PROCEDIMIENTO	Código: **S03.04.09.04**
	Versión: 01
	Vigencia: 24/09/2025
Dueño del proceso: Oficina de Administración	

GESTIÓN DE VULNERABILIDADES TECNICAS

	Nombres y Apellidos	Cargo	Firma y Sello
Elaborado por:	Manuel Aguilar Cori	Oficial de Seguridad y Confianza Digital	Firmado digitalmente por: AGUILAR CORI Manuel Isidro FAU 20380799643 hard Fecha: 23/09/2025 14:46:27
	Víctor Chávez Gómez	Jefe de Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:32:49
Revisado por:	Apolinar Madrid Escobar	Jefe (dt) de la Oficina de Planeamiento y Presupuesto	Firmado digitalmente por: MADRID ESCOBAR Apolinar Junior FAU 20380799643 hard Fecha: 23/09/2025 16:37:05
Aprobado por:	Alberto Blas Ortiz	Jefe de la Oficina de Administración	

Versión	Descripción de Cambios (indicar sección de corresponder)	Fecha
01	Versión inicial	24/09/2025

1. BASE LEGAL

1.1. ISO/IEC 27001:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos” (en adelante ISO/IEC 27001).

1.2. NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos (en adelante NTP-ISO/IEC 27001).

1.3. ISO/IEC 27002 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante ISO/IEC 27002).

1.4. NTP-ISO/IEC 27002:2022 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante NTP-ISO/IEC 27002).

1.5. Versión Actualizada de la Directiva N° 02-2015-SERVIR/GPGSC Régimen Disciplinario y Procedimiento Sancionador de la Ley N° 30057, Ley del Servicio Civil.

1.6. Reglamento Interno de los Servidores Civiles - RIS de la Agencia de Promoción de la Inversión Privada – PROINVERSIÓN.

1.7. Código de Ética de la Agencia de la Promoción de la Inversión Privada PROINVERSIÓN.

2. DEFINICIONES Y SIGLAS

2.1. Definiciones

2.1.1. **Activo de Información:** Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la empresa y tiene un ciclo de vida.

2.1.2. **Ciberseguridad:** Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.

2.1.3. **Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.

2.1.4. **Disponibilidad:** Propiedad de ser accesible y utilizable por petición de una entidad autorizada.

2.1.5. **Evento o Suceso:** Ocurrencia o cambio de un conjunto particular de circunstancias.

Nota 1: Un evento puede ser una o más ocurrencias, y puede tener varias causas.
Nota 2: Un evento puede consistir en algo que no sucede.
Nota 3: Un evento a veces puede ser referido como un "incidente " o "accidente”.

2.1.6. **Evento de Seguridad de Información**: Ocurrencia identificada de un sistema, servicio o el estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación antes desconocida que puede ser la seguridad relevante.

2.1.7. **Gestión de Incidentes de Seguridad de Información:** Aseguramiento que el acceso lógico a los activos de información está autorizado y Procesos para detectar, informar, evaluar, responder frente a, y aprender de incidentes de seguridad de la información.

2.1.8. **Incidente de Seguridad de Información**: Evento único o una serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

2.1.9. **Integridad:** Propiedad de exactitud y lo completo.

2.1.10. **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Nota 1: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.

2.1.11. **SIEM**: Es una solución de seguridad que ayuda a las organizaciones a detectar y responder a amenazas antes de que causen daño. Las herramientas SIEM recopilan, analizan y correlacionan datos de diversas fuentes dentro de una infraestructura de TI para identificar posibles riesgos y vulnerabilidades

2.1.12. **Sistema de Gestión de la 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 del riesgo y de mejora continua.

2.1.13. **Vulnerabilidad:** Susceptibilidad o disposición a ser afectado negativamente por una amenaza o riesgo

2.2. Siglas:

- CGTD: Comité de Gobierno y Transformación Digital.
- SGSI: Sistema de Gestión de Seguridad de la Información.
- OSCD: Oficial de Seguridad y Confianza Digital.

3. RESPONSABILIDADES

3.1. Del Oficial de Seguridad y Confianza Digital (OSCD)

3.1.1. Definir los lineamientos de gestión de vulnerabilidades técnicas.
3.1.2. Realizar coordinaciones con el Especialista de Tecnología de Información y Redes, la atención de cualquier detección de potenciales vulnerabilidades técnicas.
3.1.3. Informar a la alta dirección de cualquier desviación o vulnerabilidad técnica que pueda representar un riesgo para la institución y requiera mediación ejecutiva.
3.1.4. Implementar y mantener controles de seguridad de la información que puedan responder de manera efectiva a las vulnerabilidades técnicas detectadas.
3.1.5. Planificar y realizar la revisión de cumplimiento de controles.

