Ambiente

Gestión de Vulnerabilidades de TI

Proceso

Gestión de Servicios de Información y Soporte Tecnológico

Versión 2

26/06/2025

Tabla de Contenido

1. INTRODUCCIÓN

El Ministerio de Ambiente y Desarrollo Sostenible, en el marco de la implementación de los lineamientos de la Política de Gobierno, Seguridad Digital y el Modelo de Seguridad y Privacidad de la Información-MSPI, continúa fortaleciendo sus capacidades institucionales mediante esfuerzos orientados a garantizar una prestación eficiente, segura y oportuna de los servicios dirigidos a la ciudadanía, otras entidades del Estado y diversos sectores. A través de procesos de mejora continua, se identifican, abordan y proponen nuevos retos que contribuyen a una gestión más efectiva y alineada con los principios de seguridad de la información.

El propósito de este documento es establecer un marco integral, claro y efectivo para la gestión de vulnerabilidades dentro de la Entidad. La gestión de vulnerabilidades constituye un proceso crítico para la seguridad de la información, ya que permite identificar, evaluar, priorizar y mitigar debilidades que podrían ser explotadas por amenazas internas o externas.

La guía define el proceso y roles asociados a dicha gestión, con el objetivo de proteger adecuadamente los activos de información, reducir los riesgos operativos y garantizar la continuidad de los servicios tecnológicos ante posibles incidentes de seguridad de la información. Para facilitar el monitoreo, análisis y toma de decisiones, la gestión de vulnerabilidades se apoya en el uso de herramientas tecnológicas como Power BI. A través de esta plataforma, se consolidan y visualizan los datos relacionados con vulnerabilidades detectadas, su nivel de criticidad, estado de remediación y tendencias, permitiendo una supervisión continua y la priorización de acciones correctivas de forma oportuna y efectiva.

2. OBJETIVO

Establecer directrices claras para la identificación, evaluación, priorización y tratamiento de vulnerabilidades de seguridad en sistemas, redes, dispositivos, servicios y aplicaciones de la entidad. Con el propósito de reducir los riesgos asociados a incidentes de seguridad que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos de información, mediante la adopción de medidas preventivas, correctivas y de mejora continua que fortalezcan la seguridad de la información en la entidad.

3. ALCANCE

Su aplicación abarca la identificación, análisis, priorización, y remediación de vulnerabilidades en los servicios y recursos tecnológicos de la entidad. Además, define responsabilidades y lineamientos para el seguimiento y mejora continua del proceso de gestión de vulnerabilidades.

4. MARCO LEGAL Y NORMATIVIDAD

Además de las normativas locales mencionadas, este documento también considera las normativas nacionales vigentes en Colombia, que establecen lineamientos, políticas y estándares para la gestión de riesgos, la seguridad digital y la respuesta a incidentes. Asimismo, incorpora estándares internacionales ampliamente reconocidos como la norma ISO/IEC 27001, referente para la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI), y la guía NIST SP 800-40, que proporciona buenas prácticas para la gestión de vulnerabilidades y actualizaciones de seguridad en infraestructuras tecnológicas. A continuación, se detallan los principales marcos normativos considerados:

- Decreto 338 de 2022: Se formaliza la Definición y el alcance de los Equipos de respuesta a Incidentes Cibernéticos.
- Directiva Presidencial 03 del 15 de marzo de 2021: Respecto a lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Resolución 02277 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".
- Decreto 612 de 2018: Artículo 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Artículo12. Plan de Seguridad y Privacidad de la Información (...)
- NTC-ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información.
- NTC-ISO/IEC 27001: Código prácticas para la Gestión de Seguridad en la Información.
- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información: Ministerio de Tecnologías de la Información y Comunicaciones de Colombia.
- NIST SP 800-40: Publicación del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos que ofrece lineamientos técnicos y operativos para una gestión eficaz de parches y actualizaciones de seguridad, como medida preventiva ante vulnerabilidades en sistemas tecnológicos.

5. ROLES Y RESPONSABILIDADES

Profesional de Seguridad de la Información de la OTIC

- Ejecutar el procedimiento **P-A-GTI-11** "Gestionar la Operación de Servicios Tecnológicos" para la gestión de vulnerabilidades técnicas, específicamente en la etapa de "**Análisis Periódico de Vulnerabilidades**".
- Elaborar y presentar el cronograma de vulnerabilidades programadas anualmente ante el jefe de la OTIC para su revisión y aprobación. Una vez aprobado, deberá socializarse con las partes interesadas y se hará seguimiento a su ejecución, conforme a los plazos establecidos.
- Ejecuta el escaneo y/o reescaneo de vulnerabilidades sobre los activos solicitados, conforme a las solicitudes registradas a través de la mesa de asistencia y cronograma. Socializa los resultados obtenidos y presenta propuestas de remediación basadas en las vulnerabilidades identificadas mediante la plataforma de gestión de vulnerabilidades del Ministerio. Asimismo, coordina con las partes interesadas el cumplimiento de los plazos establecidos y realiza seguimiento a su ejecución.
- Presentar el informe anual de resultados de la gestión de vulnerabilidades al jefe de la OTIC.
- Registrar los resultados generados por la plataforma de gestión de vulnerabilidades, priorizando su incorporación en el tablero de control en Power BI. En caso de no ser posible, se deberá registrar en el formato F-A-GTI-11 "Registro de pruebas y remediación de vulnerabilidades técnicas", garantizando en todo caso la trazabilidad, el análisis y el seguimiento integral de la gestión de vulnerabilidades.
- Deberá garantizar que toda la documentación generada durante el proceso sea debidamente organizada, registrada y almacenada en los repositorios oficiales establecidos, tales como ARCA y SharePoint, realizando esta gestión documental conforme a las políticas internas y a la Tabla de Retención Documental (TRD) vigente.

