1. OBJETIVO

Establecer las responsabilidades y actividades necesarios para identificar, analizar, evaluar, priorizar, tratar y monitorear las vulnerabilidades técnicas presentes en los activos de información de TI de la ETITC, con el fin de reducir los riesgos asociados a posibles incidentes de seguridad que afecten la confidencialidad, integridad y disponibilidad de la información. Este procedimiento se implementa en cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022 y a las directrices del Modelo de Seguridad y Privacidad de la Información – MSPI (Resolución 02277 de 2025), como facilitador para la adopción de controles proactivos, oportunos y medibles que contribuyan a mejorar la postura de seguridad y ciberseguridad institucionales.

2. ALCANCE

El presente procedimiento aplica a la identificación, análisis, gestión y tratamiento de vulnerabilidades técnicas que puedan afectar los activos de TI de la ETITC, incluyendo servidores, sistemas de información, aplicaciones instaladas, computadores de funcionarios, dispositivos de red, aplicaciones web y los procedimientos de TI asociados al aseguramiento operativo de estos activos.

El alcance comprende todas las actividades del proceso de gestión de vulnerabilidades técnicas, desde el descubrimiento y escaneo hasta la verificación de la remediación aplicada, incluyendo: identificación y documentación de vulnerabilidades, análisis técnico y contextual, emisión de recomendaciones de remediación, priorización según criticidad y riesgo, formulación de planes de acción, ejecución de remediaciones y validación posterior. Este procedimiento es aplicable a todos los activos bajo administración directa de la ETITC y a aquellos gestionados o administrados por proveedores, cuando así esté definido contractualmente o en acuerdos de niveles de servicio, proyectado a una cobertura integral en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) y del Modelo de Seguridad y Privacidad de la Información – MSPI.

3. RESPONSABILIDADES

1. Comité de Gestión y Desempeño (Alta Dirección):
Aprobar excepciones y aceptación de riesgo residual frente a vulnerabilidades no remediadas dentro del plazo.

Revisar informes ejecutivos de vulnerabilidades críticas y exposición persistente.
Definir lineamientos estratégicos para fortalecer la postura de seguridad.

Responsable del SGSI (Cumple funciones de Seguridad de la Información, Gestión de Riesgos y Auditoría Interna):
Mantener y actualizar el procedimiento.
Integrar la gestión de vulnerabilidades al SGSI, MSPI y gestión de riesgos.
Realizar la valoración del riesgo residual de vulnerabilidades según criterios institucionales.
Reportar resultados al Comité de Gestión y Desempeño.
Realizar auditoría interna al proceso, verificar controles y recomendar mejoras.
Acompañar procesos de excepción, elevarlos al Comité de acuerdo con solicitudes recibidas.

Profesional Contratista de Ciberseguridad o quien haga sus veces (Equipo de Gestión de Vulnerabilidades):
Ejecutar las actividades técnicas del proceso: descubrimiento, escaneo, análisis y priorización.
Verificar falsos positivos y correlacionar CVEs, CVSS, KEV u otros indicadores.
Emitir recomendaciones de remediación para administradores y líderes de proceso.
Revisar planes de acción, definir urgencia técnica y tiempos sugeridos.
Realizar seguimiento y validar la remediación mediante reescaneo o pruebas de verificación.
Mantener repositorios de evidencias y elaborar informes periódicos.

Líderes de Proceso (Propietarios de Activos/Servicios):
Identificar la criticidad del servicio asociado al activo afectado.
Aprobar los planes de acción de remediación.
Asignar responsables y recursos para la ejecución de las remediaciones.
Gestionar la aceptación del riesgo cuando la remediación no sea viable, elevando la solicitud al Comité.
Asegurarse que los nuevos servicios o activos se integren al alcance del procedimiento de vulnerabilidades.

Administradores de Sistemas, Infraestructura, Bases de Datos y Aplicaciones:
Documentar e implementar acciones de remediación: parches, actualizaciones, correcciones de configuración y hardening.
Coordinar ventanas de mantenimiento con Mesa de Servicio y control de Cambios.

Registrar evidencias de remediación y garantizar su integridad y trazabilidad.
Realizar pruebas funcionales posteriores a la remediación.

Mesa de Servicio (Mesa de Ayuda):
Registrar, categorizar y asignar tickets relacionados con vulnerabilidades.
Controlar el cumplimiento de los tiempos de atención y SLAs asociados.
Apoyar al seguimiento de planes de acción mediante la administración de estados y registros.
Coordinar el Control de Cambios las actividades que involucren modificaciones en ambientes productivos.

Oficial de Protección de Datos Personales:
Participar cuando una vulnerabilidad impacte datos personales o sistemas que los traten.
Evaluar el riesgo a la privacidad y recomendar medidas adicionales cuando corresponda.
Acompañar análisis de incidentes derivados de explotación de vulnerabilidades con impacto en datos personales.

Profesional Contratista de Continuidad del Negocio:
Evaluar vulnerabilidades que afecten servicios esenciales o procesos misionales críticos.
Coordinar acciones para asegurar que los planes de continuidad (BCP/DRP) consideren controles, actualizaciones o mitigaciones necesarias.
Verificar que las remediaciones no afecten la disponibilidad de los servicios críticos.

