasambientales.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Parques 20</i>	https://aulasambientales.car.gov.co/	Password Field With Auto-Complete	Low	2,6	Authentication & Session
<i>Parques 20</i>	https://aulasambientales.car.gov.co/	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Parques 20</i>	https://aulasambientales.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Parques 20</i>	https://aulasambientales.car.gov.co/	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>Parques 20</i>	https://aulasambientales.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Negocios Verdes</i>	https://negociosverdes.car.gov.co	Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header
<i>Negocios Verdes</i>	https://negociosverdes.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Negocios Verdes</i>	https://negociosverdes.car.gov.co	Password Field With Auto-Complete	Low	2,6	Authentication & Session
<i>Negocios Verdes</i>	https://negociosverdes.car.gov.co	Permissive HTTP Strict Transport Security Policy Detected	Medium	5,8	HTTP Security Header
<i>Negocios Verdes</i>	https://negociosverdes.car.gov.co	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Negocios Verdes</i>	https://negociosverdes.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Negocios Verdes</i>	https://negociosverdes.car.gov.co	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>Negocios Verdes</i>	https://negociosverdes.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Pagina Web 20</i>	https://www.car.gov.co	Insecure 'Access-Control-Allow-Origin' Header	Low	2,6	HTTP Security Header

<i>Pagina Web 2 0</i>	https://www.car.gov.co	Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header
<i>Pagina Web 2 0</i>	https://www.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Pagina Web 2 0</i>	https://www.car.gov.co	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Pagina Web 2 0</i>	https://www.car.gov.co	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>Pagina Web 2 0</i>	https://www.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Portal usuarios</i>	https://portalusuarios.car.gov.co/	Missing HTTP Strict Transport Security Policy	Medium	5,8	HTTP Security Header
<i>Portal usuarios</i>	https://portalusuarios.car.gov.co/	Missing 'X-Frame-Options' Header	Low	2,6	HTTP Security Header
<i>Portal usuarios</i>	https://portalusuarios.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Portal usuarios</i>	https://portalusuarios.car.gov.co/	Missing 'X-Content-Type-Options' Header	Low	2,6	HTTP Security Header
<i>Portal usuarios</i>	https://portalusuarios.car.gov.co/	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Portal usuarios</i>	https://portalusuarios.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Portal usuarios</i>	https://portalusuarios.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>SAE</i>	https://sae.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>SAE</i>	https://sae.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>SAE</i>	https://sae.car.gov.co	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>SAE</i>	https://sae.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Sidcar</i>	https://sidcar.car.gov.co	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Sidcar</i>	https://sidcar.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header

<i>Sidcar</i>	https://sidcar.car.gov.co	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>Sidcar</i>	https://sidcar.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Cumbre Ambiental</i>	https://cumbreambiental.car.gov.co/	Insecure 'Access-Control-Allow-Origin' Header	Low	2,6	HTTP Security Header
<i>Cumbre Ambiental</i>	https://cumbreambiental.car.gov.co/	Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header
<i>Cumbre Ambiental</i>	https://cumbreambiental.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Cumbre Ambiental</i>	https://cumbreambiental.car.gov.co/	Permissive HTTP Strict Transport Security Policy Detected	Medium	5,8	HTTP Security Header
<i>Cumbre Ambiental</i>	https://cumbreambiental.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Cumbre Ambiental</i>	https://cumbreambiental.car.gov.co/	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>Cumbre Ambiental</i>	https://cumbreambiental.car.gov.co/	Content Security Policy Missing 'Report-To'	Low	2,6	HTTP Security Header
<i>Cumbre Ambiental</i>	https://cumbreambiental.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>SGIP</i>	https://sgip.car.gov.co	Missing 'X-Frame-Options' Header	Low	2,6	HTTP Security Header
<i>SGIP</i>	https://sgip.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>SGIP</i>	https://sgip.car.gov.co	Password Field With Auto-Complete	Low	2,6	Authentication & Session
<i>SGIP</i>	https://sgip.car.gov.co	Missing 'X-Content-Type-Options' Header	Low	2,6	HTTP Security Header
<i>SGIP</i>	https://sgip.car.gov.co	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>SGIP</i>	https://sgip.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>SGIP</i>	https://sgip.car.gov.co	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>SGIP</i>	https://sgip.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header

