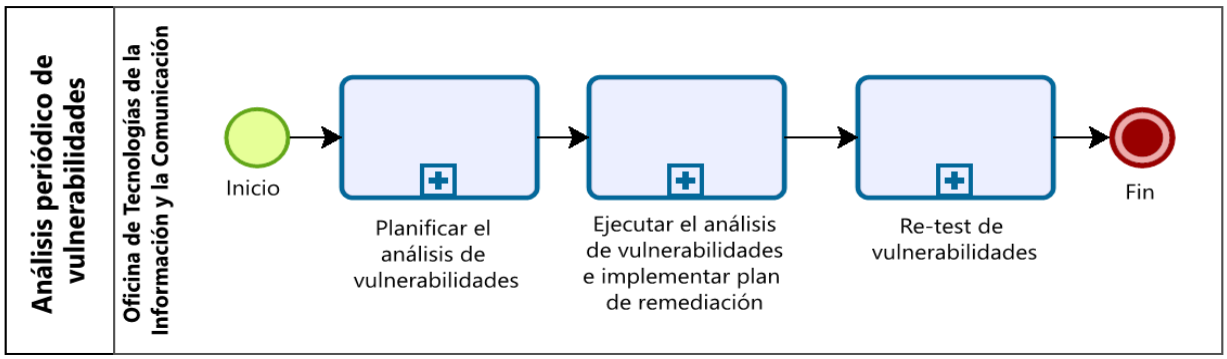
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	**ANÁLISIS PERIÓDICO DE VULNERABILIDADES** **Proceso: Gestión de Servicios de Información y Soporte Tecnológico**	SOMOSIG Sistema Integrado de Gestión
Versión: 02	**Vigencia:** 21/11/2023	**Código:** P-A-GTI-10

