INFORME EJECUTIVO	
LUGAR: Secretaria de TIC	**FECHA:** 19/07/2022
NOMBRE: German Yobany Beltran Rondon	**CARGO:** Secretaria de TIC
PROCESO: Gestión de TIC	
SUB-PROCESO: No Aplica	
ASUNTO: Informe de análisis Ciberseguridad del Portal Web **www.alcaldianeiva.gov.co**	

Acorde a los lineamientos establecidos por MINTIC la entidad debe adoptar medidas para garantizar la seguridad digital y mitigar riesgos de incidentes cibernéticos o filtración de datos personales o sensibles en sus servicios digitales es por ello que la Alcaldía de Neiva ha trabajo en la implementación y mejora continua de su sistema de gestión de seguridad y privacidad (MSPI) de la información, conforme con las buenas prácticas internacionales, basándose en estándares como la ISO 27000 y/o los recomendados por el Instituto Nacional de Tecnología y Estándares (NIST, por sus siglas en inglés).

Es así, como la entidad ha implementado controles como los enumerados a continuación para garantizar la protección de sus servicios digitales:

1. Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).
2. Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios.
3. Ocultar y restringir páginas de acceso administrativo.
4. Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.
5. Crear copias de respaldo.
6. Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.
7. Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones.
8. Revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Project (OWASP).
9. Implementar monitoreos de seguridad sobre la plataforma tecnológica que hace parte del sitio web (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios).
10. Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.

Adicional a esto, se han implementado las siguientes medidas a nivel de programación del código fuente:

1. Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones.
2. Cumplir con la estandarización de código fuente para portales web, siguiendo las buenas prácticas del W3C (World

Web Wide Consortium), de forma que permita la correcta visualización de la información a los usuarios.
3. Cumplir con los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO, incluyendo la validación de la codificación.
4. Incluir lenguaje común de intercambio para la generación y divulgación de la información y datos estructurados y no estructurados dispuestos en medios electrónicos, como los sitios web de los sujetos obligados y el Portal Único del Estado Colombiano GOV.CO.

Es por lo que en el presente informe, se plasma el análisis de estado del portal web de la entidad teniendo en cuenta los parámetros de seguridad y las pruebas de ciberseguridad realizadas por el personal de la entidad así:

Análisis de vulnerabilidades:

1. Rastreo de origen DNS:

Se realiza la labor de rastreo del direccionamiento y registros DNS asociados al portal web: www. alcaldianeiva.gov.co, se evidencia que el portal nos arroja datos sobre la tecnología utilizada, dirección IP, y proveedor de internet.

Esto se cataloga como una vulnerabilidad dado que permite establecer entornos para direccionar posibles ataques cibernéticos al portal.

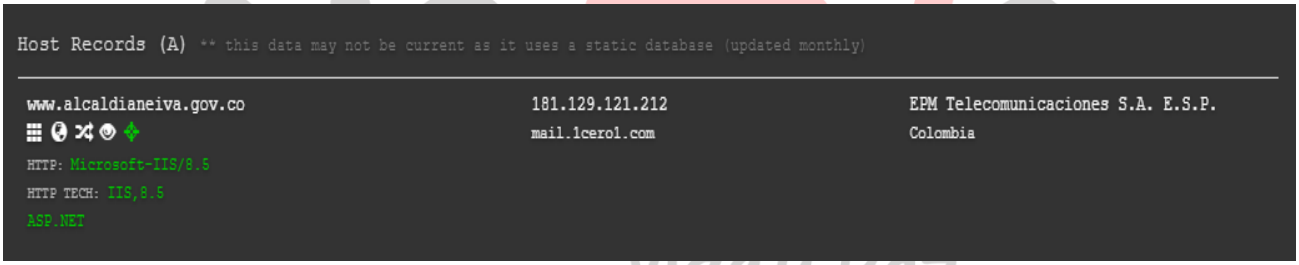

Ilustración 1 Reporte de rastro DNS.