<i>Sidcar Colab</i>	https://sidcar-colab.car.gov.co/	Missing HTTP Strict Transport Security Policy	Medium	5,8	HTTP Security Header
<i>Sidcar Colab</i>	https://sidcar-colab.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Sidcar Colab</i>	https://sidcar-colab.car.gov.co/	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Sidcar Colab</i>	https://sidcar-colab.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>SIGU</i>	https://sigu.car.gov.co	Missing 'X-Frame-Options' Header	Low	2,6	HTTP Security Header
<i>SIGU</i>	https://sigu.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>SIGU</i>	https://sigu.car.gov.co	Missing 'X-Content-Type-Options' Header	Low	2,6	HTTP Security Header
<i>SIGU</i>	https://sigu.car.gov.co	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>SIGU</i>	https://sigu.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>SIGU</i>	https://sigu.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Singelia</i>	https://singelia.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Singelia</i>	https://singelia.car.gov.co	Password Field With Auto-Complete	Low	2,6	Authentication & Session
<i>Singelia</i>	https://singelia.car.gov.co	Access Restriction Bypass Via Origin Spoof	Medium	5	Authentication & Session
<i>Singelia</i>	https://singelia.car.gov.co	Permissive HTTP Strict Transport Security Policy Detected	Medium	5,8	HTTP Security Header
<i>Singelia</i>	https://singelia.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Singelia</i>	https://singelia.car.gov.co	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>Singelia</i>	https://singelia.car.gov.co	Content Security Policy Missing 'Report-To'	Low	2,6	HTTP Security Header
<i>Singelia</i>	https://singelia.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header

<i>CDA</i>	https://simaav.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>CDA</i>	https://simaav.car.gov.co	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>CDA</i>	https://simaav.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Huella de Carbono</i>	https://huella-carbono.car.gov.co	Insecure 'Access-Control-Allow-Origin' Header	Low	2,6	HTTP Security Header
<i>Huella de Carbono</i>	https://huella-carbono.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Huella de Carbono</i>	https://huella-carbono.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Huella de Carbono</i>	https://huella-carbono.car.gov.co	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>Huella de Carbono</i>	https://huella-carbono.car.gov.co	OpenAPI Permissive Input Validation	Medium	6,8	Web Applications
<i>Huella de Carbono</i>	https://huella-carbono.car.gov.co	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>Huella de Carbono</i>	https://huella-carbono.car.gov.co	Content Security Policy Missing 'Report-To'	Low	2,6	HTTP Security Header
<i>Huella de Carbono</i>	https://huella-carbono.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Pescar II</i>	https://pescar.car.gov.co/	Missing HTTP Strict Transport Security Policy	Medium	5,8	HTTP Security Header
<i>Pescar II</i>	https://pescar.car.gov.co/	Missing 'X-Frame-Options' Header	Low	2,6	HTTP Security Header
<i>Pescar II</i>	https://pescar.car.gov.co/	Missing 'X-Content-Type-Options' Header	Low	2,6	HTTP Security Header
<i>Pescar II</i>	https://pescar.car.gov.co/	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Pescar II</i>	https://pescar.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Sidcar Ambiental</i>	https://sidcarambiental.car.gov.co/	Missing 'X-Frame-Options' Header	Low	2,6	HTTP Security Header
<i>Sidcar Ambiental</i>	https://sidcarambiental.car.gov.co/	Password Field With Auto-Complete	Low	2,6	Authentication & Session

<i>Sidcar Ambiental</i>	https://sidcarambiental.car.gov.co/	Missing 'X-Content-Type-Options' Header	Low	2,6	HTTP Security Header
<i>Sidcar Ambiental</i>	https://sidcarambiental.car.gov.co/	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Sidcar Ambiental</i>	https://sidcarambiental.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Sidcar Ambiental</i>	https://sidcarambiental.car.gov.co/	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>Condor</i>	https://orion.car.gov.co	Missing HTTP Strict Transport Security Policy	Medium	5,8	HTTP Security Header
<i>Condor</i>	https://orion.car.gov.co	Missing 'X-Frame-Options' Header	Low	2,6	HTTP Security Header
<i>Condor</i>	https://orion.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Condor</i>	https://orion.car.gov.co	Missing 'X-Content-Type-Options' Header	Low	2,6	HTTP Security Header
<i>Condor</i>	https://orion.car.gov.co	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Condor</i>	https://orion.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Condor</i>	https://orion.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Missing HTTP Strict Transport Security Policy	Medium	5,8	HTTP Security Header
<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Missing 'X-Frame-Options' Header	Low	2,6	HTTP Security Header
<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Missing 'X-Content-Type-Options' Header	Low	2,6	HTTP Security Header
<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header
<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header