Proveedores y Terceros:
Cumplir los requisitos contractuales respecto al parcheo y gestión de vulnerabilidades.
Proveer evidencias de remediación y participar en actividades de verificación.
Ajustar configuraciones, versiones o servicios según instrucciones de la ETITC.

4. DEFINICIÓN DE TÉRMINOS

ACTIVO DE INFORMACIÓN DE TI: Cualquier recurso tecnológico —físico, lógico o documental— que permite almacenar, procesar, transmitir o proteger información y que es necesario para la operación y seguridad de los servicios institucionales. Incluye

infraestructura, hardware, software, aplicaciones, datos, configuraciones, documentación técnica y servicios asociados, propios o de terceros.

BCP (BUSINESS CONTINUITY PLAN) Y **DRP (DISASTER RECOVERY PLAN):** Son planes que establecen las acciones, recursos y procedimientos necesarios para mantener los servicios y operaciones críticas de la ETITC de forma continua o recuperarse rápidamente ante interrupciones, fallas graves o desastres que afecten la infraestructura de TI o los servicios tecnológicos.

HARDENING: Actividad de fortalecer la seguridad de un activo de TI mediante la reducción de su superficie de ataque. Incluye la eliminación de servicios innecesarios, la aplicación de configuraciones seguras, el cierre de puertos no utilizados, la deshabilitación de funciones por defecto, el refuerzo de políticas de autenticación y la aplicación de buenas prácticas que minimizan vulnerabilidades explotables.

MESA DE SERVICIO: es el punto único de contacto para la recepción, registro, clasificación y seguimiento de requerimientos, incidentes y actividades operativas de TI. Facilita la coordinación entre usuarios y equipos técnicos, garantiza la trazabilidad de las solicitudes y soporta procesos como gestión de cambios y remediación de vulnerabilidades.

PARCHE: actualización de software diseñada para corregir vulnerabilidades, errores o fallas de seguridad identificadas en un sistema, aplicación o componente tecnológico. Su finalidad es mejorar la protección, estabilidad y funcionamiento del activo de TI afectado.

TICKET DE MESA DE SERVICIO: Es el registro formal y trazable de una solicitud, incidente, requerimiento técnico o actividad operativa de TI que ingresa a través de la Mesa de Servicio. Documenta la información necesaria para gestionar, asignar, dar seguimiento y cerrar la atención, facilitando el control y la evidencia del proceso.

5. REQUISITOS Y CONDICIONES GENERALES

Para aquella información pública clasificada y/o reservada de intercambio de información física o digital con proveedores se debe firmar de mutuo acuerdo el GSI-SI-FO-01 Compromiso de Confidencialidad en cuanto al uso y divulgación de información de la ETITC.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
1. Identificar los activos a evaluar	Profesional Contratista de Ciberseguridad + Líderes de Proceso	N/A	N/A	N/A
2. Programar e informar el escaneo de vulnerabilidades al líder de proceso y Administradores de TI / Aplicaciones / Bases de Datos	Profesional Contratista de Ciberseguridad	N/A	N/A	Correo electrónico
3. Ejecutar el escaneo de vulnerabilidades a los activos identificados	Profesional Contratista de Ciberseguridad	N/A	N/A	Reporte técnico de escaneo
4. Validar los resultados y eliminar falsos positivos	Profesional Contratista de Ciberseguridad	N/A	N/A	N/A
5. Priorizar las vulnerabilidades según criticidad impacto y explotabilidad	Profesional Contratista de Ciberseguridad + Responsable SGSI	N/A	N/A	N/A
6. Solicitar la remediación, acompañada con las recomendaciones técnicas para su solución a través de un Ticket en la mesa de servicio, adjuntando	Profesional Contratista de Ciberseguridad	N/A	N/A	Ticket en Software de gestión

