


	INFORME EJECUTIVO	FOR-GGMIPG-17	
		Versión: 01	
		Vigente desde: Marzo 19 del 2021	

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	
<p>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 trabajado 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).</p> <p>Es así, como la entidad ha implementado controles como los enumerados a continuación para garantizar la protección de sus servicios digitales:</p> <ol style="list-style-type: none"> 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. <p>Adicional a esto, se han implementado las siguientes medidas a nivel de programación del código fuente:</p> <ol style="list-style-type: none"> 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 	

La versión vigente y controlada de este documento, solo podrá ser consultada a través del link SG www.alcaldianeiva.gov.co. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es responsabilidad de la Alcaldía de Neiva

	INFORME EJECUTIVO	FOR-GGMIPG-17	
		Versión: 01	
		Vigente desde: Marzo 19 del 2021	

- Web Wide Consortium), de forma que permita la correcta visualización de la información a los usuarios.
- Cumplir con los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO, incluyendo la validación de la codificación.
 - 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.

```
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

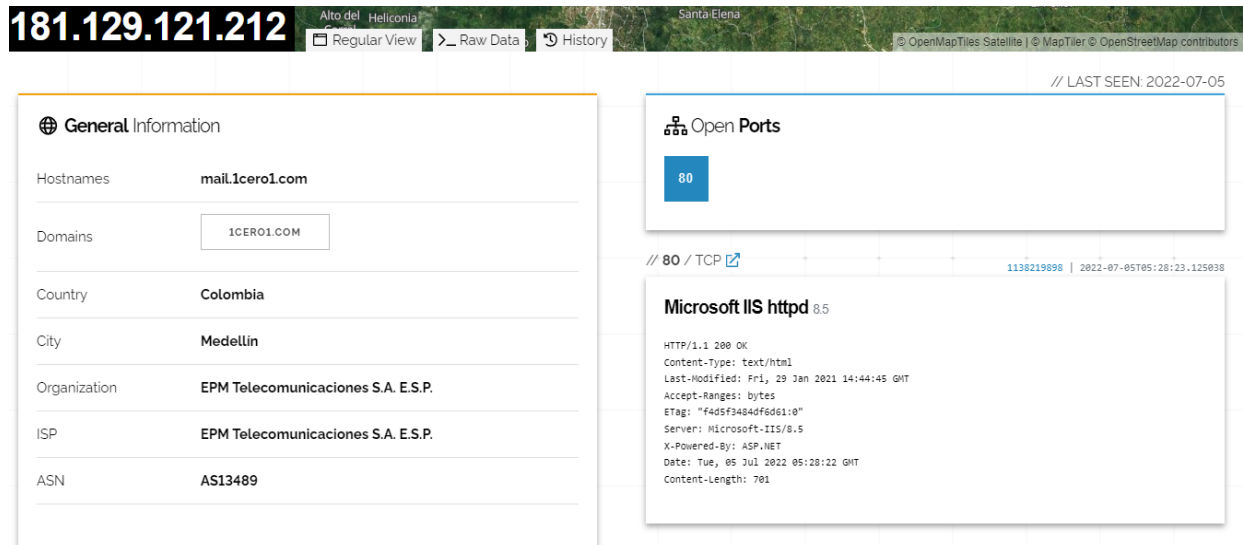
www.alcaldianeiva.gov.co      181.129.121.212      EPM Telecomunicaciones S.A. E.S.P.
📄 🌐 🛡️ 🟢                               mail.1cerol.com      Colombia
HTTP: Microsoft-IIS/8.5
HTTP TECH: IIS,8.5
ASP.NET
```

Ilustración 1 Reporte de rastreo 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.io:

a. Shodan:



181.129.121.212 Alto del Heliconia Santa Elena

Regular View Raw Data History

OpenMapTiles Satellite MapTiler OpenStreetMap contributors

// LAST SEEN: 2022-07-05

General Information

Hostnames: mail.1cero1.com

Domains: 1CERO1.COM

Country: Colombia

City: Medellin

Organization: EPM Telecomunicaciones S.A. E.S.P.

ISP: EPM Telecomunicaciones S.A. E.S.P.

