Entidad	Fondo de Previsión Social del Congreso de la República – FONPRECON
Fecha de la prueba	24/06/2025
Fecha de reporte	25/06/2025
Tipo de reporte	Prueba de Vulnerabilidades
Activo	https://www.fonprecon.gov.co/
Observaciones	Ninguna

Glosario de términos: [1]

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Son un conjunto de medidas y prácticas que las organizaciones implementan para proteger la confidencialidad, integridad y disponibilidad de la información.
- **CVE:** (Common Vulnerabilities and Exposures), es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware que está desarrollado y mantenido por el MITRE con el respaldo de la comunidad de ciberseguridad. CVE proporciona una base de datos de referencia que permite a los investigadores de seguridad, fabricantes y responsables de seguridad de las organizaciones identificar y gestionar de manera más eficiente los problemas de seguridad.

[1] https://www.iso27000.es/glosario.html

- **CWE:** CWE (Common Weakness Enumeration) se puede ver como un diccionario, cuyo propósito principal es identificar y clasificar vulnerabilidades comunes que pueden existir en el software y los sistemas. Al catalogar estas vulnerabilidades, el CWE provee de un lenguaje común y detallado para discutir y abordar los riesgos.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Matriz Mitre:** La organización MITRE ha desarrollado una matriz para el seguimiento y análisis de los incidentes detectados en el mundo industrial que recopila gran parte de las tácticas, técnicas y procedimientos utilizados.
- **Mitre:** Es una organización estadounidense sin fines de lucro con sedes en Bedford, Massachusetts, y McLean, Virginia. Administra centros de investigación y desarrollo financiados por el gobierno federal (FFRDC) que apoyan a varias agencias del gobierno de los EE. UU. en los campos de la aviación, la defensa, la atención médica, la seguridad nacional y la ciberseguridad.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

NOTA: La información contenida en el presente documento tiene como finalidad informar a la entidad su postura de seguridad de los activos informáticos expuestos en Internet, de manera que sean tomadas las medidas pertinentes y apropiadas de cara a minimizar la probabilidad de ocurrencia de algún evento que pueda comprometer la Disponibilidad, Confidencialidad e Integridad de la Información allí gestionada. De igual manera, desde el CISRT Salud se exime cualquier tipo de responsabilidad sobre las labores de mitigación desarrolladas, ya que las recomendaciones presentadas obedecen a las buenas prácticas de

seguridad documentadas, las cuales servirán de apoyo y consulta para una evaluación y análisis en profundidad por parte de los responsables encargados al interior de la organización, de manera tal que no se vean impactados los servicios de las aplicaciones objeto de mitigación.

Resumen del informe:

Como parte del ejercicio de monitoreo realizado por el CSIRT Salud, fue realizado un nuevo escaneo de vulnerabilidades sobre la URL: https://www.fonprecon.gov.co/, perteneciente al *Fondo de Previsión Social del Congreso de la República – FONPRECON*, con el fin de evaluar los avances en la mitigación de las vulnerabilidades reportadas en los periodos anteriores y la validación de la presencia de nuevas alertas a considerar.

Detalles del escaneo de vulnerabilidades:

Para el desarrollo de la presente actividad, fue empleado la herramienta WAS (Web Aplication Scanning) de Tenable que hace parte de las herramientas de monitoreo de seguridad adquiridas por el Ministerio de Salud y Protección Social para la implementación del CSIRT Salud.

Las pruebas realizadas fueron bajo el escenario de caja negra, es decir, sin credenciales o información sobre el activo a escanear y principalmente con la data que podría obtener un tercero que accede a la aplicación desde internet. Dicho escenario no emplea técnicas invasivas sobre los objetos analizados, por lo cual no hay afectación alguna sobre los servicios prestados.

Listado de vulnerabilidades:

Es importante destacar que es necesario revisar cuidadosamente los resultados aquí presentados ya que dichas novedades exponen a la entidad a una amplia variedad de ataques que pueden comprometer la confidencialidad, integridad y disponibilidad de la información que es gestionada a través dicho portal.