Líder Técnico del Activo

- Deberá registrar la solicitud a través de la Plataforma de gestión y mesa de asistencia - GEMA y escalarla al Especialista Nivel 2 para su atención oportuna cuando las vulnerabilidades detectadas generen incidencias o requieran apoyo adicional.
- Es responsable de revisar y coordinar con el profesional de la seguridad de la información, el plan de remediación de las vulnerabilidades identificadas, evaluando la viabilidad técnica y operativa de su implementación. En caso de que no sea posible aplicar las medidas correctivas, deberá justificar formalmente la aceptación del riesgo y coordinar, junto con el profesional de seguridad de la información, la definición e implementación de controles compensatorios adecuados.

Jefe de la OTIC

- Revisa el alcance propuesto y aprueba el Cronograma de vulnerabilidades programadas anualmente por el profesional de seguridad de la información.
- Es notificado sobre aquellas vulnerabilidades críticas que no puedan ser remediadas y en estos casos, es responsable de tomar las decisiones correspondientes respecto a la aceptación del riesgo asociado.

6. INTEGRACIÓN CON OTROS DOCUMENTOS

- **P-A-GTI-11** Gestionar la Operación de Servicios Tecnológicos

El procedimiento busca asegurar la continuidad y el buen funcionamiento de los servicios tecnológicos del Ministerio de Ambiente y Desarrollo Sostenible mediante lineamientos y buenas prácticas en las etapas de Gestión de Incidentes y Gestión de Cambios. Además, reconoce que la corrección de vulnerabilidades puede implicar cambios en el entorno productivo.

- **M-E-GET-04** Manual de Políticas Específicas de Seguridad y Privacidad de la Información

Este documento tiene como objetivo: Proporcionar a los funcionarios, contratistas, y demás partes interesadas del Ministerio de Ambiente y Desarrollo Sostenible, las políticas y lineamientos de obligatorio cumplimiento con el fin de gestionar la seguridad de la información asegurando la integridad, confidencialidad y disponibilidad de la información, así como lo relacionado con la privacidad de la información (datos personales).

- **M-A-GTI-03** Manual para la Gestión de Incidentes de Seguridad y Privacidad de la Información

Este documento tiene como objetivo: Proporcionar a los funcionarios, contratistas, y demás partes interesadas del Ministerio de Ambiente y Desarrollo Sostenible, las políticas y lineamientos de obligatorio cumplimiento con el fin de gestionar la seguridad de la información asegurando la integridad, confidencialidad y disponibilidad de la información, así como lo relacionado con la privacidad de la información (datos personales).

7. GESTIÓN DE LAS VULNERABILIDADES

Esta guía contempla la planificación y ejecución del análisis de vulnerabilidades, la evaluación y la implementación de planes de remediación, seguidos de pruebas de verificación. Su objetivo es corregir fallos que puedan afectar sistemas, plataformas, servicios, redes o aplicaciones, fortaleciendo así la defensa ante amenazas cibernéticas y apoyando la continuidad operativa. Este procedimiento está formalizado en el **P-A-GTI-11** "Gestionar la Operación de Servicios Tecnológicos" etapa "Análisis Periódico de Vulnerabilidades".

7.1 Clasificación de las Vulnerabilidades

Las vulnerabilidades identificadas se dividen en cuatro niveles de criticidad: críticas, altas, medias y bajas. Esta clasificación toma en cuenta dos factores principales: el daño que podrían causar (impacto) y la facilidad con la que pueden ser aprovechadas (probabilidad de explotación). Con esto, es posible priorizar las acciones de mitigación, concentrando los esfuerzos en los riesgos más importantes y urgentes.