<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>Pagina Web 1 0</i>	https://car1.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Censo usuarios PORH</i>	https://censousuarios.car.gov.co/	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>Censo usuarios PORH</i>	https://censousuarios.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Censo usuarios PORH</i>	https://censousuarios.car.gov.co/	Password Field With Auto-Complete	Low	2,6	Authentication & Session
<i>Censo usuarios PORH</i>	https://censousuarios.car.gov.co/	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>Censo usuarios PORH</i>	https://censousuarios.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Bochicar</i>	https://ittpa.car.gov.co/	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>Bochicar</i>	https://ittpa.car.gov.co/	Content Security Policy Missing 'Report-To'	Low	2,6	HTTP Security Header
<i>Bochicar</i>	https://ittpa.car.gov.co/	Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header
<i>Bochicar</i>	https://ittpa.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Bochicar</i>	https://ittpa.car.gov.co/	Mixed Resource Detection	Medium	5,8	Web Applications
<i>Bochicar</i>	https://ittpa.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Bochicar</i>	https://ittpa.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Ecosistema II</i>	https://ecosistemadigital.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Ecosistema II</i>	https://ecosistemadigital.car.gov.co/	Permissive HTTP Strict Transport Security Policy Detected	Medium	5,8	HTTP Security Header
<i>Ecosistema II</i>	https://ecosistemadigital.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Ecosistema II</i>	https://ecosistemadigital.car.gov.co/	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header

<i>Ecosistema II</i>	https://ecosistemadigital.car.gov.co/	Content Security Policy Missing 'Report-To'	Low	2,6	HTTP Security Header
<i>Ecosistema II</i>	https://ecosistemadigital.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Geourbana</i>	https://geourbana.car.gov.co/	Insecure 'Access-Control-Allow-Origin' Header	Low	2,6	HTTP Security Header
<i>Geourbana</i>	https://geourbana.car.gov.co/	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Geourbana</i>	https://geourbana.car.gov.co/	Password Field With Auto-Complete	Low	2,6	Authentication & Session
<i>Geourbana</i>	https://geourbana.car.gov.co/	Insecure Cross-Origin Resource Sharing Configuration	Medium	4,3	HTTP Security Header
<i>Geourbana</i>	https://geourbana.car.gov.co/	Missing Content Security Policy	Low	2,6	HTTP Security Header
<i>Geourbana</i>	https://geourbana.car.gov.co/	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Geourbana</i>	https://geourbana.car.gov.co/	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header
<i>Luppe</i>	https://luppe.car.gov.co	Cookie Without HttpOnly Flag Detected	Low	2,6	HTTP Security Header
<i>Luppe</i>	https://luppe.car.gov.co	Cookie Without Secure Flag Detected	Low	2,6	HTTP Security Header
<i>Luppe</i>	https://luppe.car.gov.co	Password Field With Auto-Complete	Low	2,6	Authentication & Session
<i>Luppe</i>	https://luppe.car.gov.co	Password Submitted Using GET Method	Medium	5	Web Applications
<i>Luppe</i>	https://luppe.car.gov.co	PHPinfo Information Disclosure	Medium	5	Web Applications
<i>Luppe</i>	https://luppe.car.gov.co	Missing 'Cache-Control' Header	Low	2,6	HTTP Security Header
<i>Luppe</i>	https://luppe.car.gov.co	Permissive Content Security Policy Detected	Low	2,6	HTTP Security Header
<i>Luppe</i>	https://luppe.car.gov.co	Login Form Cross-Site Request Forgery	Low	2,6	Cross Site Request Forgery
<i>Luppe</i>	https://luppe.car.gov.co	Content Security Policy Missing 'Report-To'	Low	2,6	HTTP Security Header
<i>Luppe</i>	https://luppe.car.gov.co	Cookie Without SameSite Flag Detected	Low	2,6	HTTP Security Header

Anexo H

	FORMATO INFORME DE RESULTADOS DE ESCANEOS			GGD-PR-XX-FR-02
PROCESO	GESTIÓN DE GOBERNANZA DIGITAL	Versión 1	Fecha: XX-XXXX-2026	Página 1 de 2

Este formato consolida los resultados de las pruebas de seguridad dinámica (DAST) ejecutadas sobre los sistemas de información de la Corporación, presentando un componente técnico (dirigido al área de Desarrollo de Aplicaciones y Sistemas de Información) y un componente gerencial (dirigido a la alta dirección).

