 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GIT-PR-003
	PROCEDIMIENTO: GESTIÓN DE VULNERABILIDADES TÉCNICAS	Versión: 1
		Fecha: 03/Oct/2025

PROCEDIMIENTO: GESTIÓN DE VULNERABILIDADES TÉCNICAS	
OBJETIVO:	Establecer las actividades para la gestión de vulnerabilidades de seguridad técnica de los sistemas de información e infraestructura tecnológica de la Superintendencia de Notariado y Registro (SNR), utilizando metodologías y herramientas, con el fin de mantener un nivel de aseguramiento adecuado para mitigar los riesgos asociados.
ALCANCE:	Limite Inicial: Elaborar plan anual de gestión de vulnerabilidades técnicas.
	Limite Final: Remediación de vulnerabilidades y amenazas técnicas.
PRODUCTOS:	Informe ejecutivo y técnico de vulnerabilidades, formato de gestión de vulnerabilidades técnicas.
RESPONSABLE:	Líder Estratégico: Jefe Oficina Tecnologías de la Información Líder Operativo: Coordinador de Servicios de Tecnológicos, Coordinación Innovación y Desarrollo, Coordinación Sistemas de Información

1. GLOSARIO

Activo: cualquier cosa de valor que se utilice y es necesaria para completar una tarea empresarial. Los activos incluyen elementos tangibles e intangibles. (CISCO - Administración de Amenazas Cibernéticas).

Análisis del riesgo: proceso que permite comprender la naturaleza del riesgo y determinar el nivel del riesgo. (NTC-ISO/IEC 27000).

Confidencialidad: propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados. (NTC-ISO/IEC 27000).

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad autorizada. (NTC-ISO/IEC 27000).


Dueño del riesgo: persona o entidad que tiene la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (NTC-ISO/IEC 27000).

Mitigación: reducir la probabilidad o la gravedad de una pérdida por amenazas. (CISCO - Administración de Amenazas Cibernéticas).

Pruebas de penetración – pentest o hackeo ético: uso de técnicas y herramientas de piratería para penetrar las defensas de la red e identificar la profundidad de la penetración potencial. (CISCO - Administración de Amenazas Cibernéticas).

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más ausando daños o perjuicios a la Organización. (MAGERIT – versión 3.0, libro I – Método).

Vulnerabilidad: cualquier falla o debilidad que permita que una amenaza cause daño y dañe un activo. Algunos ejemplos pueden ser el código de error, las configuraciones incorrectas y el incumplimiento de los procedimientos. (CISCO - Administración de Amenazas Cibernéticas).

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GIT-PR-003
		Versión: 1
	PROCEDIMIENTO: GESTIÓN DE VULNERABILIDADES TÉCNICAS	Fecha: 03/Oct/2025


2. CONDICIONES GENERALES:

2.1. Normatividad:


- Ley 1928 de 2018 “Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.”
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.”
- Ley Estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales.”
- Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.”
- Estrategia Nacional Digital de Colombia 2023 – 2026.
- Decreto 338 de 2022 “Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”.
- Decreto 1078 del 26 de mayo de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Resolución 500 del 10 marzo de 2021 “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”.

2.2. Políticas de operación

1. Este procedimiento deberá tener en cuenta la política general y políticas específicas del Sistema de Gestión de Seguridad de la Información (SGSI).

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GIT-PR-003
	PROCEDIMIENTO: GESTIÓN DE VULNERABILIDADES TÉCNICAS	Versión: 1
		Fecha: 03/Oct/2025