NIVEL DE CRITICIDAD	DESCRIPCIÓN	IMPACTO	EJEMPLO DE REMEDIACIÓN
Crítica	Vulnerabilidad explotable de forma remota o automatizada, sin autenticación previa. Permite comprometer totalmente el activo.	Acceso total a información sensible, interrupción de servicios críticos, pérdida de control del activo.	- Aplicar parche/corrección inmediatamente (cambios de urgencia). - Aislar el sistema si es necesario. - Bloquear accesos.
Alta	Requiere algún nivel de autenticación o interacción limitada, pero su explotación tiene alto impacto.	Pérdida parcial de confidencialidad, integridad o disponibilidad.	- Aplicar parches en un máximo de 5 días. - Reforzar controles de acceso. - Actualizar configuraciones. - Monitorear posibles intentos de explotación.
Media	Vulnerabilidad con limitaciones técnicas para ser explotada o bajo impacto en caso de explotación.	Riesgo moderado, afecta activos no críticos o que no comprometen directamente información sensible.	- Programar corrección en un plazo razonable (15-30 días) - Documentar mitigación - Aplicar actualizaciones de software - Evaluar controles existentes

NIVEL DE CRITICIDAD	DESCRIPCIÓN	IMPACTO	EJEMPLO DE REMEDIACIÓN
Baja	Dificultad alta de explotación o impacto menor. Generalmente son recomendaciones de buenas prácticas.	Impacto limitado, sin afectación significativa a los procesos o información.	- Corregir en siguientes ciclos de mantenimiento. - Documentar como mejora continua. - No requiere acción inmediata.

Tabla de criticidades de vulnerabilidades, fuente: elaboración propia.

7.2 Procedimiento

I. Identificación de los activos

Para los escaneos programados, el Profesional de Seguridad de la OTIC realiza la consulta del inventario actualizado de activos de información y, con base en el nivel de exposición, complejidad de operación y las solicitudes específicas recibidas selecciona y prioriza los activos a analizar.

II. Planificación del análisis de vulnerabilidades

Durante esta fase, el Profesional de Seguridad de la OTIC junto con el Jefe de OTIC determinan la periodicidad y metodologías técnicas a emplear para la identificación y evaluación de vulnerabilidades. La planificación debe estar estrictamente alineada con el procedimiento institucional **P-A-GTI-11** "Análisis Periódico de Vulnerabilidades", asegurando la adherencia a las normativas, estándares y mejores prácticas establecidas para la gestión integral de la seguridad informática.

Actividades:

- Elaboración del cronograma de vulnerabilidades programadas para el análisis de vulnerabilidades por parte del Profesional de Seguridad de la OTIC.
- Socialización del cronograma al Jefe de la OTIC para su revisión y aprobación,
- en caso de rechazo, redefinición del alcance y replanificación del análisis, si es aprobado, se debe socializar el cronograma con los interesados para su conocimiento y coordinación.

III. Ejecución del análisis de vulnerabilidades

La ejecución del análisis de vulnerabilidades, a cargo del Profesional de Seguridad de la OTIC, consiste en realizar escaneos conforme al cronograma de vulnerabilidades programadas aprobado y solicitudes registradas a través de la herramienta de asistencia a los activos previamente identificados, utilizando la herramienta de gestión de vulnerabilidades.

Los resultados obtenidos se consolidan y registran prioritariamente en el Dashboard de Power BI, en la herramienta de gestión de vulnerabilidades, con el fin de facilitar el seguimiento, la trazabilidad y la toma de decisiones. En caso de no estar disponible esta herramienta, se podrá utilizar el formato **F-E-GET-11** "Registro de pruebas y remediación de vulnerabilidades técnicas".

Actividades:

- Verificar el listado de activos aprobadas para el periodo vigente (según el cronograma de vulnerabilidades programadas).
- Configurar y ejecutar el escaneo o reescaneo.
- Descargar los resultados generados por la herramienta de gestión de vulnerabilidades y almacenarlos en la carpeta "JSON" del sitio de SharePoint, destinada a la actualización del tablero de control en Power BI. En caso de que el tablero no se encuentre operativo, se deberá diligenciar manualmente el formato **F-A-GTI-11** "Registro de pruebas y remediación de vulnerabilidades técnicas" como respaldo de la información.

IV. Tablero de Control (Power BI)

Para ejecutar el análisis de vulnerabilidades, es fundamental garantizar una adecuada gestión de la información. Con el fin de asegurar el correcto funcionamiento del Tablero de Control, a continuación, se describen los pasos a seguir para el almacenamiento de los datos en SharePoint y su integración con la herramienta de visualización.

Se deberá respetar estrictamente la nomenclatura de los archivos conforme al formato establecido así:

- Descargar los resultados generados por la herramienta de gestión de vulnerabilidades y almacenarlos en la carpeta "JSON" del sitio de SharePoint, destinada a la actualización del tablero de control en Power BI.

https://ticminambiente.sharepoint.com/:f:/s/Centrodeinformacinyambiental/EjpY7-03fBJOqBE83YCJ8ZQBj1hJQhmbskEqS56tKMxKpg?e=1EZuGs.

- El nombre del archivo debe comenzar con un número identificador asignado al ciclo de evaluación de un aplicativo o sistema específico. Este número debe mantenerse igual en todos los archivos relacionados con ese mismo ciclo, incluidos los generados en reescaneos posteriores (retests), para reflejar que pertenecen al mismo proceso o ciclo de evaluación del sistema analizado.

Ejemplo: **1**-CARDINALAPI2-WAS_Retest_test_cardinal_api2_28_05_2025.json

El número asignado a un aplicativo solo debe cambiar cuando se inicie **un nuevo ciclo de pruebas** del sistema. Por lo tanto, no se deben reutilizar números previamente asignados al mismo aplicativo si se desea reflejar en el dashboard los datos correspondientes a un nuevo ciclo. No obstante, diferentes aplicativos pueden compartir el mismo número, ya que la numeración no es exclusiva entre ellos.