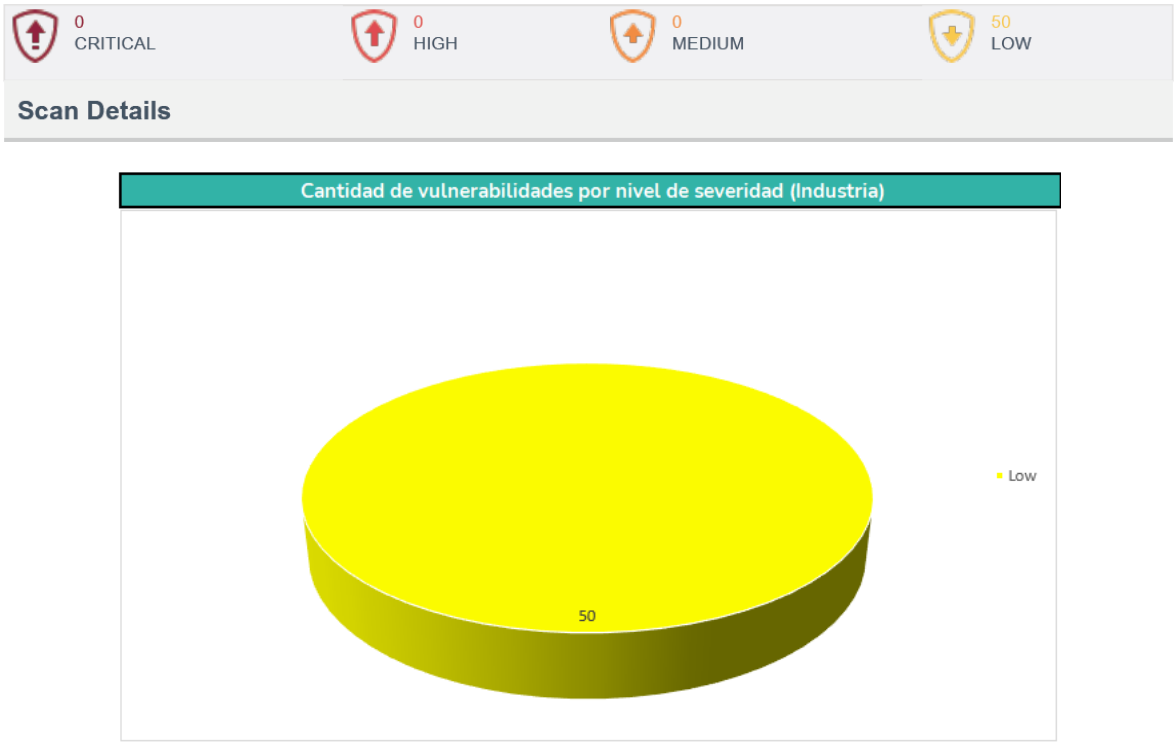


Figura 1. Resultados obtenidos

El 100% de las vulnerabilidades encontradas tienen categoría baja, por lo que la URL tiene un riesgo poco significativo que pueda llegar afectar la confidencialidad, integridad o disponibilidad de la información allí contenida.

Severidad	Nombre	Familia	Instancias	CVSSv3 Base Score	Remediación:
Low	Permissive Content Security Policy Detected	HTTP Security Header	25	3.1	La Política de Seguridad de Contenido (CSP) es un estándar de seguridad web que ayuda a mitigar ataques como el cross-site scripting (XSS), el clickjacking o problemas de contenido mixto. La CSP proporciona mecanismos a los sitios web para restringir el contenido que los navegadores pueden cargar.
Low	Content Security Policy Missing 'Report-To'	HTTP Security Header	25	3.1	Agregue la directiva 'report-to' a su encabezado de Política de seguridad de contenido existente.

Análisis de resultados:

- Como resultado de la prueba realizada fue encontrado que la URL de la entidad no posee vulnerabilidades críticas, altas, ni medias, lo que denota un nivel adecuado de seguridad a este activo tecnológico.

- De las vulnerabilidades categorizadas como bajas, es recomendado validar las configuraciones de seguridad de las cabeceras HTTP de manera que se cuenten con todos los mecanismos de protección a disposición.

Aspectos por tener en cuenta:

Conforme a las mitigaciones planteadas en el presente documento, se profundizan a continuación aspectos relevantes que deben ser tenidos en cuenta previo a la definición del plan de trabajo para las remediaciones:

Amenaza	Observación

HTTP Security Header	• Propuesta de configuración:
	  ○ Respecto al encabezado Content-Security-Policy, tenga en cuenta que la aplicabilidad de la política depende del contexto de ejecución.
	  ○ El encabezado Clear-Site-Datahará que el navegador tome tiempo de procesamiento adicional para la respuesta HTTP, por lo tanto, configúrelo en la función de cierre de sesión cuando sea posible.
	  ○ Para el encabezado Permissions-Policy, como actualmente solo es compatible con navegadores basados en Chromium , el valor propuesto se generó con este sitio y se probó con la versión 137.0.7124.0de Chromium para especificar solo las funciones compatibles.
	• Evitar la divulgación de información a través de encabezados HTTP.

Amenaza	Observación
	• Evite la exposición a secuencias de comandos entre sitios al alojar archivos cargados • Prevenir problemas de configuración incorrecta de CORS • Evitar la divulgación de información a través de los archivos almacenados en caché local del navegador • Prevenir derivaciones de CSP

Recomendaciones:

- Continuar con las labores de mitigación que se han venido desarrollando en el portal institucional de la entidad, en aras de mantener las condiciones de seguridad adecuadas.
- Realizar auditorías regulares de las configuraciones del sistema y del software.
- Mantener el monitoreo de la URL para estar al tanto del surgimiento de cualquier tipo de vulnerabilidad y así tomar las medidas respectivas en el momento adecuado.
- Validar las configuraciones de seguridad de las cabeceras http con el fin de robustecerlas

Fuentes:

- https://www.iso27000.es/glosario.html
- https://www.tarlogic.com/es/glosario-ciberseguridad/cve/
- https://cwe.mitre.org
- https://owasp.org/