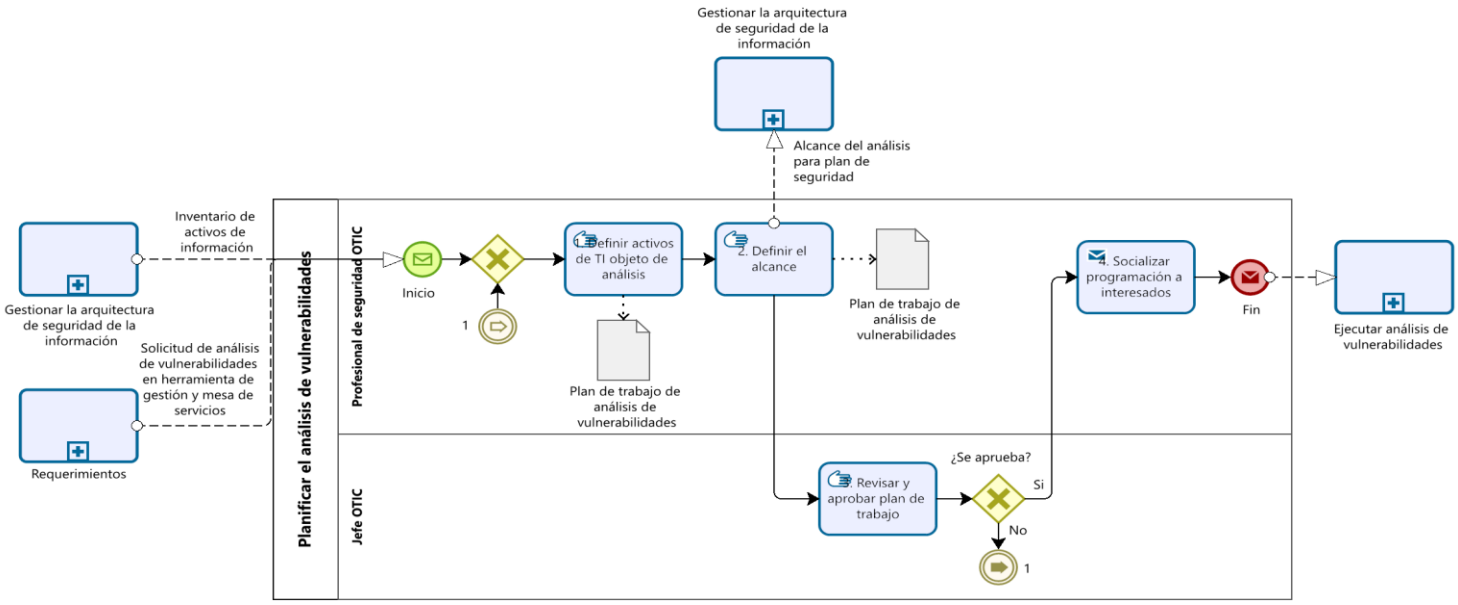
1. OBJETIVO(S)	Identificar, clasificar y remediar las vulnerabilidades en los activos de TI, para salvaguardar la información de la entidad frente a posibles brechas de seguridad existentes.
2. ALCANCE	El presente documento tiene como alcance identificar vulnerabilidades técnicas a los siguientes activos: sistemas operativos, aplicativos, base de datos, almacenamiento, infraestructura, conectividad, equipos de usuario final, cuentas de usuario siempre y cuando la herramienta adquirida por el Ministerio cuente con el licenciamiento y las funcionalidades anteriormente mencionadas. Inicia con la planificación de activos objeto del análisis de vulnerabilidades, continua con la ejecución del análisis de vulnerabilidades e implementación del plan de remediación y finaliza con el Re-test de vulnerabilidades.
3.POLITICAS DE OPERACIÓN	* El Ministerio de Ambiente y Desarrollo Sostenible debe gestionar las vulnerabilidades de acuerdo con las políticas definidas en el presente procedimiento. * La identificación de vulnerabilidades no debe interrumpir el cumplimiento de las actividades misionales de la entidad. * El Administrador de la herramienta de vulnerabilidades debe realizar escaneos de vulnerabilidades a los activos de información definidos conforme al plan de trabajo, o por solicitud a través de la Herramienta de gestión y mesa de servicios en el momento que se requiera. * Las vulnerabilidades críticas y altas deben remediarse, a menos que haya una razón que lo impida, la justificación debe ser conocida y aprobada por el Jefe de la OTIC. Para las vulnerabilidades de nivel medio o bajo, será el Profesional de seguridad de la OTIC quien defina si requiere o no remediación. * El Profesional de Seguridad de la OTIC deberá presentar un resumen ejecutivo del resultado de la gestión de vulnerabilidades de TI ante la Jefatura de la OTIC. * El Profesional de Seguridad de la OTIC debe realizar el seguimiento y verificación de que los responsables hayan gestionado las acciones definidas para corregir las vulnerabilidades. * Todo análisis de vulnerabilidades debe contar con plan de remediación; así se asuman las vulnerabilidades o implementen las acciones propuestas en dicho plan, se debe realizar un Re-test.
4. NORMAS Y DOCUMENTOS DE REFERENCIA	**Decreto 1008 de 2018:** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". **Decreto 1499 de 2017:** ARTÍCULO 2.2.22.1.5. Articulación y complementariedad con otros sistemas de gestión. El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de Seguridad de la Información. **Decreto 612 de 2018**: Artículo 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, 12. Plan de Seguridad y Privacidad de la Información. **Directiva Presidencial 02 de 2022:** Reiteración de la Política Publica en Materia de Seguridad Digital. **NTC-ISO/IEC 27001:2013:** Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). **NTC-ISO/IEC 27002:2013:** Tecnología de la información. Código prácticas para la Gestión de Seguridad en la Información. **Resolución 500 del 10 de marzo de 2021:** por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.