- Continuar con un guion medio (-) sin espacio y no utilizar guion bajo (_).

Ejemplo: 1-CARDINALAPI2-WAS_Retest_test_cardinal_api2_28_05_2025.json

- Nombre del aplicativo: Se debe escribir en **mayúscula sostenida** conservando ese formato de manera uniforme en todos los casos. Si el nombre es compuesto (más de 2 palabras lo separa por un guion medio).

Ejemplo: 1-**CARDINALAPI2-WAS**_Retest_test_cardinal_api2_28_05_2025.json).

Solo el nombre del aplicativo debe separarse con guion medio (-). Cualquier información adicional en el nombre del archivo debe separarse con guion bajo (_) y escribirse en minúscula, utilizando mayúscula únicamente en la letra inicial de la primera palabra. Se debe evitar el uso de espacios en blanco.
Ejemplo: 1-CARDINALAPI2-WAS**_Retest_test_cardinal_api2_28_05_2025**.json

- Fecha del escaneo: Cada archivo cargado debe incluir, al final del nombre, la fecha en que se realizó el escaneo, utilizando el formato día-mes-año, separada por guion bajo.
Ejemplo: 1-CARDINALAPI2-WAS_Retest_test_cardinal_api2_**28_05_2025**.json

Los archivos agregados a la fuente de (SharePoint) serán procesados únicamente durante las actualizaciones programadas en el servicio de Power BI, por lo que los cambios no se reflejarán en el tablero hasta la próxima ejecución o hasta que se realice una actualización manual desde el mismo servicio, adicionalmente la creación de subcarpetas dentro del directorio JSON no está permitida, debido a que el Power Bi no es capaz de identificar subniveles o subcategorías.

V. Formato F-A-GTI-11 Registro de pruebas y remediación de vulnerabilidades técnicas

Este formato debe utilizarse únicamente en caso de que la herramienta de gestión de vulnerabilidades no se encuentre disponible. Su diligenciamiento es manual y debe realizarse conforme a las instrucciones establecidas en la tabla de instrucciones contenida en el mismo formato, la cual indica cómo registrar adecuadamente la información correspondiente.

VI. Validar la remediación de las vulnerabilidades

El profesional de seguridad de la OTIC será el responsable de ejecutar las actividades de validación y seguimiento correspondiente a la remediación de vulnerabilidades, conforme a los planes definidos. Estas actividades se llevarán a cabo a solicitud de los líderes técnicos responsables de los activos y de las remediaciones, asegurando que las acciones correctivas implementadas hayan mitigado efectivamente las vulnerabilidades identificadas.

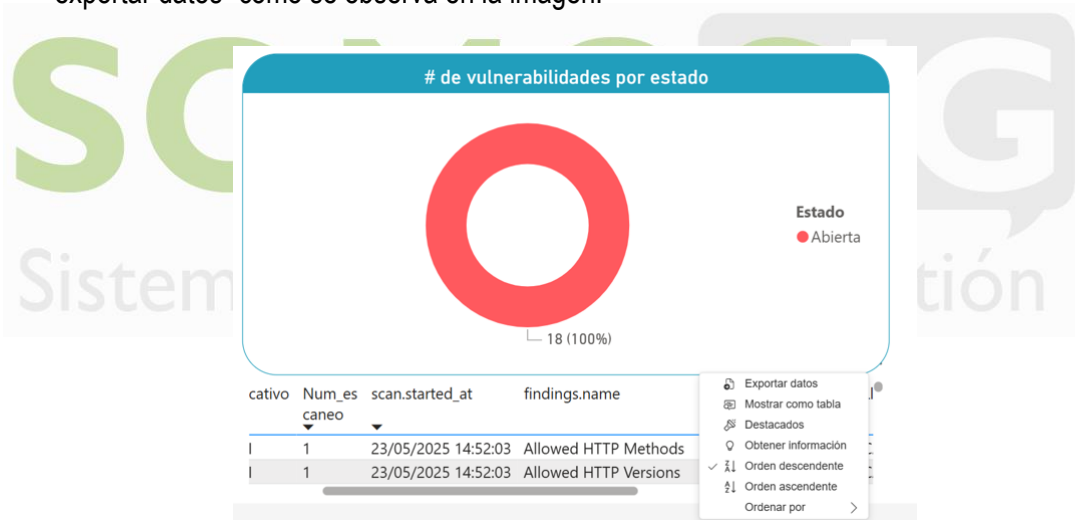
VII. Priorización de las vulnerabilidades

La priorización de vulnerabilidades se fundamenta en una evaluación integral del riesgo, que considera la severidad, la probabilidad de explotación, la exposición del activo y la frecuencia con la que la vulnerabilidad aparece en diferentes instancias. De este modo, vulnerabilidades recurrentes pueden recibir mayor prioridad, incluso si su severidad es media. En caso de no llevarse a cabo la evaluación profesional correspondiente, el Profesional de Seguridad de la OTIC será responsable de realizar el seguimiento necesario y gestionar los posibles efectos derivados de los riesgos identificados.