1. Datos generales del informe:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Período de evaluación	01 al 15 de septiembre de 2026
Número de sistemas evaluados	25
Fecha de elaboración del informe	16 de septiembre de 2026
Elaborado por	Diego Andrés Contreras Pérez

2. Resumen ejecutivo (componente gerencial)

Síntesis del estado general de seguridad de los sistemas evaluados.

SISTEMA DE INFORMACIÓN	CRÍTICA	ALTA	MEDIA	BAJA	TOTAL
Luppe	0	0	2	8	10
Singelia	0	0	2	6	8
Pagina Web 1 0	0	0	1	8	9
Elecciones	0	0	1	7	8
Negocios Verdes	0	0	1	7	8
Cumbre Ambiental	0	0	1	7	8
Huella de Carbono	0	0	1	7	8
Geoambiental	0	0	1	6	7
Portal usuarios	0	0	1	6	7
Condor	0	0	1	6	7
Bochicar	0	0	1	6	7
Geourbana	0	0	1	6	7
Ecosistema II	0	0	1	5	6
Pescar II	0	0	1	4	5
Sidcar Colab	0	0	1	3	4
Parques 2 0	0	0	0	8	8
SGIP	0	0	0	8	8
Pagina Web 2 0	0	0	0	6	6
SIGU	0	0	0	6	6
Sidcar Ambiental	0	0	0	6	6
Censo usuarios PORH	0	0	0	5	5
SAE	0	0	0	4	4
Sidcar	0	0	0	4	4
CDA	0	0	0	3	3
Formulacar	0	0	0	2	2
TOTAL	0	0	17	144	161

Recomendaciones prioritarias:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Recomendaciones	1. [Media, CVSS 6.8] OpenAPI Permissive Input Validation: Implementar validación estricta de esquemas de entrada en la definición OpenAPI/Swagger, restringiendo tipos, rangos y formatos permitidos por parámetro. 2. [Media, CVSS 5.8] Permissive HTTP Strict Transport Security Policy Detected: Ajustar la directiva HSTS especificando un max-age adecuado y evaluando la inclusión de includeSubDomains. 3. [Media, CVSS 5.8] Missing HTTP Strict Transport Security Policy: Implementar la cabecera Strict-Transport-Security en todas las respuestas HTTPS del sistema. 4. [Media, CVSS 5.8] Mixed Resource Detection: Servir la totalidad de los recursos del sitio (scripts, hojas de estilo, imágenes) mediante HTTPS, eliminando referencias a contenido HTTP no cifrado. 5. [Media, CVSS 5.0] Access Restriction Bypass Via Origin Spoof: Revisar la lógica de control de acceso basada en cabeceras Origin/Referer y reforzarla con autenticación y autorización del lado del servidor. 6. [Media, CVSS 5.0] Password Submitted Using GET Method: Modificar el formulario de autenticación para que las credenciales se envíen exclusivamente mediante el método POST. 7. [Media, CVSS 5.0] PHPinfo Information Disclosure: Eliminar o restringir el acceso público al archivo de diagnóstico phpinfo() en el entorno de producción. 8. [Media, CVSS 4.3] Insecure Cross-Origin Resource Sharing Configuration: Ajustar la configuración CORS para no combinar el origen comodín (*) con el envío de credenciales. 9. [Baja, CVSS 2.6] Insecure 'Access-Control-Allow-Origin' Header: Restringir la cabecera Access-Control-Allow-Origin a una lista explícita de orígenes autorizados, evitando el uso de comodín (*). 10. [Baja, CVSS 2.6] Cookie Without HttpOnly Flag Detected: Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente. 11. [Baja, CVSS 2.6] Cookie Without Secure Flag Detected: Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS. 12. [Baja, CVSS 2.6] Missing 'Cache-Control' Header: Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible. 13. [Baja, CVSS 2.6] Permissive Content Security Policy Detected: Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.