3.2. Jefatura de TI

3.2.1. Revisar y aprobar plan de remediación de vulnerabilidades.

3.3. Del Especialista de tecnologías de información y redes

3.3.1. Resolver oportunamente incidencias asociados a vulnerabilidades técnicas.
3.3.2. Ejecutar prueba de vulnerabilidad interno.
3.3.3. Monitorear constantemente los sistemas, servidores y equipos de redes, asegurando que se encuentren actualizados en su versión más reciente.
3.3.4. Preparar plan de remediaciones a las vulnerabilidades técnicas detectadas.
3.3.5. Informar al OSCD periódicamente sobre la identificación de potenciales amenazas detectadas que puedan afectar la infraestructura de la entidad, producto de una vulnerabilidad técnica detectada.

3.4. Del Especialista de tecnologías de información externo

3.4.1. Ejecutar pruebas de vulnerabilidad externo.
3.4.2. Preparar informe de vulnerabilidades técnicas detectadas e informar a PROINVERSION.

4. GENERALIDADES

4.1. Análisis de vulnerabilidades interno

4.1.1. Con el objetivo de identificar información de vulnerabilidades recientes, cada administrador de sistemas debe verificar las recomendaciones de los fabricantes de los

sistemas de información de PROINVERSION y evaluar su aplicación, de acuerdo con la criticidad del mismo.

4.1.2. Asimismo, de forma inopinada los administradores de sistemas o el Oficial de Seguridad y Confianza Digital, pueden revisar fuentes externas, con el objetivo de identificar si existen vulnerabilidades técnicas asociadas a la tecnología utilizada en PROINVERSION, como: https://www.cvedetails.com/index.php.

4.1.3. Toda vez que se descubra una vulnerabilidad de seguridad, se debe seguir la aplicación de parches de seguridad.

4.1.4. El OSCD es el encargado de administrar toda la información referida a vulnerabilidades de seguridad.

4.1.5. Así mismo se encargará de monitorear que los administradores de sistemas elaboren y actualicen el registro de vulnerabilidades, cuya información estará compuesta por los datos consignados por los fabricantes.

4.1.6. Toda vez que el OSCD actualice el registro de vulnerabilidades, publicará y comunicará a cada uno de los administradores involucrados la ubicación del documento que contiene la información de las vulnerabilidades.

4.2. Análisis de vulnerabilidades externo

4.2.1. Anualmente se programará actividades de escaneo de vulnerabilidades externo, con el objetivo de identificar potenciales vulnerabilidades en la plataforma tecnológica de PROINVERSION y complementar el análisis interno.

4.2.2. Una vez culminado el escaneo de vulnerabilidades externo, con los resultados obtenidos se procederá a planificar la aplicación de remediaciones y se incluirá en las actividades de atención de vulnerabilidades.

4.3. Atención de vulnerabilidades

4.3.1. Los administradores involucrados designarán al especialista que consideren, la atención de la vulnerabilidad asignada, en cuyo registro tendrán que consignar la siguiente información de carácter obligatorio para su respectivo seguimiento:

- Responsable de atención
- Fecha programada de atención
- Estado de atención
- Comentarios

4.3.2. Toda vez que los especialistas responsables de la atención de vulnerabilidades efectúen alguna acción sobre las vulnerabilidades deberán de actualizar el registro especificando las actividades realizadas y actualizando los campos obligatorios indicados en el punto anterior.

4.3.3. El registro actualizado se enviará al OSCD, quien efectuará el seguimiento del cumplimiento de su atención.

4.4. Gestión de parches de seguridad

4.4.1. Asegurar que todos los componentes de sistemas y software cuenten con los parches de seguridad más recientes, proporcionados por los fabricantes.

4.4.2. Es responsabilidad de cada administrador de componente de sistema, monitorear periódicamente (de preferencia mensualmente), la publicación de parches de seguridad por parte de los fabricantes, así como la evaluación e implementación de los mismos.

4.4.3. Los parches de seguridad catalogados como importantes (críticos) deberán de ser instalados dentro del periodo de 30 días, contando desde la fecha de su lanzamiento.

4.4.4. Los parches de seguridad catalogados como menos críticos deberán de ser instalados dentro del periodo de 90 días, contando desde la fecha de su lanzamiento.

4.4.5. En el caso que no se realice la instalación de los parches de seguridad dentro del periodo indicado en el acápite anterior, se deberá registrar, los motivos por los cuales no se ha efectuado la instalación del parche de seguridad, una descripción del riesgo al cual se encuentra expuesto el servicio y una descripción de las acciones y controles compensatorios implementados a fin de mitigar los riesgos de no instalar los parches de seguridad.

