1. OBJETIVO

Identificar, monitorear, controlar y gestionar de manera oportuna las vulnerabilidades detectadas y reportadas en la infraestructura tecnológica (aplicaciones, sistemas de información, activos de información). Esto tiene como propósito mantener un nivel adecuado de seguridad mediante la documentación, el monitoreo continuo y la implementación de medidas de remediación, contribuyendo a la mitigación de riesgos y a la prevención de incidentes de seguridad.

2. ALCANCE

El proceso inicia con la identificación de los riesgos asociados a la seguridad de la información, a partir del inventario de los activos de información, continúa con el análisis de vulnerabilidades sobre estos activos, y culmina con la implementación de acciones orientadas a la mitigación, remediación efectiva de las vulnerabilidades detectadas y documentar las lecciones aprendidas.

3. ENTRADAS

- Detección de vulnerabilidades identificadas o reportadas a través de la mesa de ayuda, correo electrónico y herramientas de software de seguridad perimetral asociadas.
- Escaneo semestral de vulnerabilidades en la infraestructura tecnológica del ICANH.

4. LINEAMIENTOS DE OPERACIÓN

- El Oficial de Seguridad asignado es el responsable de realizar la identificación de las vulnerabilidades. Además, deberá elaborar un cronograma que permita coordinar y ejecutar los análisis previamente programados.
- Es responsabilidad de los líderes y equipos de trabajo informar sobre cualquier aplicación o sistema de información a utilizar en las áreas del ICANH.
- El personal técnico encargado de la custodia o administración de los activos tecnológicos debe realizar las acciones necesarias para gestionar las vulnerabilidades técnicas identificadas en la infraestructura tecnológica y sistemas de información
- Para la realización de análisis de vulnerabilidades de los sistemas de información, se debe contar con el inventario de activos de información actualizado en el cual se identifique el responsable técnico, con el fin que realicen las actividades de actualización que corresponda.
- El Oficial de Seguridad debe realizar un escaneo de vulnerabilidades en los activos de información en producción, al menos una vez cada semestre.
- La identificación de vulnerabilidades no debe irrumpir en el cumplimiento de las actividades misionales y administrativas de la entidad.
- El Oficial de Seguridad realiza el análisis de vulnerabilidades técnicas utilizando la herramienta disponible por la entidad (con licencia en versión paga) para la ejecución de esta actividad.
- El Oficial de Seguridad debe realizar una evaluación de vulnerabilidades a cualquier software solicitado por las diferentes áreas antes de su instalación en los equipos de usuario final.
- El Oficial de Seguridad debe implementar medidas preventivas y correctivas tras el escaneo de vulnerabilidades, con el objetivo de reaccionar de manera oportuna ante cualquier brecha de seguridad.
- Los resultados de los escaneos realizados a la infraestructura tecnológica, aplicaciones, sistemas de información y hosts, incluyendo las vulnerabilidades encontradas y las recomendaciones o remediaciones de seguridad, deben ser documentados en informes, bitácoras, archivos o registros, y enviados a los responsables técnicos para su respectiva revisión y seguimiento.

5. DEFINICIONES

- **ACTIVO DE INFORMACIÓN:** Son cualquier dato, información, conocimiento, software, hardware, servicio de TI, almacenamiento de datos, equipo de TI que tiene valor para la empresa.

- **ACTIVOS TECNOLÓGICOS CRÍTICOS:** Son componentes tecnológicos esenciales para el funcionamiento y continuidad operativa de una organización. Su falla o interrupción puede afectar significativamente la consecución de objetivos, prestación de servicios, generación de ingresos y la reputación institucional.

- **BRECHAS DE SEGURIDAD:** Es un incidente que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos. Es decir, permite acceder sin autorización a información. Normalmente, se produce cuando un intruso logra sortear los mecanismos de seguridad.

- **INFRAESTRUCTURA DE TI:** Es todo el hardware, software, redes, instalaciones, etc., que se necesitan para desarrollar, probar, entregar, monitorear, controlar o dar soporte a servicios de TI y a aplicaciones. El término incluye toda la tecnología de información, pero no a las personas, procesos y documentación asociados.

- **OFICIAL DE SEGURIDAD:** Es el responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones orientadas a fortalecer la seguridad de la información. Su labor se centra en garantizar los pilares fundamentales de la seguridad: confidencialidad, integridad y disponibilidad.

- **RESPONSABLE TÉCNICO**: Es la persona o equipo encargado de asegurar el funcionamiento, mantenimiento y soporte técnico de un sistema. Sus tareas incluyen gestionar la infraestructura, implementar mejoras, resolver incidentes, cumplir con las políticas de seguridad y monitorear el rendimiento y la disponibilidad del sistema, asegurando que opere conforme a los requisitos de la organización.

- **RIESGO:** Daño potencial causado por ataques a los sistemas de TI y eventos potenciales como posibles amenazas, vulnerabilidades o debilidades en los sistemas, redes, aplicaciones y datos de una organización que podrían ser explotados.