CAMPO	DESCRIPCIÓN / DILIGENCIAR
	14. [Baja, CVSS 2.6] Content Security Policy Missing 'Report-To': Agregar la directiva report-to/report-uri a la política CSP para monitorear violaciones de la política. 15. [Baja, CVSS 2.6] Cookie Without SameSite Flag Detected: Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF. 16. [Baja, CVSS 2.6] Missing Content Security Policy: Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación. 17. [Baja, CVSS 2.6] Missing 'X-Frame-Options' Header: Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking. 18. [Baja, CVSS 2.6] Missing 'X-Content-Type-Options' Header: Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP. 19. [Baja, CVSS 2.6] Password Field With Auto-Complete: Deshabilitar el autocompletado en los campos de contraseña mediante el atributo autocomplete="new-password". 20. [Baja, CVSS 2.6] Login Form Cross-Site Request Forgery: Implementar un token anti-CSRF único por sesión en el formulario de autenticación.

3. Detalle técnico de hallazgos (componente técnico)

Detalle de cada hallazgo identificado.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Bochicar	Mixed Resource Detection	A02 - Cryptographic Failures	Media (5.8)	Servir la totalidad de los recursos del sitio (scripts, hojas de estilo, imágenes) mediante HTTPS, eliminando referencias a contenido HTTP no cifrado.
Bochicar	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
				scripts y recursos a los estrictamente necesarios.
Bochicar	Content Security Policy Missing 'Report-To'	A04 - Insecure Design	Baja (2.6)	Agregar la directiva report-to/report-uri a la política CSP para monitorear violaciones de la política.
Bochicar	Cookie Without HttpOnly Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente.
Bochicar	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Bochicar	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Bochicar	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
CDA	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
CDA	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
CDA	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
				para mitigar ataques CSRF.
Censo usuarios PORH	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
Censo usuarios PORH	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Censo usuarios PORH	Password Field With Auto-Complete	A05 - Security Misconfiguration	Baja (2.6)	Deshabilitar el autocompletado en los campos de contraseña mediante el atributo autocomplete="new-password".
Censo usuarios PORH	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
Censo usuarios PORH	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Condor	Missing HTTP Strict Transport Security Policy	A02 - Cryptographic Failures	Media (5.8)	Implementar la cabecera Strict-Transport-Security en todas las respuestas HTTPS del sistema.
Condor	Missing 'X-Frame-Options' Header	A04 - Insecure Design	Baja (2.6)	Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Condor	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Condor	Missing 'X-Content-Type-Options' Header	N/A	Baja (2.6)	Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP.
Condor	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Condor	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Condor	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Cumbre Ambiental	Permissive HTTP Strict Transport Security Policy Detected	A02 - Cryptographic Failures	Media (5.8)	Ajustar la directiva HSTS especificando un max-age adecuado y evaluando la inclusión de includeSubDomains.
Cumbre Ambiental	Insecure 'Access-Control-Allow-Origin' Header	A05 - Security Misconfiguration	Baja (2.6)	Restringir la cabecera Access-Control-Allow-Origin a una lista explícita de orígenes autorizados, evitando el uso de comodín (*).
Cumbre Ambiental	Cookie Without HttpOnly Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Cumbre Ambiental	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Cumbre Ambiental	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Cumbre Ambiental	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
Cumbre Ambiental	Content Security Policy Missing 'Report-To'	A04 - Insecure Design	Baja (2.6)	Agregar la directiva report-to/report-uri a la política CSP para monitorear violaciones de la política.
Cumbre Ambiental	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Ecosistema II	Permissive HTTP Strict Transport Security Policy Detected	A02 - Cryptographic Failures	Media (5.8)	Ajustar la directiva HSTS especificando un max-age adecuado y evaluando la inclusión de includeSubDomains.
Ecosistema II	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Ecosistema II	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Ecosistema II	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
Ecosistema II	Content Security Policy Missing 'Report-To'	A04 - Insecure Design	Baja (2.6)	Agregar la directiva report-to/report-uri a la política CSP para monitorear violaciones de la política.
Ecosistema II	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Elecciones	Permissive HTTP Strict Transport Security Policy Detected	A02 - Cryptographic Failures	Media (5.8)	Ajustar la directiva HSTS especificando un max-age adecuado y evaluando la inclusión de includeSubDomains.
Elecciones	Insecure 'Access-Control-Allow-Origin' Header	A05 - Security Misconfiguration	Baja (2.6)	Restringir la cabecera Access-Control-Allow-Origin a una lista explícita de orígenes autorizados, evitando el uso de comodín (*).
Elecciones	Cookie Without HttpOnly Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente.
Elecciones	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Elecciones	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Elecciones	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
Elecciones	Content Security Policy Missing 'Report-To'	A04 - Insecure Design	Baja (2.6)	Agregar la directiva report-to/report-uri a la política CSP para monitorear violaciones de la política.
Elecciones	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Formulacar	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Formulacar	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Geoambiental	Missing HTTP Strict Transport Security Policy	A02 - Cryptographic Failures	Media (5.8)	Implementar la cabecera Strict-Transport-Security en todas las respuestas HTTPS del sistema.
Geoambiental	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Geoambiental	Missing 'X-Frame-Options' Header	A04 - Insecure Design	Baja (2.6)	Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Geoambiental	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Geoambiental	Missing 'X-Content-Type-Options' Header	N/A	Baja (2.6)	Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP.
Geoambiental	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Geoambiental	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Geourbana	Insecure Cross-Origin Resource Sharing Configuration	A07 - Identification and Authentication Failures	Media (4.3)	Ajustar la configuración CORS para no combinar el origen comodín (*) con el envío de credenciales.
Geourbana	Insecure 'Access-Control-Allow-Origin' Header	A05 - Security Misconfiguration	Baja (2.6)	Restringir la cabecera Access-Control-Allow-Origin a una lista explícita de orígenes autorizados, evitando el uso de comodín (*).
Geourbana	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Geourbana	Password Field With Auto-Complete	A05 - Security Misconfiguration	Baja (2.6)	Deshabilitar el autocompletado en los campos de contraseña mediante el atributo autocomplete="new-password".