ASN: AS13489

Open Ports

80

// 80 / TCP

1138219898 | 2022-07-05T05:28:23.125838

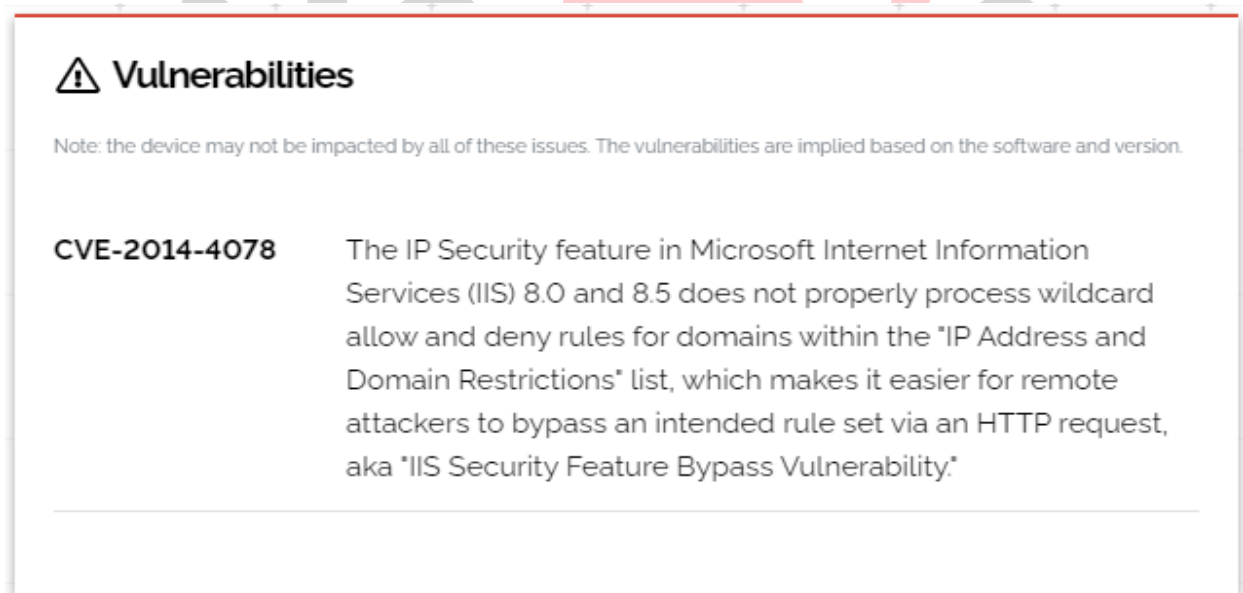
Microsoft IIS httpd 8.5

```

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 29 Jan 2021 14:44:45 GMT
Accept-Ranges: bytes
ETag: "f4d5f34040f6061:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Tue, 05 Jul 2022 05:28:22 GMT
Content-Length: 701

```

Ilustración 2 Información del servidor web recopilada.







Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-4078 The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

Ilustración 3 Vulnerabilidades reportadas.

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

 	INFORME EJECUTIVO	FOR-GGMIPG-17	 
		Versión: 01	
		Vigente desde: Marzo 19 del 2021	

b. Censys

181.129.121.212

As of: Jul 21, 2022 8:07am UTC | Latest

[Summary](#)
[Explore](#)
[History](#)
[WHOIS](#)

Basic Information

OS	Microsoft Windows Server 2012 R2
Network	EPM Telecomunicaciones S.A. E.S.P. (CO)
Routing	181.129.0.0/16 via AS8065
Protocols	80/HTTP , 4100/HTTP

Ilustración 4 Información de servidor web recopilada.

80/HTTP

TCP

Observed Jul 21, 2022 at 6:01am UTC

Software

[VIEW ALL DATA](#)

[GO](#)

- [Microsoft IIS 8.5](#)
- [Microsoft Windows](#)
- [Microsoft ASP.NET](#)
- [Microsoft Windows Server 2012 R2](#)

Details

http://181.129.121.212

Request	GET /
Protocol	HTTP/1.1
Status Code	200
Status Reason	OK
Body Hash	sha1:aef6cc11166bfd1a98960aca00a894dec6ac5a2e
HTML Title	IIS Windows Server
Response Body	EXPAND

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>\r\nContent-Length: 608\r\n
services.banner_hex	485454502f312e3120323030204f4b0d0a436f6e74656e742d547970653a20746578742f68746d6c0d0a436f6e74656e742d456e636f64696e673a20677a69700d0a4c6173742d4d6f6469666665643a204672692c203239204a616e20323032312031343a34343a343520474d540d0a4163636570742d52616e6765733a2062797465730d0a455461673a20226634643566333438346466366436313a30220d0a566172793a204163636570742d456e636f64696e670d0a5365727665723a204d6963726f736f66742d4949532f382e350d0a582d506f77657265642d42793a204153502e4e45540d0a446174653a20203c52454441435445443e0a436f6e74656e742d4c656e6774683a203630380d0a
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:

Objetivo: Perfil:

Comando:

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS Servidor
alcaldianeiva.gov.c

```

nmap -T4 -A -v alcaldianeiva.gov.co
Nmap scan report for alcaldianeiva.gov.co (181.129.121.212)
Host is up (0.16s latency).
rDNS record for 181.129.121.212: mail.1cerol.com
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 8.5
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_   _http-server-header: Microsoft-IIS/8.5
|_   _http-title: Did not follow redirect to https://www.alcaldianeiva.gov.co
443/tcp    open  ssl/https
|_ http-generator: Microsoft SharePoint
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_   http-server-header:
|_     Microsoft-HTTPAPI/2.0
|_     Microsoft-IIS/8.5
|_   http-title: Inicio
|_ Requested resource was https://alcaldianeiva.gov.co/Paginas/Inicio.aspx
ssl-cert: Subject: commonName=alcaldianeiva.gov.co
Subject Alternative Name: DNS:alcaldianeiva.gov.co
Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
Public Key type: rsa
Public Key bits: 3072
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2022-06-19T13:02:19
Not valid after: 2022-09-17T13:02:18
MD5:      eaad d4f7 da06 0058 80b2 e4eb bb0c 2692
SHA-1:    02ed 8196 253c 04ff 65ac 2d18 5018 39d0 28c2 2969

```

Ilustración 7 Análisis NMAP

Objetivo: Perfil:

Comando:



Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

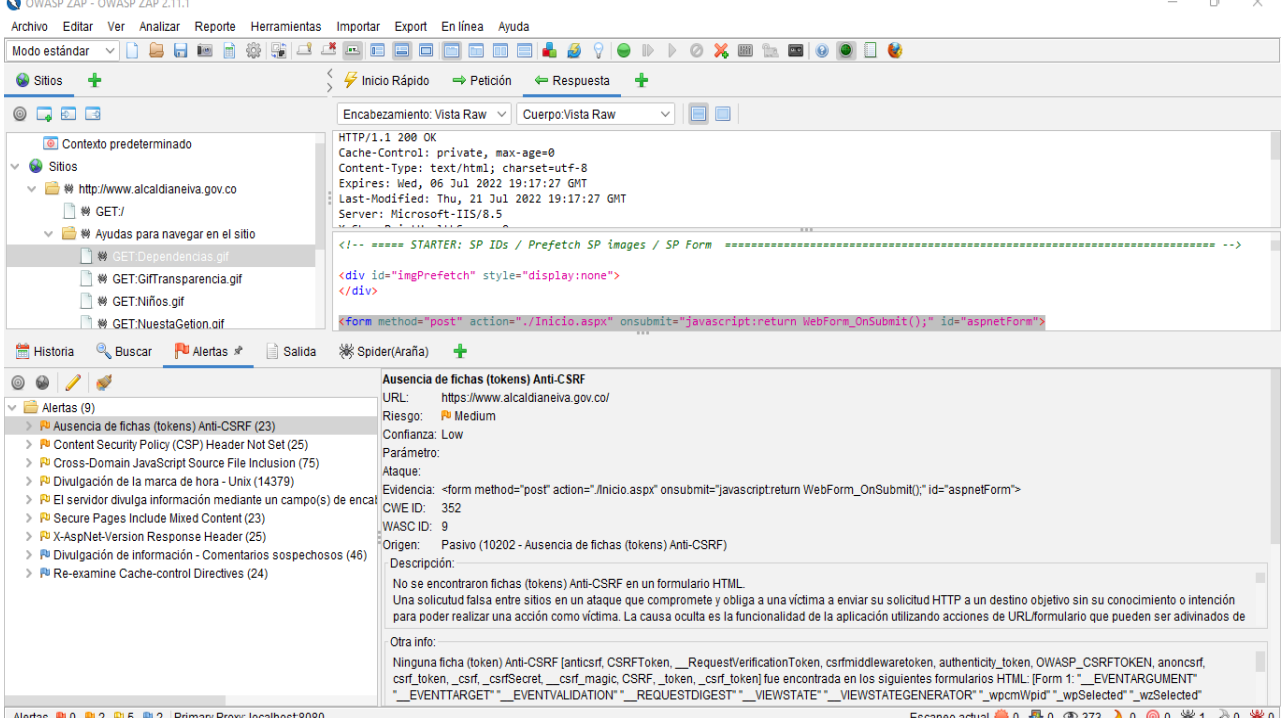
OS Servidor
alcaldianeiva.gov.c

Puerto	Protocolo	Estado	Servicio	Versión
80	tcp	open	http	Microsoft IIS httpd 8.5
443	tcp	open	https	

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:

	INFORME EJECUTIVO	FOR-GGMIPG-17	
		Versión: 01	
		Vigente desde: Marzo 19 del 2021	



Ausencia de fichas (tokens) Anti-CSRF
 URL: https://www.alcaldianeiva.gov.co/
 Riesgo: Medium
 Confianza: Low
 Parámetro:
 Ataque:
 Evidencia: <form method="post" action="/Inicio.aspx" onsubmit="javascript:return WebForm_OnSubmit(); id="aspnetForm">
 CWE ID: 352
 WASC ID: 9
 Origen: Pasivo (10202 - Ausencia de fichas (tokens) Anti-CSRF)
 Descripción:
 No se encontraron fichas (tokens) Anti-CSRF en un formulario HTML.
 Una solicitud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de

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 la 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.