2. Escaneo de vulnerabilidades

Se realiza el escaneo de vulnerabilidades a través del direccionamiento encontrado para verificar si el portal cuenta con las medidas de protección necesarias a nivel de ciberseguridad para esto se utilizan dos escáner web: shodan.io y censys.oi:

a. Shodan:

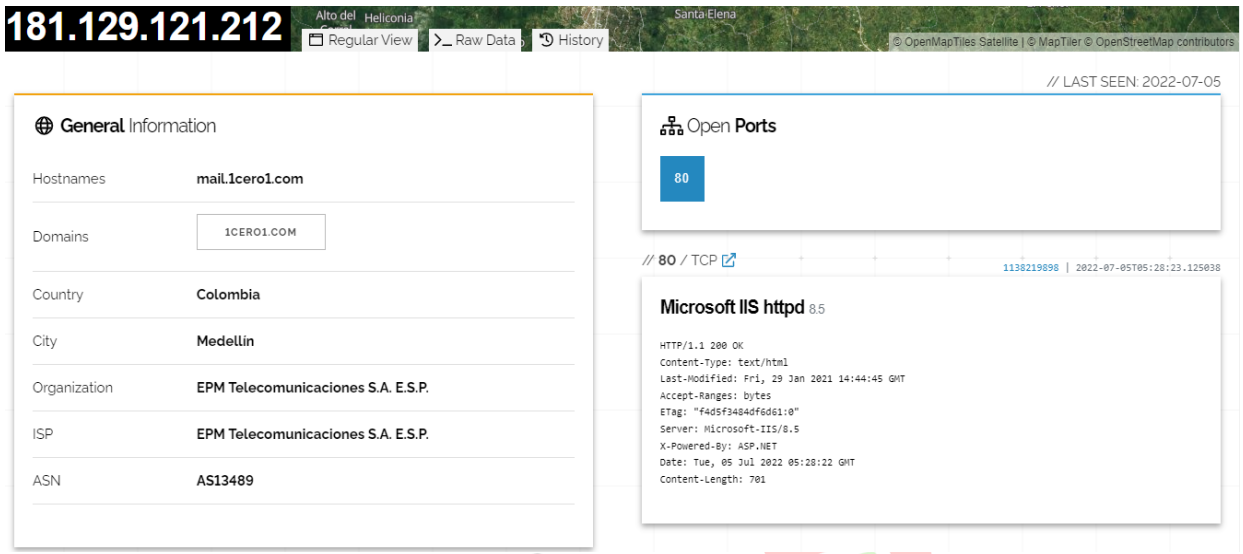

Ilustración 2 Información del servidor web recopilada.