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Geourbana	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Geourbana	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Geourbana	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Huella de Carbono	OpenAPI Permissive Input Validation	A03 - Injection	Media (6.8)	Implementar validación estricta de esquemas de entrada en la definición OpenAPI/Swagger, restringiendo tipos, rangos y formatos permitidos por parámetro.
Huella de Carbono	Insecure 'Access-Control-Allow-Origin' Header	A05 - Security Misconfiguration	Baja (2.6)	Restringir la cabecera Access-Control-Allow-Origin a una lista explícita de orígenes autorizados, evitando el uso de comodín (*).
Huella de Carbono	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Huella de Carbono	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Huella de Carbono	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
				scripts y recursos a los estrictamente necesarios.
Huella de Carbono	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
Huella de Carbono	Content Security Policy Missing 'Report-To'	A04 - Insecure Design	Baja (2.6)	Agregar la directiva report-to/report-uri a la política CSP para monitorear violaciones de la política.
Huella de Carbono	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Luppe	Password Submitted Using GET Method	A04 - Insecure Design	Media (5.0)	Modificar el formulario de autenticación para que las credenciales se envíen exclusivamente mediante el método POST.
Luppe	PHPinfo Information Disclosure	A01 - Broken Access Control	Media (5.0)	Eliminar o restringir el acceso público al archivo de diagnóstico phpinfo() en el entorno de producción.
Luppe	Cookie Without HttpOnly Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente.
Luppe	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Luppe	Password Field With Auto-Complete	A05 - Security Misconfiguration	Baja (2.6)	Deshabilitar el autocompletado en los campos de contraseña