5. PROCEDIMIENTO

5.1. FLUJOGRAMA "ANÁLISIS PERIÓDICO DE VULNERABILIDADES"



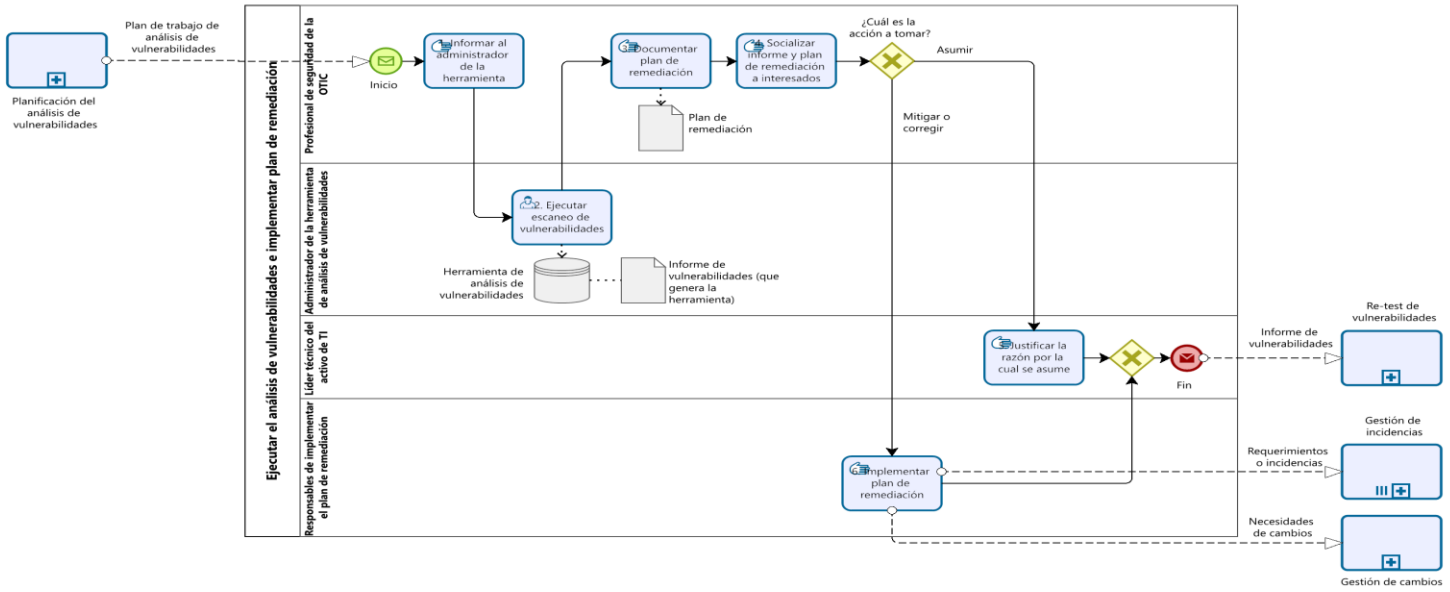
5.1.1. FLUJOGRAMA "PLANIFICAR EL ANÁLISIS DE VULNERABILIDADES"



5.1.2. ACTIVIDADES "PLANIFICAR EL ANÁLISIS DE VULNERABILIDADES"

Nº.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Definir activos de TI objeto de análisis	P	El Profesional de Seguridad de OTIC con base en el inventario de activos de información y las solicitudes de análisis de vulnerabilidades recibidas a través de la herramienta de gestión y mesa de servicios deberá definir los activos a los que se les realizará el análisis de vulnerabilidades y elaborar el plan de trabajo.	Profesional de seguridad de OTIC		Plan de trabajo de análisis de vulnerabilidades - Elaborado (Cronograma en Excel)
2	Definir el alcance	P	El Profesional de seguridad de OTIC debe determinar el alcance del análisis de vulnerabilidades con base en la herramienta que se empleará para la realización de las pruebas.	Profesional de seguridad de OTIC		Plan de trabajo de análisis de vulnerabilidades - Actualizado (Cronograma en Excel)
3	Revisar y aprobar plan de trabajo	P	El Jefe de la OTIC debe revisar y aprobar el plan de trabajo incluido el cronograma para la realización de las pruebas de análisis de vulnerabilidades ¿Se aprueba? Si, continua con la actividad 4 No, continua con la actividad 1.	Jefe OTIC	X	Plan de trabajo de análisis de vulnerabilidades - Aprobado
4	Socializar programación a interesados	H	El profesional de seguridad de OTIC debe Socializar el Plan de trabajo a las partes interesadas y hacer seguimiento con base en las fechas definidas. Fin de la etapa, continuar con la etapa "Ejecutar el análisis de vulnerabilidades e implementar plan de remediación".	Profesional de seguridad de OTIC		Plan de trabajo de análisis de vulnerabilidades - Socializado