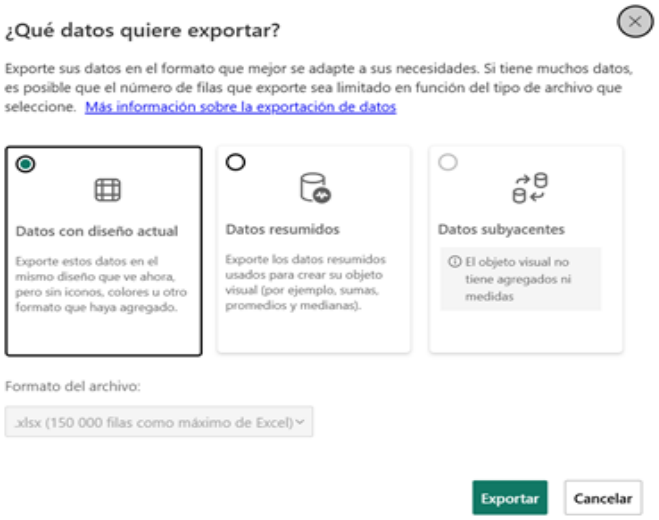
Tablero de Control (Power BI)

El profesional de seguridad de la OTIC, deberá diligenciar cuadro "# de vulnerabilidades por estado", el cual alimenta el Tablero de Control y permite que la información sea procesada y visualizada correctamente para su presentación, seguimiento y socialización. Paso:

- Actualizar estado de vulnerabilidades: Descargar en la sección "# de vulnerabilidades por estado" del Power BI la tabla de vulnerabilidades únicas haciendo clic en la opción "exportar datos" cómo se observa en la imagen:

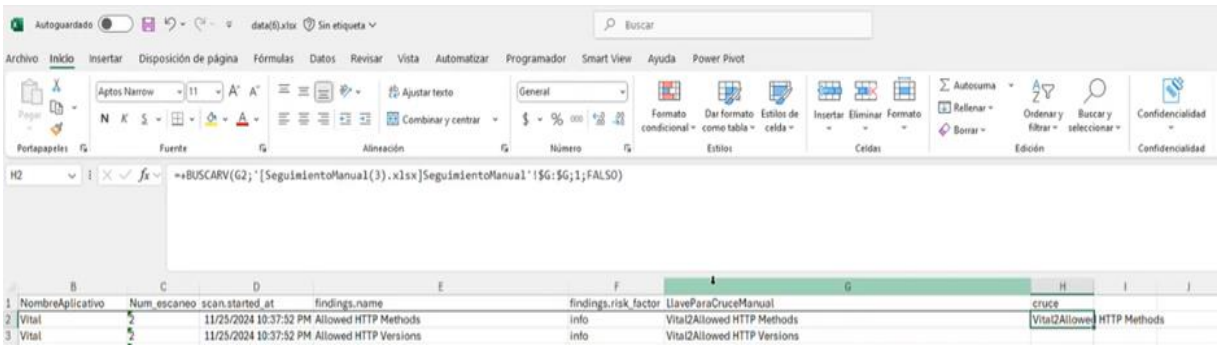


- Posteriormente se selecciona la opción "Datos con diseño actual".

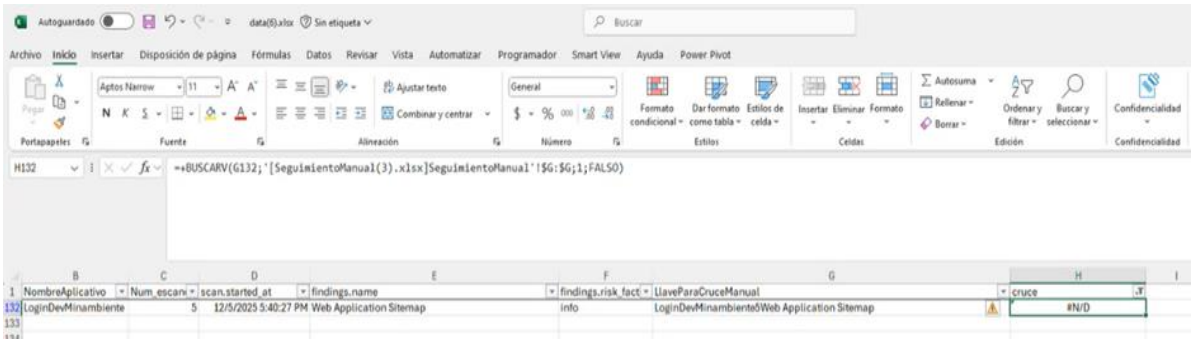


- Se procede a comparar la información exportada contra el archivo en Excel "SeguimientoManual" subido en la carpeta "Seguimientos" del sharepoint de la siguiente manera:
  Usar la columna "LlaveParaCruceManual" del archivo exportado para cruzar la información con el archivo "SeguimientoManual" e identificar así cuáles son las nuevas vulnerabilidades encontradas.