- **SISTEMAS DE INFORMACIÓN:** Es un conjunto de componentes interconectados que trabajan juntos para recoger, procesar, almacenar y distribuir datos con un propósito específico. Estos componentes pueden incluir hardware (como ordenadores, servidores, equipos de almacenamiento, etc.), software (como sistemas operativos, aplicaciones, bases de datos, etc.) y datos (como información sobre clientes, productos, transacciones, etc.).

- **VULNERABILIDAD:** es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad, Hay varios tipos de vulnerabilidades hardware, software, aplicaciones o sistemas de información que pueden ser explotadas por atacantes.

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro (Documento que se deja como evidencia de ejecución)	Punto de Control
1.	Revisar si existe un reporte de vulnerabilidad.	Identificar si existe detección de vulnerabilidades identificadas o reportadas a través de la mesa de ayuda, correo electrónico y herramientas de software de seguridad perimetral asociadas. De ser así pasar a la actividad No.5, de lo contrario continuar en la actividad No.2.	Oficial de Seguridad del área funcional de Tecnología y Sistemas de información	Correo, tiquete de mesa de ayuda o reporte del software de seguridad perimetral asociadas.	No aplica.
2.	Identificar los activos de información.	Identificar los activos de información a los cuales se les debe realiza el escaneo de vulnerabilidades conforme a lo establecido en el documento GTI-GUI-03-DA-02 Activos de información e infraestructura crítica.	Oficial de Seguridad del área funcional de Tecnología y Sistemas de información	Inventario de activos de información e infraestructuras críticas de TI, matriz clasificación de los activos de información.	La identificación de activos se realiza en la Matriz de Clasificación de los Activos de Información y este documento se actualiza de forma anual.
3.	Realizar la elaboración del plan para la ejecución de análisis de vulnerabilidades.	Diseñar un plan y presentar un cronograma de actividades en el cual se detalle los activos a los cuales se les debe realizar el análisis de vulnerabilidades, tomando en cuenta el inventario de activos de información identificado en la anterior actividad y los reportes recibidos o detectados.	Oficial de Seguridad del área de Tecnología y Sistemas de Información	Plan y cronograma del análisis de vulnerabilidades.	El plan y cronograma debe tener en cuenta todos los reportes de vulnerabilidades realizados a través de la mesa de ayuda, correo electrónico, así como las detectadas por las herramientas de software de seguridad perimetral asociadas.
4.	Revisar y aprobar plan de trabajo.	Revisar que el plan y el cronograma incluyan todos los activos de información y la infraestructura tecnológica de la entidad. En caso de tener observaciones se informan al Oficial de Seguridad para el ajuste pertinente de lo contrario continuar en la actividad No.4.	Responsable del área de Tecnología y Sistemas de Información	Plan y cronograma aprobados	Revisar frente al Inventario de activos de información e infraestructuras críticas de TI y lo descrito en la matriz clasificación de los activos de información garantizando que todos los activos se encuentren programados para el análisis e igualmente que las fechas de ejecución de análisis de vulnerabilidades no interrumpan la operación de la entidad.
5.	Ejecutar el análisis de vulnerabilidades.	Iniciar el escaneo y análisis de vulnerabilidades de los activos de información y de la infraestructura tecnológica de la entidad de acuerdo con el plan y cronograma aprobado o el reporte recibido, llevando un registro de las pruebas y evidencias generadas en el escaneo.	Oficial de Seguridad del área de Tecnología y Sistemas de Información	Informes, Bitácora, archivos.	Garantizar que el escaneo se haya realizado a todos los activos de información y la infraestructura tecnológica.
6.	Notificar resultado del escaneo de vulnerabilidades	Remitir por correo el informe al responsable del activo de información y de la infraestructura tecnológica de la entidad, el cual debe incluir los resultados del análisis y	Oficial de Seguridad del área de Tecnología y	Informe del resultado del análisis.	Garantizar que el informe contenga tanto los resultados del escaneo como las