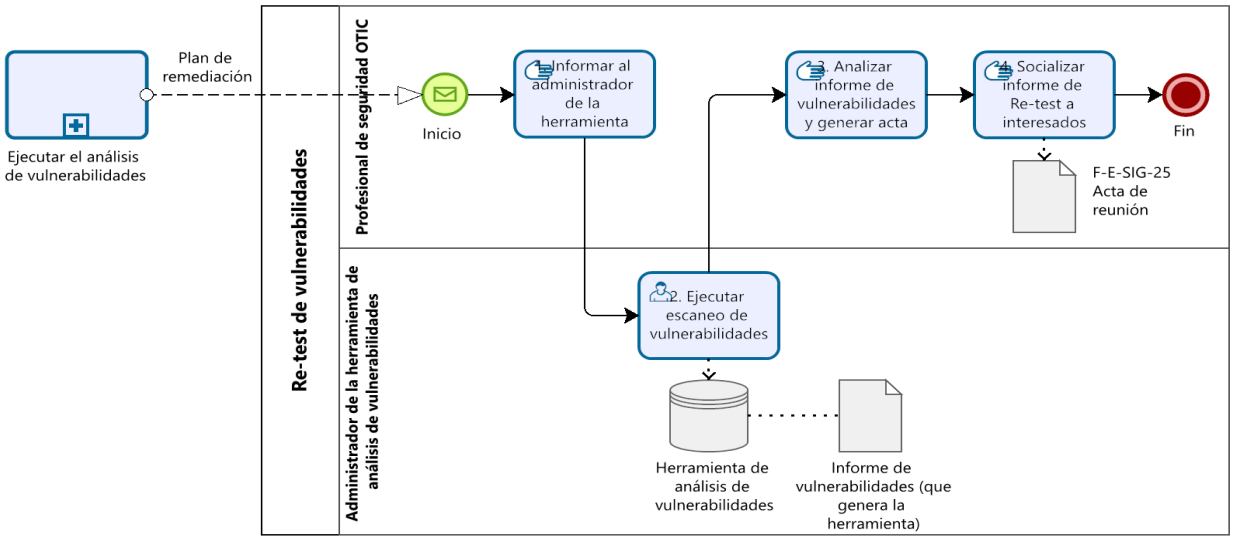
5.2.1. FLUJOGRAMA "EJECUTAR EL ANÁLISIS DE VULNERABILIDADES E IMPLEMENTAR PLAN DE REMEDIACIÓN"