  Para ello en una columna vacía del archivo exportado se debe realizar una búsqueda con la fórmula **BUSCARV,** comparando así los valores de la columna "LlaveParaCruceManual" con la columna "Llave" del archivo "SeguimientoManual". En la siguiente imagen se observa la fórmula utilizada:



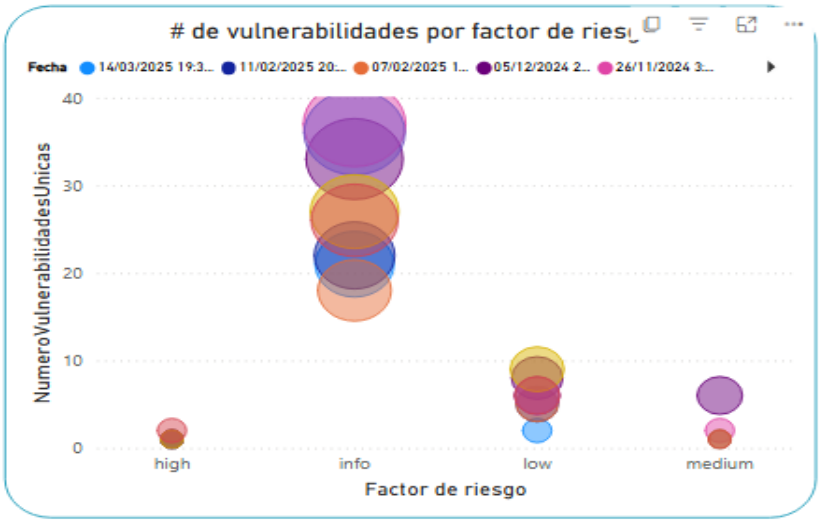
- Las vulnerabilidades nuevas o no encontradas aparecerán con un valor "#N/D" como se observa en la siguiente imagen:



Las vulnerabilidades que no se encuentren registradas deberán agregarse al final del archivo de seguimiento “SeguimientoManual” y diligenciar manualmente las columnas “Estado”, “Responsable”, “Fecha de seguimiento”, “Evidencia”, “Fecha propuesta de solución” y “Observaciones”.

- Finalmente se guarda y sobrescribe el archivo “SeguimientoManual” en la carpeta “Seguimientos” para que así ver la información actualizada de las vulnerabilidades encontradas en los sistemas y el seguimiento a las mismas.

Uno de los dashboards disponibles refleja la categorización de los hallazgos, facilitando la toma de decisiones al clasificar los riesgos en niveles lo que permite priorizar su atención de manera clara y eficiente según su impacto en los sistemas y servicios tecnológicos del Ministerio.



Formato F-A-GTI-11 Registro de pruebas y remediación de vulnerabilidades técnicas

En caso de estar utilizando el formato para la evaluación del estado, es fundamental verificar que la información registrada sea completa, precisa y esté actualizada. Esto garantiza que el cuadro de

análisis del estado refleje de manera exacta la situación actual de los activos evaluados, permitiendo una correcta interpretación y toma de decisiones.

VIII. Remediación

Con base en la priorización realizada, se diseñan e implementan planes de acción orientados a la corrección o mitigación de las vulnerabilidades identificadas, procurando minimizar el impacto. Estas acciones pueden incluir actualizaciones de software, aplicación de parches, ajustes de configuración o el fortalecimiento de controles de acceso.

Los resultados son socializados por el Profesional de Seguridad de la OTIC con los líderes técnicos y sus equipos responsables, con el fin de coordinar una respuesta oportuna y eficaz. En este proceso, se documentan de manera detallada las instancias, sistemas, subsistemas o componentes afectados por cada vulnerabilidad, incluyendo información técnica, como direcciones IP, nombres de host, entornos operativos, niveles de exposición, entre otros.

El plan de remediación debe ser validado por los responsables, y en caso de requerirse, se gestionan solicitudes de soporte o cambio para aplicar las medidas en los entornos correspondientes. Se evalúa la viabilidad técnica y operativa de cada acción propuesta; si la remediación directa no es posible, se deben definir y documentar controles compensatorios que reduzcan el riesgo residual.

NOTA

En aquellos casos donde no sea viable implementar medidas correctivas de forma inmediata, se deberá elaborar un informe técnico justificativo que respalde la decisión y sustente formalmente la propuesta de **asumir el riesgo**, el cual será remitido al Jefe de la OTIC para su análisis y aprobación.

IX. Retest y Validación

El Profesional de Seguridad de la OTIC realiza un nuevo escaneo del activo (retest) con el propósito de verificar la efectividad de las acciones de remediación implementadas. Los resultados obtenidos deben ser registrados en el formato correspondiente (F-A-GTI-11 Registro de pruebas y remediación de vulnerabilidades técnicas) o en el Dashboard de Power BI, según el medio que se esté utilizando, con el fin de garantizar su seguimiento, trazabilidad y análisis continuo.