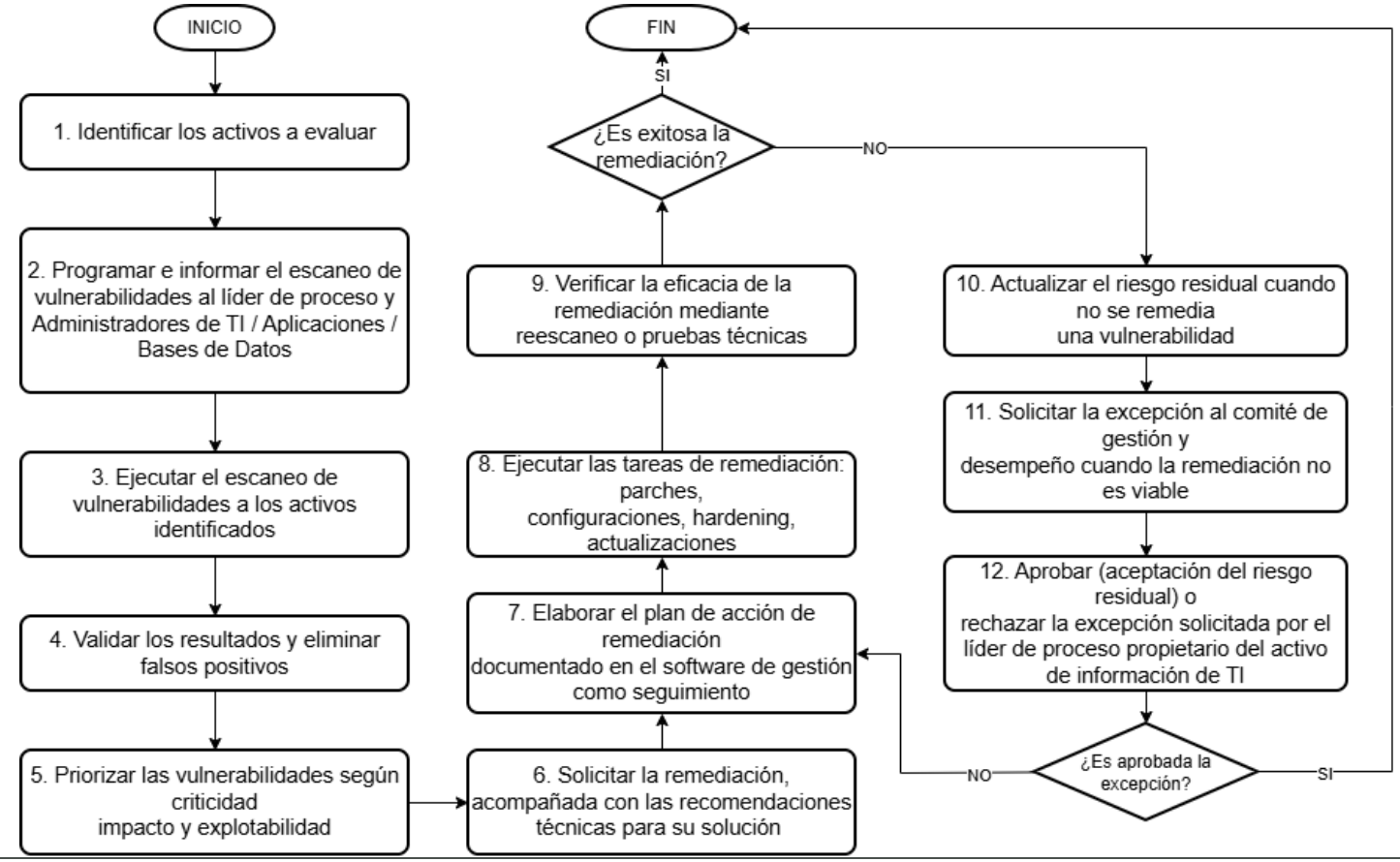
DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
documentación de recomendaciones (puede ser el mismo reporte técnico)				
7. Elaborar el plan de acción de remediación documentado en el software de gestión como seguimiento del caso abierto a partir del Ticket anterior	Líder de Proceso o Administradores de TI / Aplicaciones / Bases de Datos	Validación a cargo del Responsable SGSI cuando aplique	N/A	Plan de acción aprobado y documentado en el software de gestión como seguimiento del caso
8. Ejecutar las tareas de remediación: parches, configuraciones, hardening, actualizaciones	Administradores de TI / Aplicaciones / Bases de Datos	Control de cambios vía Mesa de Servicio	N/A	Evidencias de remediación (capturas, logs, RFC) documentadas en el software de gestión
9. Verificar la eficacia de la remediación mediante reescaneo o pruebas técnicas, en caso de ser exitosa la remediación se da por cerrado y en caso contrario se continua con la siguiente actividad.	Profesional Contratista de Ciberseguridad	Comparación con escaneo previo	N/A	Informe de verificación / remediación de vulnerabilidad adjuntado en el software de gestión
10. Actualizar el riesgo residual cuando no se remedia una vulnerabilidad	Responsable SGSI	De acuerdo con la metodología institucional de riesgos	N/A	Registro de riesgo residual en matriz de riesgos

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
11. Solicitar la excepción al comité de gestión y desempeño cuando la remediación no es viable	Líder del Proceso	N/A	N/A	Solicitud formal de excepción
12. Aprobar (aceptación del riesgo residual) o rechazar la excepción solicitada por el líder de proceso propietario del activo de información de TI. En caso de rechazo regresa al paso 7	Comité de Gestión y Desempeño	Comité	N/A	Acta con registro de excepción aprobada o rechazada

7.ANEXOS:

GSI-SI-FO-01 COMPROMISO DE CONDIFENCIALIDAD EN CUANTO AL USO Y DIVULGACION DE INFORMACIÓN DE LA ETITC

8. DIAGRAMA DE FLUJO



10. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
31/03/2026	1	Adopción del procedimiento

ELABORÓ	REVISÓ	APROBÓ
JORGE A. TAMAYO REINEL. Profesional de Seguridad de la Información	**JAVIER DIAZ MORALES** Profesional del Sistema de Gestión de Calidad	**YANETH JIMENA PIMIENTO CORTÉS** Líder del Proceso de Aseguramiento