5.2.2. ACTIVIDADES "EJECUTAR EL ANÁLISIS DE VULNERABILIDADES E IMPLEMENTAR PLAN DE REMEDIACIÓN"

Nº.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Informar al administrador de la herramienta	H	El Profesional de Seguridad OTIC debe informar al Administrador de la herramienta de análisis de vulnerabilidades sobre el escaneo que se requiere ejecutar según lo establecido en el plan de trabajo.	Profesional de seguridad de OTIC		
2	Ejecutar escaneo de vulnerabilidades	H	El Administrador de la herramienta de análisis de vulnerabilidades debe realizar el escaneo de vulnerabilidades a los activos de TI en los plazos previstos en el cronograma y hacer seguimiento a la ejecución.	Administrador de la herramienta de análisis de vulnerabilidades		Informe de vulnerabilidades que genera la herramienta
3	Documentar plan de remediación	H	El Profesional de Seguridad OTIC debe generar un plan de remedición e identificar los riesgos asociados para remediar las vulnerabilidades.	Profesional de seguridad de OTIC	X	Informe de vulnerabilidades que genera la herramienta con plan de remedición - Elaborado
4	Socializar informe y plan de remediación a interesados	H	El Profesional de Seguridad OTIC debe socializar a los interesados el informe del resultado del análisis de vulnerabilidades y el plan de remediación. ¿Cuál es la acción a tomar? Asumir, continuar con la actividad 5 Mitigar o corregir, continuar con la actividad 6.	Profesional de seguridad de OTIC		Informe de vulnerabilidades y plan de remediación socializado
5	Justificar la razón por la cual se asume	H	El Líder técnico del activo de TI debe justificar la aceptación del riesgo. Fin de la etapa, continuar con "Re-test de vulnerabilidades"	Líder técnico del activo de TI		Justificación de acciones asumidas en plan de remediación
6	Implementar plan de remediación	H	El Responsable de Implementar Plan de Remediación debe gestionar las acciones definidas. En caso de identificar incidencias o requerimientos asociados a la vulnerabilidad se debe realizar la solicitud por medio de la herramienta de gestión de servicios de TI. En caso de identificar necesidades de cambios asociados al plan de remediación se debe realizar la solicitud conforme al procedimiento P-A-GTI-04 Gestión de cambios. Fin de la etapa, continuar con "Re-test de vulnerabilidades"	Responsables de implementar el plan de remediación	X	Plan de remediación implementado

5.3.1. FLUJOGRAMA "RE-TEST DE VULNERABILIDADES"



5.3.2. ACTIVIDADES "RE-TEST DE VULNERABILIDADES"

Nº.	ACTIVIDAD	CICLO PHVA	DESCRIPCIÓN	RESPONSABLE	PC	REGISTRO
1	Informar al administrador de la herramienta	H	El Profesional de Seguridad OTIC debe informar y solicitar un re-test al Administrador de la herramienta de vulnerabilidades que permita evidenciar que el plan de remediación fue satisfactorio.	Profesional de seguridad OTIC		
2	Ejecutar escaneo de vulnerabilidades	H	El Administrador de la herramienta de análisis de vulnerabilidades debe ejecutar el re-test para evidenciar si la vulnerabilidad se mitigó.	Administrador de la herramienta de análisis de vulnerabilidades	X	Informe de vulnerabilidades (que genera la herramienta)
3	Analizar informe de vulnerabilidades y generar acta	V	El Profesional de Seguridad OTIC debe analizar los resultados del comparativo de cuales vulnerabilidades se mitigaron y cuales no.	Profesional de seguridad OTIC		
4	Socializar informe de Re-test a interesados	A	El Profesional de Seguridad OTIC debe socializar el informe del re-test a interesados y el comparativo de la gestión realizada en el cierre de las vulnerabilidades. Nota: Si en el Retest se identifican nuevas vulnerabilidades es recomendable incluirlas en el plan de trabajo. Fin del procedimiento.	Profesional de seguridad OTIC	X	F-E-SIG-25 Acta de Reunión

6. TÉRMINOS Y DEFINICIONES

Activo de TI: Es todo recurso de TI que genera, procesa, transporta y/o resguarda información necesaria para la operación y el cumplimiento de los objetivos del BCE, por lo tanto, se requiere proteger su confidencialidad, integridad y disponibilidad de las amenazas propias de su naturaleza y características.
Amenaza de seguridad de la información: surgen a partir de la existencia de vulnerabilidades, es decir, que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.
Ciberataque: En computadoras y redes de computadoras un ataque es un intento de exponer, alterar, desestabilizar, eliminar para obtener acceso sin autorización o utilizar un activo. Está asociado a cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático (ordenador, red privada etc.)
Equipos informáticos: Son equipos que permiten almacenar y procesar información.
Prueba Re-test : Es la actividad de realizar pruebas de verificación a la solución de las vulnerabilidades presentadas en los diferentes entregables solicitados
Herramienta de análisis de vulnerabilidades: Es una herramienta o solución que se utiliza para analizar y evaluar una computadora, red o aplicación para detectar vulnerabilidades y amenazas conocidas.
Sistemas de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
Vulnerabilidad: Es una debilidad o deficiencia de seguridad, que puede ser materializada por una amenaza.