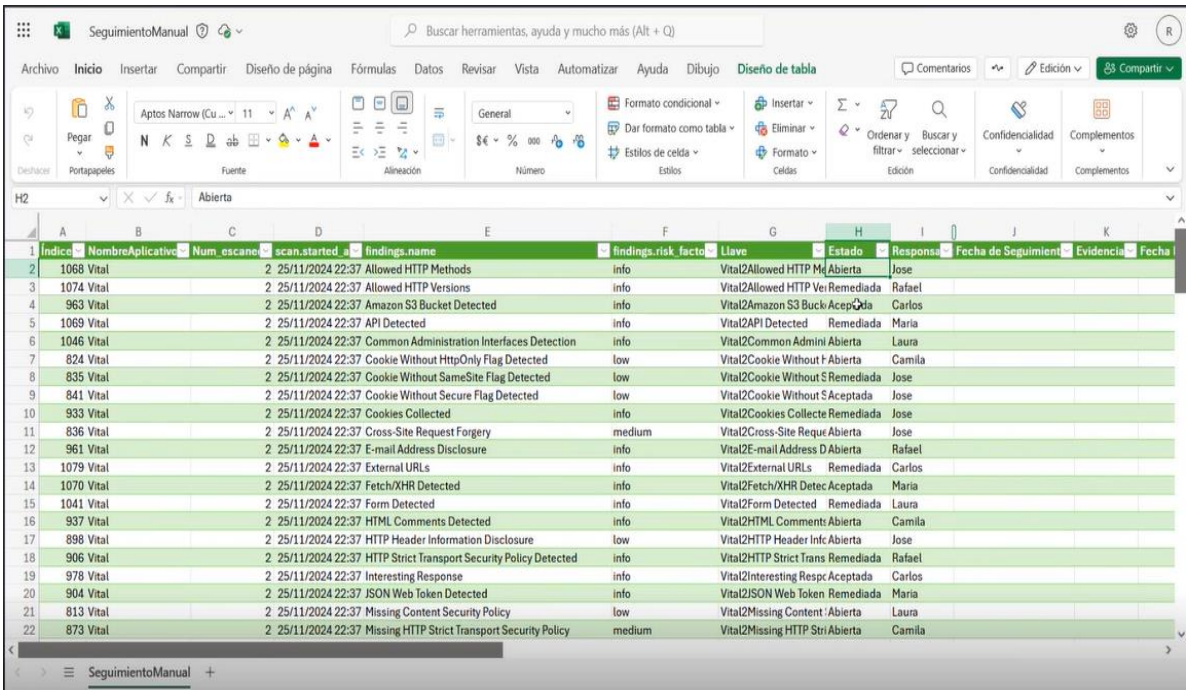
Si la vulnerabilidad ha sido corregida con éxito, los resultados se socializan con los equipos técnicos responsables. En caso contrario, se convoca una mesa técnica para evaluar la situación y definir, conforme a lo establecido.

Tablero de Control (Power BI)

Una vez analizada la información, el Profesional de Seguridad de OTIC deberá actualizar manualmente el cuadro de seguimiento, registrando en la columna H el estado actual de cada vulnerabilidad (aceptada, remediada o abierta) y en la columna I los responsables asignados para su remediación, así como completar los demás campos correspondientes con la información técnica disponible.

Directorio en donde se realizará el seguimiento manual a las vulnerabilidades:

https://ticminambiente.sharepoint.com/:f:/s/Centrodeinformacinyambiental/Eu59Nr6mFEFMh49gz2S3dgABqtsPt8vkTaiPtv2L1iAcRQ?e=fpx1mA



