1. OBJETIVO:

Establecer las acciones correspondientes para gestionar las vulnerabilidades tecnológicas que soportan los procesos institucionales, con el fin de minimizar los riesgos a los que está expuesta la información para el cumplimiento de los requisitos regulatorios aplicables y la política de seguridad y privacidad de la información de la entidad.

2. ALCANCE:

Inicia con la elaboración del documento de actividades de análisis de vulnerabilidades el cual incluye el cronograma de actividades, con el fin de realizar el análisis de vulnerabilidades sobre los servicios establecidos en el alcance y termina con la elaboración y presentación del informe final de las acciones y vulnerabilidades encontradas.

3. GENERALIDADES: No aplica.

4. DESCRIPCIÓN DE ACTIVIDADES:

No	Descripción de la actividad	Responsable	Registro
	Inicio		
1	Elaborar documento de actividades de análisis de vulnerabilidades el cual incluye el cronograma de actividades, con el fin de realizar el análisis de vulnerabilidades sobre los servicios establecidos en el alcance aprobado por el/la Subgerente de las Tecnologías de la Información y Comunicaciones. El profesional proyecta el documento con la metodología de acuerdo con el alcance definido por el Subgerente. **Nota 1:** El cronograma debe incluir las actividades, los responsables, fechas y horarios de ejecución de las pruebas. **Nota 2:** Para definir el alcance del análisis de vulnerabilidades se debe tener en cuenta como insumo el inventario de activos de información de la entidad y qué tipo de pruebas de vulnerabilidades se realizará.	Subgerente de las Tecnologías de la Información y Comunicaciones Profesional designado como Oficial de Seguridad de la Información por la Subgerencia de las Tecnologías de la Información y Comunicaciones	Documento de actividades de análisis de vulnerabilidades
2 P.C	Presentar el cronograma de actividades para el análisis de vulnerabilidades, el cual deberá ser aprobado por el o la Subgerente de las Tecnologías de la Información y Comunicaciones. ¿Se aprueba el cronograma de actividades? Si: Continuar con la actividad 3. No: Regresar a la actividad 1.	Subgerente de las Tecnologías de la Información y Comunicaciones Profesional designado como Oficial de Seguridad de la Información por la Subgerencia de las Tecnologías de la Información y Comunicaciones	Documento de actividades de análisis de vulnerabilidades Correo electrónico

No	Descripción de la actividad	Responsable	Registro
3	Notificar, por medio de correo electrónico, a los líderes de los procesos involucrados y los responsables de los sistemas de información e infraestructura sobre el inicio de pruebas y análisis de vulnerabilidades, indicando las fechas de ejecución de las pruebas.	Profesional designado como Oficial de Seguridad de la Información por la Subgerencia de las Tecnologías de la Información y Comunicaciones	Correo electrónico
4	Ejecutar el análisis de vulnerabilidades de acuerdo con el alcance definido en el Documento de actividades de análisis de vulnerabilidades, y tomar capturas de pantalla para dejar evidencia en el informe de la vulnerabilidad encontrada. **Nota:** durante la ejecución se deben monitorear los servicios que se encuentran en análisis.	Profesional designado como Oficial de Seguridad de la Información por la Subgerencia de las Tecnologías de la Información y Comunicaciones	Logs o pantallas de ejecución
5	Elaborar el informe de vulnerabilidades, el cual debe contener el detalle técnico de la prueba ejecutada y el plan de remediación o sugerencias aplicables que permitan eliminar o controlar la vulnerabilidad.	Profesional designado como Oficial de Seguridad de la Información por la Subgerencia de las Tecnologías de la Información y Comunicaciones	Informe de vulnerabilidades y plan de remediación
6	Ejecutar el plan de remediación con los profesionales de infraestructura y desarrollo para la implementación de los controles de seguridad, requeridos e identificados, quienes ejecutarán las acciones correspondientes. El reporte de la ejecución del plan de remediación, debe enviarse por correo electrónico a todos los involucrados en la afectación por la vulnerabilidad identificada. **Nota:** Para sistemas de información que sean críticos en la entidad se deben implementar controles en ambientes de prueba antes de desplegarlos en ambientes de producción.	Profesionales designados en Infraestructura y Desarrollo por la Subgerencia de las Tecnologías de la Información y Comunicaciones	Correo electrónico.
7	Ejecutar retesting, realizando nuevas pruebas de vulnerabilidad con el fin de validar la correcta implementación de los controles de seguridad y tomar capturas de pantalla para dejar evidencia en el informe final de las acciones y vulnerabilidades encontradas.	Profesional designado como Oficial de Seguridad de la Información por la Subgerencia de las Tecnologías de la Información y Comunicaciones	Logs o pantallas de ejecución
8	Elaborar y presentar el informe final de las acciones y vulnerabilidades encontradas. Este informe final debe ser remitido por correo electrónico a todos los involucrados en la afectación por la vulnerabilidad identificada.	Profesional designado como Oficial de Seguridad de la Información por la Subgerencia de las Tecnologías de la Información y Comunicaciones	Informe Final Correo Electrónico
	Fin		

Punto de Control: P.C.

5. **RESULTADO FINAL:** Vulnerabilidades cerradas.

6. **DEFINICIONES:**

Plan de remediación: Es la proyección de las actividades a desarrollar para arreglar, corregir o parchear la vulnerabilidad antes de que pueda llegar a ser una amenaza de seguridad.

Remediación: Acción que permite arreglar o corregir una vulnerabilidad a fin de minimizar el impacto en la organización.

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas

7. DOCUMENTOS DE REFERENCIA:

- Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto1008 de 14 de junio 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 número 1078 de 2015.
- Resolución 500 de 2021 de MinTic: 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".
- Documento Conpes 3995 de 2020 Política nacional de confianza y seguridad digital.
- Política de Seguridad y Privacidad de la Información
- Manual de Políticas de Seguridad de la Información

8. RELACIÓN DE FORMATOS:

CODIGO	NOMBRE DEL FORMATO
	No aplica

9. ANEXOS: No aplica

10. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio
16/01/2023	V2 GTI-PR-03	Se actualiza el documento contemplando lo siguiente: Redacción en el objetivo, se establece inicio y finalización en el alcance, eliminación del ítem responsabilidad. Cambio de estructura de presentación de la información, ajuste en cada uno de sus ítems, lo que incluye modificación en la descripción de las actividades del procedimiento, responsabilidades, cambio en la asignación del código. Todo lo anterior de acuerdo con las directrices establecidas en el Procedimiento de Elaboración, Modificación o Anulación de Documentos y Control de Documentos.
14/12/2022	V1 GTI-PR-03	Modificación de pie de página según manual de identidad de atenea y asignación cuadro control de cambios.

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	María Alejandra Suarez Rojas	Profesional Contratista – Subgerencia de Tecnologías de la información y las comunicaciones	25/08/2023
Revisó	Lira Jazmín Pineda Moreno	Subgerente de Tecnologías de la información y las Comunicaciones	25/08/2023
Aprobó	Lira Jazmín Pineda Moreno	Subgerente de Tecnologías de la información y las Comunicaciones	25/08/2023