5. SECUENCIA DE ACTIVIDADES

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Programar prueba de vulnerabilidad técnica			
1	Seleccionar activos a los cuales se les realizara prueba de vulnerabilidad técnica • Inventario de activos: Mantener actualizado el registro de hardware, software y servicios expuestos	Área de TI.	OSCD
2	Definir tipo de prueba de vulnerabilidad Interno: Realizado por el Especialista de Tecnologías de Información y Redes Externo: Realizado por especialista de tecnologías de información externo, con experiencia en el manejo de herramientas de escaneo de vulnerabilidades ¿Es prueba interna? **Si:** Ir a tarea 3 **No:** Ir a tarea 5	Área de TI.	OSCD
Ejecutar prueba de vulnerabilidad técnica interna			
3	Ejecutar prueba de vulnerabilidad interna Especialista de Tecnología de Información y Redes, realiza prueba de detección de vulnerabilidades en la plataforma tecnológica de PROINVERSION, considerando los siguientes inputs: Reportes de proveedores, análisis interno, entre otros)	Área de TI.	Especialista de Tecnología de Información y Redes
4	Elaborar informe de vulnerabilidades internas	Área de TI.	Especialista de Tecnología de Información y Redes
Ejecutar prueba de vulnerabilidad técnica externa			
5	Ejecutar prueba de vulnerabilidad externa Especialista de TI externo realiza prueba de detección de vulnerabilidades con monitoreo de especialistas de tecnologías de información y redes de **PROINVERSION** Para el escaneo de vulnerabilidades se pueden utilizar herramientas como: Tenable, Qualys, Rapid7	Área de TI.	Especialista de Tecnologías de Información Externo
6	Elaborar informe de vulnerabilidades externa	Área de TI.	Especialista de Tecnologías de Información Externo
Preparar plan de remediación de vulnerabilidades			
7	Analizar resultados de pruebas de vulnerabilidad efectuadas	Área de TI	Especialista de Tecnología de Información y Redes
8	Elaborar plan de remediación de vulnerabilidades técnicas Una vez obtenidos los resultados de pruebas de vulnerabilidad interna o externa, se procede a clasificar y organizar por orden de prioridad los resultados, con el fin de dar atención a las mismas **Priorización**: • Basada en CVSS (Common Vulnerability Scoring System) o metodologías internas. • Considerar: ○ Impacto potencial (confidencialidad, integridad, disponibilidad). ○ Explotabilidad (facilidad de ataque). ○ Contexto de la organización	Área de TI	Especialista de Tecnología de Información y Redes
Revisar plan de remediación			
9	Revisar plan de remediación de vulnerabilidades técnicas propuesto	Área de TI	OSCD
Aprobar plan de remediación de vulnerabilidades			
10	Evaluar plan de remediaciones de vulnerabilidades propuesto ¿Se requiere aprobación? Si: Ir a tarea 11 No: Ir a tarea 8	Área de TI	Jefe de TI
11	Aprobar plan de remediación de vulnerabilidades	Área de TI	Jefe de TI

Ejecutar remediaciones de vulnerabilidades			
12	Ejecutar remediaciones de vulnerabilidades técnicas Se aplican medidas según el riesgo: • Parcheo/Actualización: Aplicar parches de seguridad. • Controles compensatorios: Si no hay parche disponible (Ej: segmentación de red, reglas de WAF). • Aceptación del riesgo: Solo si el impacto es bajo y está justificado.	Área de TI	Especialista de Tecnología de Información y Redes
Documentación de atención de vulnerabilidades			
13	Documentar atención de vulnerabilidades técnicas • Reportes: Incluir hallazgos en revisiones de la dirección. • Actualización del SGSI: Ajustar políticas según lecciones aprendidas. • KPI's: ○ Tiempo promedio de detección y remediación ○ Número de vulnerabilidades críticas sin parches	Área de TI	OCSD
Fin			