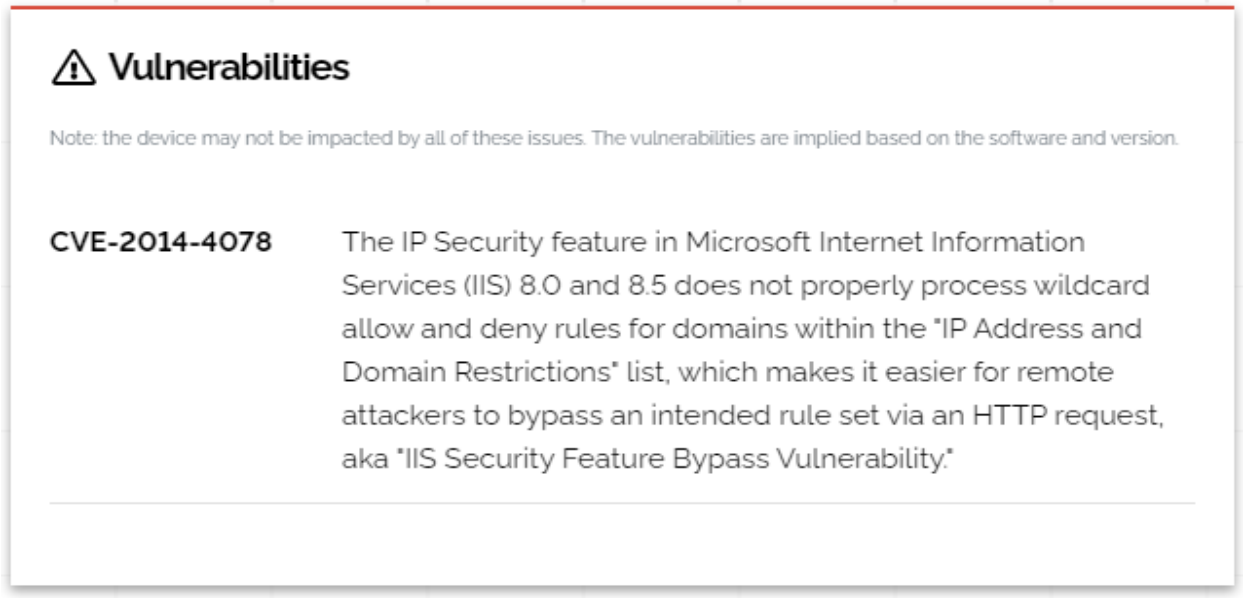

Ilustración 3 Vulnerabilidades reportadas.

Este resultado nos arroja vulnerabilidades sobre el servidor web utilizado IIS CVE-2014-4078

b. Censys

Ilustración 4 Información de servidor web recopilada.

Ilustración 5 Información de cabeceras http publicadas en el puerto 80

80/HTTP TCP

View Definition

Attribute	Value
services.banner	HTTP/1.1 200 OK\r\nContent-Type: text/html\r\nContent-Encoding: gzip\r\nLast-Modified: Fri, 29 Jan 2021 14:44:45 GMT\r\nAccept-Ranges: bytes\r\nETag: "f4d5f3484df6d61:0"\r\nVary: Accept-Encoding\r\nServer: Microsoft-IIS/8.5\r\nX-Powered-By: ASP.NET\r\nDate: <REDACTED>\nContent-Length: 608\r\n
services.banner_hex	485454502f312e3120323030204f4b0d0a436f6e74656e742d547970653a20746578742f68746d6c0d0a436f6e74656e742d456e636f64696e673a20677a69700d0a4c6173742d4d6f6469666965643a204672692c203239204a616e20323032312031343a34343a343520474d540d0a4163636570742d52616e6765733a2062797465730d0a455461673a2022663464356633343834646636643631 3a30220d0a566172793a204163636570742d456e636f64696e670d0a5365727665723a204d6963726f736f66742d4949532f382e350d0a582d506f77657265642d42793a204153502e4e45540d0a446174653a20203c5245444143544543e0a436f6e74656e742d4c656e6774683a203630380d0a
services.extended_service_name	HTTP
services.http.request.method	GET
services.http.request.uri	http://181.129.121.212/
services.http.request.headers.User_Agent	Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)
services.http.request.headers.Accept	*/*
services.http.response.protocol	HTTP/1.1

Ilustración 6 Información de cabeceras http publicadas en el puerto 80

Este resultado nos arroja vulnerabilidades similares sobre el mismo tipo de servidor, adicional no nos muestra ningún tipo de protección en las cabeceras http del portal.

De igual manera se realiza un escaneo de los puertos del servidor para verificar si hay más entornos vulnerables asociados:

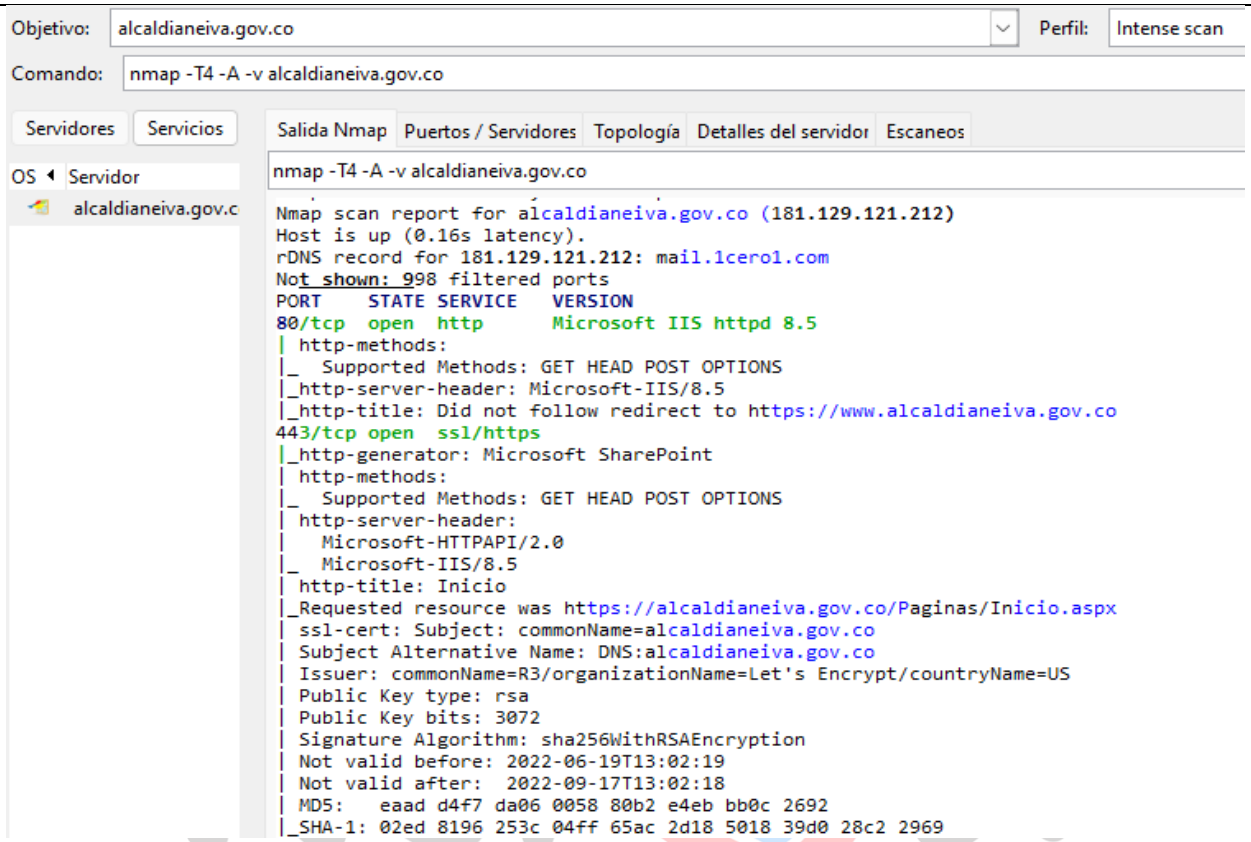

Ilustración 7 Análisis NMAP

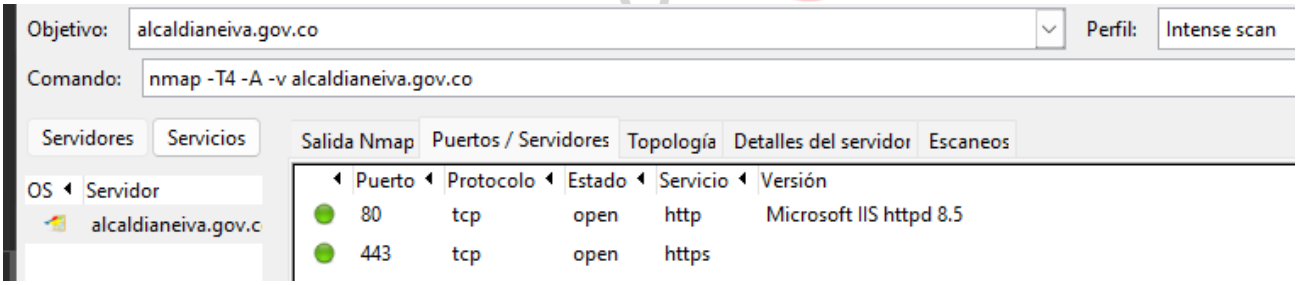

Ilustración 8 Resultados NMAP

Se evidencia el estado de puertos abiertos 80 y 443 para http y https respectivamente, se aprovecha esto para realizar un análisis con la herramienta OWASP ZAP:

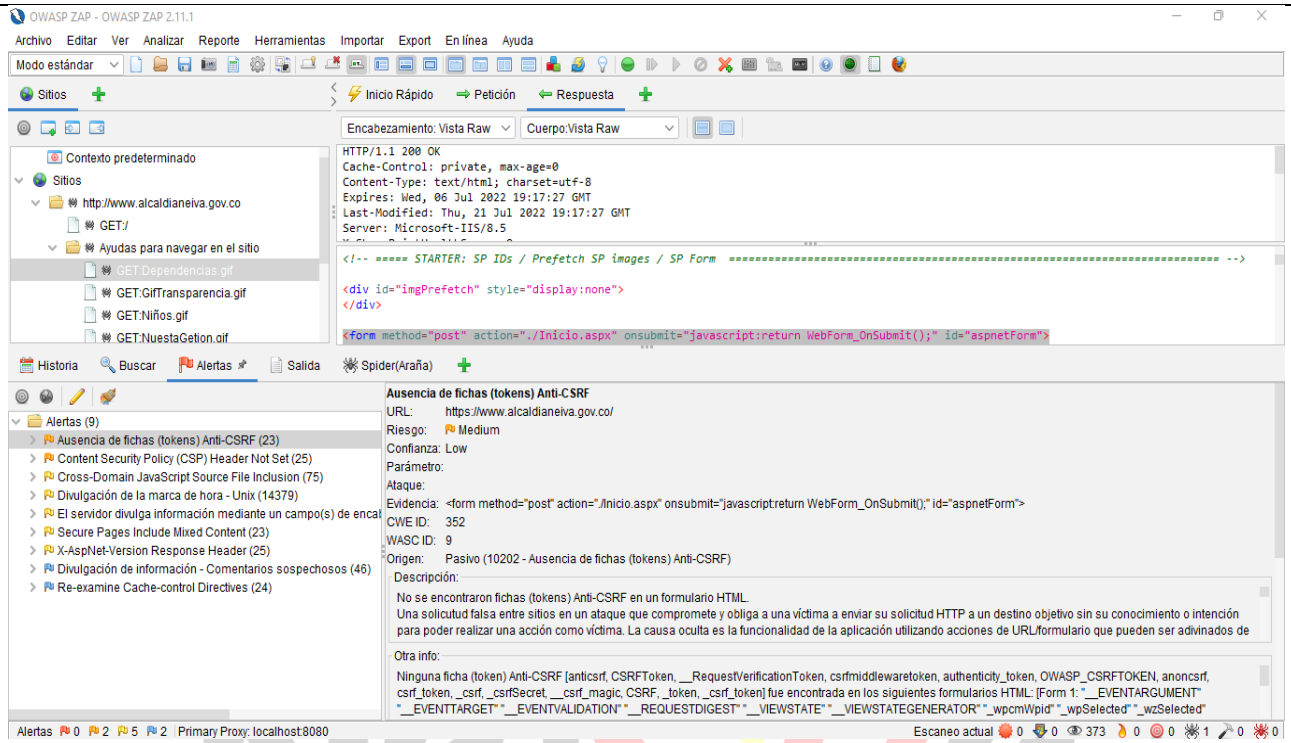

Ilustración 9 Análisis OWASP

En este análisis el sitio nos reporta 9 alertas relacionadas a la codificación del sitio y divulgación de información por parte del servidor web.

Este análisis de vulnerabilidades nos permite adoptar las medidas necesarias para garantizar las protección de la información de nuestros usuarios e impedir que cibercriminales exploten las vulnerabilidades reportadas. La secretaria de TIC trabaja constantemente en la mejora continua de sus procesos y de los lineamientos establecidos en la política general de seguridad de la información de la entidad.

Atentamente,

GERMAN YOBANY BELTRAN RONDON
Secretario de TIC.

Proyecto:
Luis Ernesto Arias Méndez.
Contratista - Esp. Seguridad de la información.