1. Objetivo.

Establecer el procedimiento para identificar las actividades, responsabilidades y mecanismos técnicos para la realización de análisis periódicos de vulnerabilidades en los activos tecnológicos de la Gobernación de Nariño, con el fin de mitigar riesgos y fortalecer la seguridad digital institucional.

2. Alcance.

Este procedimiento aplica a todos los activos de información, servicios, sistemas, servidores, redes, aplicaciones y plataformas en la nube (pública o privada) gestionados por la Secretaría TIC de la Gobernación de Nariño, inicia con la programación de análisis de vulnerabilidades, ejecución contralada de escaneo y termina con la aplicación de correctivos para disminuir o eliminar vulnerabilidades

3. Definiciones.

- **Activo de información:** toda información, elementos, servicios o personas, relacionados con la producción o tratamiento de información, que tengan valor para la entidad, y por lo tanto se deben administrar y proteger.

- **Acuerdo de confidencialidad:** es el mecanismo mediante el cual regulamos los aspectos relativos a la seguridad de la información en una prestación de servicios, acorde a las funciones a desempeñar en la entidad.

- **Amenaza:** es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

- **Análisis de vulnerabilidades:** proceso sistemático para identificar, clasificar y evaluar vulnerabilidades (debilidades) en activos de información.

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.

- **Backup de información:** se refiere a la copia y archivo de datos de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

- **COLCERT:** es el grupo de respuesta a emergencias cibernéticas de Colombia, un equipo técnico que sirve como punto de contacto nacional para coordinar la prevención y respuesta a incidentes de seguridad digital en el país. Su misión es fortalecer la ciberseguridad del sector público y privado, gestionando vulnerabilidades y atendiendo emergencias para proteger la infraestructura tecnológica nacional.

- **Confidencialidad:** propiedad que determina que la información sólo esté disponible y sea

revelada a individuos, entidades o procesos autorizados.

- **Control:** son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Custodio:** es una parte designada de la entidad, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

- **Datacenter:** se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

- **Disponibilidad de la información:** se refiere a la seguridad que la información puede ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

- **Impacto:** resultado de un incidente de seguridad de la información.

- **Incidente de seguridad de la información:** ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la

- **Integridad:** se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.

- **Mejor práctica:** una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta.

- **No repudio:** el emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

- **Nube pública/privada:** infraestructura alojada en entornos externos o virtualizados bajo acuerdos de servicio y seguridad.

- **On Premise:** infraestructura tecnológica instalada y administrada localmente por la Gobernación

- **Partes interesadas:** persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

- **Política de seguridad de la información:** declaración de alto nivel que describe los objetivos y posición de la entidad frente a la Seguridad de la información.

- **Propietario responsable de la información:** individual, entidad o dependencia que tienen bajo su responsabilidad la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

- **Propietarios de infraestructura:** administradores de recursos tecnológicos utilizados para el manejo y/o administración de la información. Son responsables por la funcionalidad, operación, continuidad, manejo y uso de todos los sistemas compartidos, las redes, el soporte y el mantenimiento, el software estándar, los sistemas telefónicos y de comunicaciones, y los servicios relacionados.

- **Riesgo:** es la probabilidad que un incidente o evento adverso ocurra para causar una pérdida o daño en un activo de información.

- **Seguridad de la información:** conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información.

- **Sistema de gestión de seguridad de la información** - **SGSI:** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Terceros:** toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

- **Tratamiento de riesgos:** a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

- **Usuarios:** personas que, directa o indirectamente, tengan algún tipo de relación con la Entidad y/o que tengan acceso a los recursos tecnológicos de la entidad.

- **Vulnerabilidad:** es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

4. Condiciones y/o políticas específicas de operación

El procedimiento de análisis de vulnerabilidades, hace parte del conjunto de procedimientos de seguridad y privacidad de la información que constituyen una base sólida para que en la Gobernación de Nariño se realice una implementación transversal de la Política de seguridad de la información y seguridad digital, para salvaguardar sus activos de información, sus procesos y los servicios que presta.

a. Las URL objeto del análisis deben estar activas durante el período de pruebas.

b. En caso de que alguna de las URL requiera autenticación, y con el consentimiento de la Entidad, se deberán proporcionar dos (2) usuarios de acceso: uno con privilegios y otro sin ellos. Es recomendable que estos usuarios sean creados específicamente para las pruebas y eliminados una vez concluidas las mismas.

c. Las pruebas de seguridad estarán sujetas a las siguientes restricciones:

- No se realizarán ataques de ingeniería social.
- No se efectuarán ataques de denegación de servicio.
- No se llevará a cabo la explotación activa de las vulnerabilidades identificadas

4.1. Descripción de actividades.

1. Planeación del Análisis

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Secretaría TIC	Inventario activos de información	Identificar los activos de información y clasificarlos según su criticidad. Diligenciar el Formato GTC-F-12 programación de análisis de vulnerabilidades determinando los activos de información, frecuencia de ejecución, ubicación, alcance técnico, herramientas a utilizar y los datos del responsable (equipo de seguridad de la Secretaría TIC o personal externo)		Equipo de seguridad Secretaría TIC	Formato GTC-F-12 diligenciado	Equipo seguridad Secretaría TIC

2. Ejecución del Escaneo

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Equipo seguridad Secretaría TIC	Formato GTC-F-12 diligenciado	Configurar el escaneo de vulnerabilidades con privilegios controlados. Ejecutar el análisis en ventanas de mantenimiento autorizadas para evitar afectaciones al servicio. Registrar la información en el Formato GTC-F-13 ejecución del análisis (fecha y hora, responsable, alcance, clasificación del resultado según severidad (crítica, alta, media, baja), documentos adjuntos (informe		Equipo de seguridad Secretaría TIC	Formato GTC-F-13 diligenciado Informe técnico	Equipo seguridad Secretaría TIC

		de análisis), plazo de corrección según severidad (Críticas ≤ 7 días, alta ≤ 15 días, media ≤ 30 días y baja ≤ 60 días) y responsable de la corrección.				

3. Acciones Correctivas.

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Equipo de seguridad Secretaría TIC	Formato GTC-F-13 diligenciado	Aplicar las acciones técnicas correctivas sobre el activo, según las vulnerabilidades detectadas y la severidad. Diligenciar la descripción de las actividades realizadas en el Formato GTC-F-14 correctivos análisis de vulnerabilidades: responsable ejecutor de las correcciones, fecha de aplicación correcciones y la descripción de los resultados obtenidos, con los documentos adjuntos que apliquen.		Equipo de seguridad Secretaría TIC	Formato GTC-F-14 diligenciado. Informe técnico	Equipo de seguridad Secretaría TIC

4. Revisión y Validación.

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Equipo de seguridad Secretaría TIC	Formato GTC-F-14 diligenciado	Realizar análisis técnico de los correctivos aplicados para confirmar la eliminación de vulnerabilidades.		Equipo de seguridad Secretaría TIC	Formato GTC-F-15 diligenciado Informe técnico	Equipo de seguridad Secretaría TIC

PROCESO ASOCIADO: GESTIÓN DE TECNOLOGÍA	DEPENDENCIA ASOCIADA: SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO

		Consolidar los resultados en un informe técnico. Presentar el informe al equipo de seguridad de la Secretaría TIC y diligenciar el Formato GTC-F-15 validación análisis de vulnerabilidades donde se describa la fecha, responsable de la verificación, si la vulnerabilidad fue eliminada y las actividades pendientes para su corrección total cuando aplique.				

5. Fin

6. Diagrama de flujo.

N/A

6. Documentos relacionados.

- Ley No 599 de 2000 - Código penal: Título VII BIS
- Ley Estatutaria 1266 De 2008
- La Ley 1273
- Artículo 1 - Adicionase el Código Penal con un título VII bis Artículo 269a Artículo 269C
- Ley Estatutaria 1581 De 2012
- Decreto 1377 De 2013
- Ley 1581 de 2012
- Decreto 886 de 2014
- Decreto 1078 de 2015
- Decreto 1078 de 2015
- Documentos CONPES 3854 - CONPES 3975
- Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Formato GTC-F-12 programación análisis de vulnerabilidades
- Formato GTC-F-13 ejecución análisis de vulnerabilidades
- Formato GTC-F-14 correctivos análisis de vulnerabilidades
- Formato GTC-F-15 validación análisis de vulnerabilidades

7. Anexos.

N/A

8. Control de cambios.

Versión	Fecha de versión	Descripción del cambio	Responsable
01	12/03/2026	Creación del documento	

9. Responsable.

El responsable de este documento es el Secretario TIC, Innovación y Gobierno Abierto, quien debe revisarlo, y si es necesario actualizarlo.

10. Revisión, aprobación y verificación.

Revisión	Aprobación	Verificación
Jonnathan Huertas Salas	Jonnathan Huertas Salas	Armando Rosero García
Secretario TIC, Innovación y Gobierno Abierto	Secretario TIC, Innovación y Gobierno Abierto	Secretario de Planeación