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
				mediante el atributo autocomplete="new-password".
Luppe	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Luppe	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
Luppe	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
Luppe	Content Security Policy Missing 'Report-To'	A04 - Insecure Design	Baja (2.6)	Agregar la directiva report-to/report-uri a la política CSP para monitorear violaciones de la política.
Luppe	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Negocios Verdes	Permissive HTTP Strict Transport Security Policy Detected	A02 - Cryptographic Failures	Media (5.8)	Ajustar la directiva HSTS especificando un max-age adecuado y evaluando la inclusión de includeSubDomains.
Negocios Verdes	Cookie Without HttpOnly Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente.
Negocios Verdes	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
				exclusivamente por HTTPS.
Negocios Verdes	Password Field With Auto-Complete	A05 - Security Misconfiguration	Baja (2.6)	Deshabilitar el autocompletado en los campos de contraseña mediante el atributo autocomplete="new-password".
Negocios Verdes	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Negocios Verdes	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Negocios Verdes	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
Negocios Verdes	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Pagina Web 1 0	Missing HTTP Strict Transport Security Policy	A02 - Cryptographic Failures	Media (5.8)	Implementar la cabecera Strict-Transport-Security en todas las respuestas HTTPS del sistema.
Pagina Web 1 0	Missing 'X-Frame-Options' Header	A04 - Insecure Design	Baja (2.6)	Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking.
Pagina Web 1 0	Missing 'X-Content-Type-Options' Header	N/A	Baja (2.6)	Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Pagina Web 1 0	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Pagina Web 1 0	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Pagina Web 1 0	Cookie Without HttpOnly Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente.
Pagina Web 1 0	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Pagina Web 1 0	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
Pagina Web 1 0	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Pagina Web 2 0	Insecure 'Access-Control-Allow-Origin' Header	A05 - Security Misconfiguration	Baja (2.6)	Restringir la cabecera Access-Control-Allow-Origin a una lista explícita de orígenes autorizados, evitando el uso de comodín (*).
Pagina Web 2 0	Cookie Without HttpOnly Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Pagina Web 2 0	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Pagina Web 2 0	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Pagina Web 2 0	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
Pagina Web 2 0	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Parques 2 0	Insecure 'Access-Control-Allow-Origin' Header	A05 - Security Misconfiguration	Baja (2.6)	Restringir la cabecera Access-Control-Allow-Origin a una lista explícita de orígenes autorizados, evitando el uso de comodín (*).
Parques 2 0	Cookie Without HttpOnly Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo HttpOnly a las cookies de sesión para impedir su acceso desde JavaScript del lado del cliente.
Parques 2 0	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Parques 2 0	Password Field With Auto-Complete	A05 - Security Misconfiguration	Baja (2.6)	Deshabilitar el autocompletado en los campos de contraseña mediante el atributo

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
				autocomplete="new-password".
Parques 2 0	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Parques 2 0	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Parques 2 0	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
Parques 2 0	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Pescar II	Missing HTTP Strict Transport Security Policy	A02 - Cryptographic Failures	Media (5.8)	Implementar la cabecera Strict-Transport-Security en todas las respuestas HTTPS del sistema.
Pescar II	Missing 'X-Frame-Options' Header	A04 - Insecure Design	Baja (2.6)	Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking.
Pescar II	Missing 'X-Content-Type-Options' Header	N/A	Baja (2.6)	Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP.
Pescar II	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Pescar II	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store)

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
				en páginas que presenten información sensible.
Portal usuarios	Missing HTTP Strict Transport Security Policy	A02 - Cryptographic Failures	Media (5.8)	Implementar la cabecera Strict-Transport-Security en todas las respuestas HTTPS del sistema.
Portal usuarios	Missing 'X-Frame-Options' Header	A04 - Insecure Design	Baja (2.6)	Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking.
Portal usuarios	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Portal usuarios	Missing 'X-Content-Type-Options' Header	N/A	Baja (2.6)	Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP.
Portal usuarios	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Portal usuarios	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Portal usuarios	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
SAE	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
SAE	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
SAE	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
SAE	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
SGIP	Missing 'X-Frame-Options' Header	A04 - Insecure Design	Baja (2.6)	Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking.
SGIP	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
SGIP	Password Field With Auto-Complete	A05 - Security Misconfiguration	Baja (2.6)	Deshabilitar el autocompletado en los campos de contraseña mediante el atributo autocomplete="new-password".
SGIP	Missing 'X-Content-Type-Options' Header	N/A	Baja (2.6)	Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP.
SGIP	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
SGIP	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
SGIP	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
SGIP	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
SIGU	Missing 'X-Frame-Options' Header	A04 - Insecure Design	Baja (2.6)	Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking.
SIGU	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
SIGU	Missing 'X-Content-Type-Options' Header	N/A	Baja (2.6)	Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP.
SIGU	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
SIGU	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
SIGU	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
				para mitigar ataques CSRF.
Sidcar	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Sidcar	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Sidcar	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
Sidcar	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Sidcar Ambiental	Missing 'X-Frame-Options' Header	A04 - Insecure Design	Baja (2.6)	Implementar la cabecera X-Frame-Options (DENY o SAMEORIGIN) para prevenir ataques de clickjacking.
Sidcar Ambiental	Password Field With Auto-Complete	A05 - Security Misconfiguration	Baja (2.6)	Deshabilitar el autocompletado en los campos de contraseña mediante el atributo autocomplete="new-password".
Sidcar Ambiental	Missing 'X-Content-Type-Options' Header	N/A	Baja (2.6)	Implementar la cabecera X-Content-Type-Options: nosniff en todas las respuestas HTTP.
Sidcar Ambiental	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Sidcar Ambiental	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Sidcar Ambiental	Login Form Cross-Site Request Forgery	A01 - Broken Access Control	Baja (2.6)	Implementar un token anti-CSRF único por sesión en el formulario de autenticación.
Sidcar Colab	Missing HTTP Strict Transport Security Policy	A02 - Cryptographic Failures	Media (5.8)	Implementar la cabecera Strict-Transport-Security en todas las respuestas HTTPS del sistema.
Sidcar Colab	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Sidcar Colab	Missing Content Security Policy	A04 - Insecure Design	Baja (2.6)	Implementar una política de Content Security Policy (CSP) adecuada al contexto de la aplicación.
Sidcar Colab	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.
Singelia	Permissive HTTP Strict Transport Security Policy Detected	A02 - Cryptographic Failures	Media (5.8)	Ajustar la directiva HSTS especificando un max-age adecuado y evaluando la inclusión de includeSubDomains.
Singelia	Access Restriction Bypass Via Origin Spoof	A07 - Identification and Authentication Failures	Media (5.0)	Revisar la lógica de control de acceso basada en cabeceras Origin/Referer y reforzarla con autenticación y autorización del lado del servidor.