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable (Cargo y/o Grupo responsable / Dependencia)	Registro (Documento que se deja como evidencia de ejecución)	Punto de Control
		las recomendaciones necesarias para mitigar las vulnerabilidades identificadas.	Sistemas de Información		recomendaciones para mitigar las vulnerabilidades.
7.	Elaborar un plan de remediaciones a las vulnerabilidades.	En relación con el Informe del resultado del análisis del activo y de la infraestructura tecnológica de la entidad, se genera un plan de remediación que define los responsables y las fechas para aplicar las recomendaciones de seguridad, evaluando la criticidad de cada vulnerabilidad encontrada y determinando cuáles deben ser solucionadas a corto, mediano y largo plazo.	Oficial de Seguridad del área de Tecnología y Sistemas de Información	Plan de remediaciones de vulnerabilidades de seguridad.	Garantizar que el plan contenga todas las remediaciones a las vulnerabilidades encontradas y tanto las fechas como la criticidad esté acorde a las mismas.
8.	Revisar y aprobar el plan de remediaciones a las vulnerabilidades.	Se revisa y aprueba que el plan de remediaciones de seguridad cumpla con la solución efectiva de las vulnerabilidades identificadas en el escaneo, si es necesario se solicitan los ajustes pertinentes al Oficial de Seguridad, de lo contrario éste procede a enviarlo por correo al responsable del activo de información o de la infraestructura tecnológica para la gestión pertinente.	Responsable área de Tecnología y Sistemas de Información.	Plan de remediaciones de vulnerabilidades de seguridad.	Garantizar que las remediaciones a corto, mediano o largo plazo estén acordes a la vulnerabilidad encontrada.
9.	Remediar las vulnerabilidades de los activos	El responsable del activo de información y de la infraestructura tecnológica debe ejecutar las acciones del plan de remediaciones de seguridad enviadas por el Oficial de Seguridad, con el objetivo de cerrar la brecha de vulnerabilidad y posteriormente debe generar y enviar por correo al Oficial de Seguridad un documento donde informe la implementación del plan de remediación.	Responsable del activo de información o de la infraestructura tecnológica	Correo electrónico con el documento de la implementación del plan de remediación.	El responsable debe realizar el seguimiento y la actualización de los controles establecidos en la MATRIZ DE APLICABILIDAD ISO 27001. Igualmente debe evaluar y verificar el progreso del plan de remediación, asegurando la corrección de las vulnerabilidades identificadas conforme a las fechas, prioridades establecidas y responsabilidades asignadas.
10.	Verificar si las remediaciones fueron mitigadas	Una vez recibido el correo con el informe de implementación del plan de remediación el Oficial de Seguridad debe realizar la verificación o escaneo al activo o a la infraestructura tecnológica. Si las vulnerabilidades fueron mitigadas se debe continuar en la actividad No. 10, de lo contrario, regresar a la actividad No. 5 para iniciar de nuevo lo establecido en el presente documento.	Oficial de seguridad / Área de Tecnología y Sistemas de información	Correo, informe del resultado del análisis del activo tecnológico	Escaneo de la infraestructura tecnológica y documentación de resultados.
11.	Documentar las lecciones aprendidas	Validar el ciclo realizado, documentando las lecciones aprendidas, y analizar la	Oficial de seguridad del área de Tecnología y	Informe lecciones aprendidas.	El conocimiento adquirido sobre lo ocurrido durante la ejecución de este

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable (Cargo y/o Grupo responsable / Dependencia)	Registro (Documento que se deja como evidencia de ejecución)	Punto de Control
		conveniencia de reevaluar o modificar actividades del procedimiento si es necesario.	Sistemas de información		procedimiento se debe documentar como lecciones aprendidas, con el fin de que a través de la reflexión y el análisis crítico de los factores que afectaron de manera positiva o negativamente el resultado esperado lleve al proceso a la mejora continua.

7. DIAGRAMA DE FLUJO

No aplica.

8. REGISTROS

Nombre	Almacenamiento
Inventario activos de información	Unidad compartida del área de tecnología/Seguridad Información/año
Matriz Clasificación de los Activos de Información	Unidad compartida del área de tecnología/Seguridad Información/año
Plan y cronograma para la realización del análisis de vulnerabilidades	Unidad compartida del área de tecnología/Seguridad Información/año
Bitácora o documento de evidencia del análisis de vulnerabilidades de los activos	Unidad compartida del área de tecnología/Seguridad Información/año
Informe del resultado del análisis.	Unidad compartida del área de tecnología/Seguridad Información/año
Plan de remediaciones de vulnerabilidades de seguridad.	Unidad compartida del área de tecnología/Seguridad Información/año
Documento de la implementación del plan de remediación.	Unidad compartida del área de tecnología/Seguridad Información/año
Correos	Unidad compartida del área de tecnología/Seguridad Información/año
Informe de lecciones aprendidas	Unidad compartida del área de tecnología/Seguridad Información/año

9. ANEXOS

Documentación Aplicable

- Sistema de Gestión de Seguridad de la Información del ICANH

Normatividad aplicable

- NTC ISO 27001 - Seguimiento y actualización a los controles contenidos en la matriz de aplicabilidad.

10. CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción general del cambio**
01	23/01/2025	Se establece el procedimiento de Gestión de Vulnerabilidades con el propósito de fortalecer la seguridad de los activos de información y tecnológicos del ICANH, asegurando su protección frente a posibles amenazas y riesgos.

ELABORÓ	**REVISÓ**	**APROBÓ**
Cargo: Profesional Área de Tecnología y Sistemas de Información	**Cargo:** Profesional Especializado Área de Tecnología y Sistemas de Información. Profesional Especializado Oficina Asesora de Planeación.	**Cargo:** Asesor de Tecnología y Sistemas de Información
Fecha: 13/01/2025	**Fecha: 22/01/2025**	**Fecha: 23/01/2025**