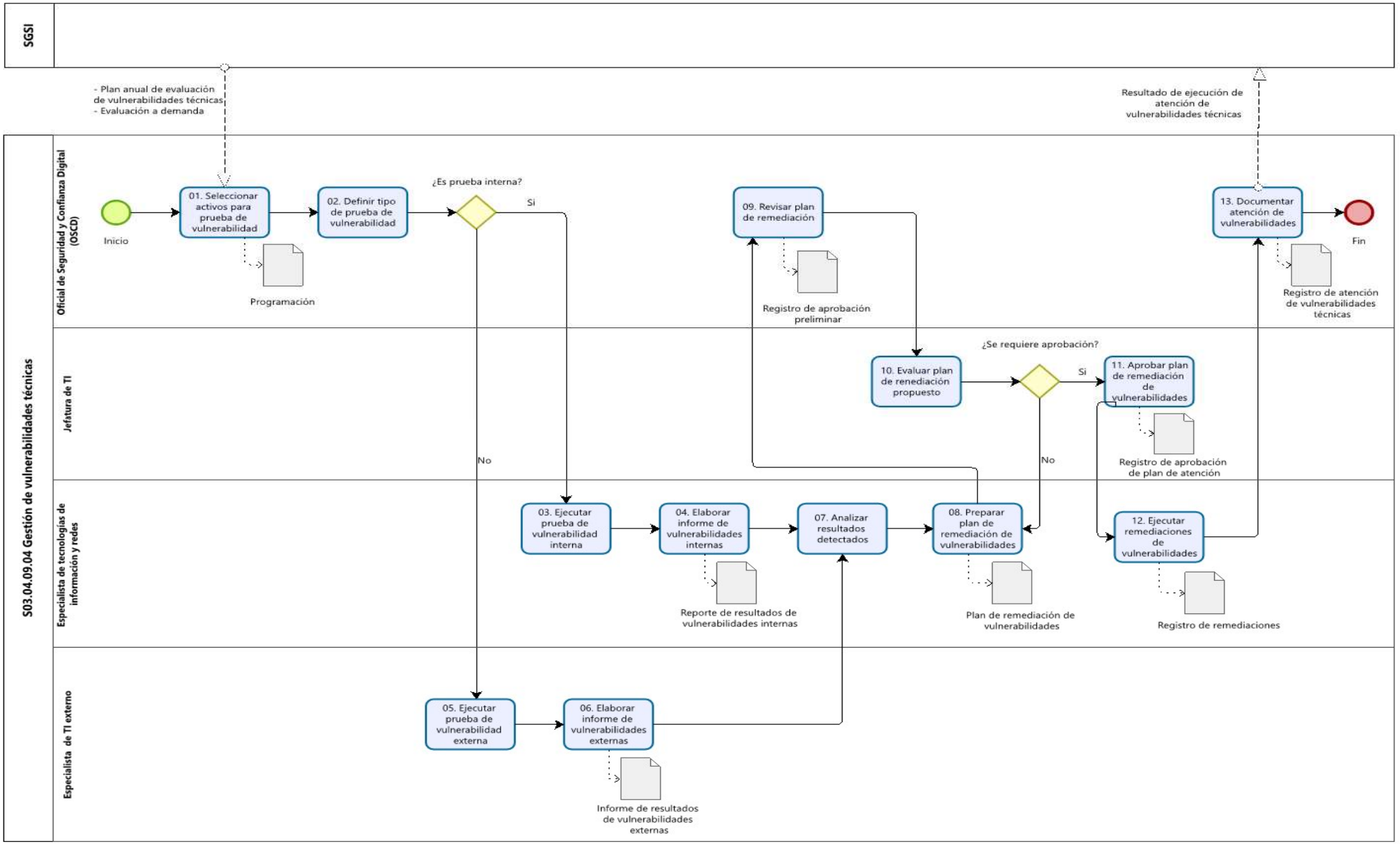
6. ANEXOS

6.1. Herramientas recomendadas para detección de vulnerabilidades técnicas
6.2. Flujograma del Procedimiento

Anexo N° 01

“Herramientas recomendadas para detección de vulnerabilidades técnicas”

- Escaneo de vulnerabilidades: Tenable, Qualys, Rapid7.
- Gestión de parches: WSUS, SCCM, ManageEngine.
- SIEM: Splunk, IBM QRadar (para correlación de eventos).


SGSI
- Plan anual de evaluación de vulnerabilidades técnicas
- Evaluación a demanda
Resultado de ejecución de atención de vulnerabilidades técnicas
S03.04.09.04 Gestión de vulnerabilidades técnicas
Oficial de Seguridad y Confianza Digital (OSCD)
Jefatura de TI
Especialista de tecnologías de información y redes
Especialista de TI externo
Inicio
01. Seleccionar activos para prueba de vulnerabilidad
Programación
02. Definir tipo de prueba de vulnerabilidad
¿Es prueba interna?
Si
No
09. Revisar plan de remediación
Registro de aprobación preliminar
10. Evaluar plan de renediación propuesto
¿Se requiere aprobación?
Si
No
11. Aprobar plan de remediación de vulnerabilidades
Registro de aprobación de plan de atención
13. Documentar atención de vulnerabilidades
Fin
Registro de atención de vulnerabilidades técnicas
03. Ejecutar prueba de vulnerabilidad interna
04. Elaborar informe de vulnerabilidades internas
Reporte de resultados de vulnerabilidades internas
07. Analizar resultados detectados
08. Preparar plan de remediación de vulnerabilidades
Plan de remediación de vulnerabilidades
12. Ejecutar remediaciones de vulnerabilidades
Registro de remediaciones
05. Ejecutar prueba de vulnerabilidad externa
06. Elaborar informe de vulnerabilidades externas
Informe de resultados de vulnerabilidades externas