SISTEMA	HALLAZGO	CATEGORÍA OWASP TOP 10 – 2021	SEVERIDAD (CVSS)	RECOMENDACIÓN DE REMEDIACIÓN
Singelia	Cookie Without Secure Flag Detected	A05 - Security Misconfiguration	Baja (2.6)	Agregar el atributo Secure a las cookies para garantizar su transmisión exclusivamente por HTTPS.
Singelia	Password Field With Auto-Complete	A05 - Security Misconfiguration	Baja (2.6)	Deshabilitar el autocompletado en los campos de contraseña mediante el atributo autocomplete="new-password".
Singelia	Missing 'Cache-Control' Header	A04 - Insecure Design	Baja (2.6)	Configurar la cabecera Cache-Control (no-store) en páginas que presenten información sensible.
Singelia	Permissive Content Security Policy Detected	A04 - Insecure Design	Baja (2.6)	Ajustar las directivas de la política CSP para restringir los orígenes de scripts y recursos a los estrictamente necesarios.
Singelia	Content Security Policy Missing 'Report-To'	A04 - Insecure Design	Baja (2.6)	Agregar la directiva report-to/report-uri a la política CSP para monitorear violaciones de la política.
Singelia	Cookie Without SameSite Flag Detected	A01 - Broken Access Control	Baja (2.6)	Configurar el atributo SameSite (Strict o Lax) en las cookies de sesión para mitigar ataques CSRF.

4. Conclusiones:

CAMPO	DESCRIPCIÓN / DILIGENCIAR
Conclusiones generales	El piloto de pruebas de seguridad dinámica (DAST) ejecutado sobre los 25 sistemas de información priorizados identificó un total de 161 hallazgos, correspondientes a 20 tipos distintos de vulnerabilidad, sin registrar hallazgos de severidad Crítica ni Alta en ninguno de los

CAMPO	DESCRIPCIÓN / DILIGENCIAR
	sistemas evaluados. La totalidad de los hallazgos se concentró en las severidades Media (17) y Baja (144), asociados principalmente a debilidades de configuración de cabeceras HTTP de seguridad y de atributos de cookies, categorizadas mayoritariamente bajo las categorías A04 (Insecure Design), A01 (Broken Access Control) y A05 (Security Misconfiguration) del OWASP Top 10:2021. Se recomienda priorizar la remediación de los 8 tipos de hallazgo de severidad Media, iniciando por "OpenAPI Permissive Input Validation" (CVSS 6.8), y posteriormente abordar de forma estandarizada los hallazgos de severidad Baja mediante el establecimiento de una configuración base de cabeceras de seguridad HTTP aplicable a todos los sistemas de información de la entidad, dada la alta recurrencia de este tipo de hallazgos entre los 25 sistemas evaluados.

5. Aprobación:

Elaborado por	Aprobado por
Diego Andrés Contreras Pérez	