Índice	NombreAplicativo	Num_escaneo	scan.started_a	findings.name	findings.risk_facto	Llave	Estado	Responsa	Fecha de Seguimient	Evidencia	Fecha
1068	Vital	2	25/11/2024 22:37	Allowed HTTP Methods	info	Vital2Allowed HTTP Me	Abierta	Jose			
1074	Vital	2	25/11/2024 22:37	Allowed HTTP Versions	info	Vital2Allowed HTTP Ve	Remediada	Rafael			
963	Vital	2	25/11/2024 22:37	Amazon S3 Bucket Detected	info	Vital2Amazon S3 Buck	Aceptada	Carlos			
1069	Vital	2	25/11/2024 22:37	API Detected	info	Vital2API Detected	Remediada	Maria			
1046	Vital	2	25/11/2024 22:37	Common Administration Interfaces Detection	info	Vital2Common Admini	Abierta	Laura			
824	Vital	2	25/11/2024 22:37	Cookie Without HttpOnly Flag Detected	low	Vital2Cookie Without H	Abierta	Camila			
835	Vital	2	25/11/2024 22:37	Cookie Without SameSite Flag Detected	low	Vital2Cookie Without S	Remediada	Jose			
841	Vital	2	25/11/2024 22:37	Cookie Without Secure Flag Detected	low	Vital2Cookie Without S	Aceptada	Jose			
933	Vital	2	25/11/2024 22:37	Cookies Collected	info	Vital2Cookies Collecte	Remediada	Jose			
836	Vital	2	25/11/2024 22:37	Cross-Site Request Forgery	medium	Vital2Cross-Site Reque	Abierta	Jose			
961	Vital	2	25/11/2024 22:37	E-mail Address Disclosure	info	Vital2E-mail Address D	Abierta	Rafael			
1079	Vital	2	25/11/2024 22:37	External URLs	info	Vital2External URLs	Remediada	Carlos			
1070	Vital	2	25/11/2024 22:37	Fetch/XHR Detected	info	Vital2Fetch/XHR Detec	Aceptada	Maria			
1041	Vital	2	25/11/2024 22:37	Form Detected	info	Vital2Form Detected	Remediada	Laura			
937	Vital	2	25/11/2024 22:37	HTML Comments Detected	info	Vital2HTML Comments	Abierta	Camila			
898	Vital	2	25/11/2024 22:37	HTTP Header Information Disclosure	low	Vital2HTTP Header Infc	Abierta	Jose			
906	Vital	2	25/11/2024 22:37	HTTP Strict Transport Security Policy Detected	info	Vital2HTTP Strict Trans	Remediada	Rafael			
978	Vital	2	25/11/2024 22:37	Interesting Response	info	Vital2Interesting Respc	Aceptada	Carlos			
904	Vital	2	25/11/2024 22:37	JSON Web Token Detected	info	Vital2JSON Web Token	Remediada	Maria			
813	Vital	2	25/11/2024 22:37	Missing Content Security Policy	low	Vital2Missing Content	Abierta	Laura			
873	Vital	2	25/11/2024 22:37	Missing HTTP Strict Transport Security Policy	medium	Vital2Missing HTTP Stri	Abierta	Camila			

Formato F-A-GTI-11 Registro de pruebas y remediación de vulnerabilidades técnicas

El Profesional de Seguridad deberá diligenciar completamente la pestaña “Retest” del formato, asegurándose de registrar la información en cada uno de los campos definidos. Posteriormente, deberá analizar los resultados consolidados en los cuadros de resumen, los cuales permiten identificar el estado actual de las vulnerabilidades, evaluar la efectividad de las acciones de remediación y facilitar la toma de decisiones.

8. TRAZABILIDAD DOCUMENTAL

- El registro técnico de las pruebas ejecutadas y de las acciones de remediación implementadas debe ser documentado de forma estructurada, reflejado en el tablero de control (Power BI) y debidamente organizado en las carpetas designadas dentro del SharePoint.

- La documentación administrativa asociada —incluyendo planes de trabajo, planes de remediación, actas de reunión y listas de asistencia— debe ser gestionada y archivada rigurosamente en el sistema de gestión documental ARCA, de acuerdo con la Tabla de Retención Documental (TRD) vigente y publicada. Esta gestión documental es esencial para garantizar la trazabilidad, integridad y disponibilidad de la información institucional. Asimismo, el formato (F-A-GTI-11) final consolidado deberá ser cargado y conservado en ARCA, conforme a las disposiciones establecidas.

9. TERMINOS Y DEFINICIONES

- **Activo de Información:** Cualquier recurso o componente tecnológico que almacena, procesa o transmite información relevante para la organización.
- **Amenaza:** Cualquier circunstancia, evento o agente potencial que puede explotar una vulnerabilidad y causar un daño o impacto negativo a los activos de información o infraestructura tecnológica. Las amenazas pueden ser intencionales, como ataques cibernéticos, o no intencionales, como desastres naturales o fallas técnicas.
- **Dashboard de Power BI:** Herramienta de visualización y monitoreo dinámico que consolida datos e indicadores para facilitar la toma de decisiones basada en información actualizada.
- **Evaluación de Riesgo:** Proceso que combina la probabilidad de ocurrencia y el impacto potencial de una amenaza o vulnerabilidad para determinar su nivel de riesgo.
- **Incidente de Seguridad:** Evento que compromete la confidencialidad, integridad o disponibilidad de la información o activos tecnológicos.
- **Plan de Remediación:** Documento que contiene las acciones específicas para corregir o mitigar las vulnerabilidades detectadas, incluyendo responsables y plazos.
- **Prioridad de Vulnerabilidad:** Orden de atención asignado a una vulnerabilidad con base en su nivel de riesgo, impacto y exposición para optimizar recursos y tiempos de respuesta.
- **Retest: Reescaneo o reevaluación**: de un activo para verificar que las acciones correctivas hayan sido efectivas en la mitigación de vulnerabilidades.
- **Riesgo:** La posibilidad de que una amenaza explote una vulnerabilidad, generando un impacto adverso en la confidencialidad, integridad o disponibilidad de los activos de información, procesos o infraestructura tecnológica. El riesgo se evalúa combinando la probabilidad de ocurrencia y la severidad del impacto resultante
- **Tabla de Retención Documental (TRD):** Instrumento administrativo que establece los tiempos y condiciones para la conservación y disposición final de la documentación institucional.
- **TI:** Tecnologías de la Información.

- **Vulnerabilidad:** Debilidad o falla en un sistema, aplicación o proceso que puede ser explotada para comprometer la seguridad de la información o activos tecnológicos.