2. Los análisis de vulnerabilidades técnicas deberán realizarse mínimo una vez por año.
3. No está permitido el uso de herramientas de escaneo o explotación de vulnerabilidades dentro de la entidad, ni la ejecución de ningún tipo de análisis o prueba por parte de entidades externas o usuarios de la entidad sin previa autorización de la Alta Dirección, Jefe de la Oficina de Tecnología de la Información o del Oficial de Seguridad de la Información, de evidenciarse lo anterior, se deberá aplicar el PROCEDIMIENTO GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN.
4. En las pruebas de penetración, la entidad podrá contratar estos servicios con terceros o hacerlo con personal de la SNR para el análisis en la infraestructura de la Entidad y en donde se considere necesario de acuerdo con la criticidad de los activos de información afectados.
5. Las pruebas de penetración deben llevarse a cabo en un entorno controlado y conforme al alcance definido. Se deberá tener autorización por escrito del jefe de la OTI para realizar pruebas que generen indisponibilidad, degradación o falla en el servicio.
6. Las herramientas utilizadas para el escaneo deben estar debidamente licenciadas o contar con derechos de uso libre.
7. Los informes, evidencias y etapas de descubrimiento deben ser confidenciales, por ningún motivo se deben divulgar, salvo estricta autorización por escrito del jefe de la OTI.
8. Cualquier evento e incidente de seguridad de la información que genere la explotación de una vulnerabilidad deberá activarse el procedimiento de gestión de Incidentes, eventos y debilidades de seguridad de la información.
9. La priorización de vulnerabilidades técnicas se establecerá de acuerdo con criterios de impacto y posibilidad de explotación. De priorizarse de una forma diferente deberá ser documentada en los informes técnicos correspondientes.
10. Los Administradores de los sistemas y/o líderes de los aplicativos deberán estar pendientes de las brechas de seguridad para mitigarlas o informarlas oportunamente.
11. Anualmente al finalizar la ejecución del Plan de gestión de Vulnerabilidades, se realizará reunión con la jefatura de tecnología para presentación de informe final de vulnerabilidades y remediaciones.

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GIT-PR-003
		Versión: 1
	PROCEDIMIENTO: GESTIÓN DE VULNERABILIDADES TÉCNICAS	Fecha: 03/Oct/2025


12. Los desarrollos o servicios que sean contratados por la Superintendencia de Notariado y Registro, y que tengan una exposición pública en internet, deberán incluir y aprobar un proceso de análisis de vulnerabilidades y Ethical hacking que debe ser asumido por el proveedor contratado. Es responsabilidad del dueño del proceso del área técnica que requiere la necesidad o el proceso a contratar, pedir asesoría de la Oficina de tecnología, para añadir esta obligación en el anexo técnico.
13. La ejecución de planes preventivos o correctivos que requieran ser aplicados en la infraestructura tecnológica, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de los colaboradores que administren dicha infraestructura tecnológica. Lo anterior, aplicando los lineamientos del PROCEDIMIENTO DE CONTROL DE CAMBIOS DE TI.
14. El plan de gestión de vulnerabilidades técnicas se realizará priorizando los activos que sean más críticos para la entidad y en el que su afectación de integridad, confidencialidad y disponibilidad puedan causar mayor impacto a la entidad. Lo anterior, con base a la matriz de riesgos de seguridad digital y catálogos de sistemas de información con los que cuenta la entidad. Así mismo, se incluirán las necesidades específicas que sean requeridas por el Jefe de Oficina de Tecnología de la Información.

3. DESCRIPCIÓN DE ACTIVIDADES DEL PROCEDIMIENTO:

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
1. ELABORAR PLAN DE GESTIÓN DE VULNERABILIDADES	1.1 Elaborar plan de gestión de vulnerabilidades donde se establece: alcance, contexto, cronograma, metodología, responsables y reportes.	Jefe de Oficina TI Oficial de seguridad Especialista de seguridad	Plan Anual de gestión de Vulnerabilidades.
2. VALIDAR Y APROBAR EL PLAN DE GESTIÓN DE VULNERABILIDADES	2. 1 Validar y aprobar el plan de gestión de vulnerabilidades, este debe contener: alcance, contexto, cronograma, metodología, responsables y reportes, dicho plan debe ser revisado y actualizado anualmente. ¿Se aprueba el plan de gestión de vulnerabilidades? Sí: Notificar. Actividad 3. No: Volver a la actividad 1, solicitar correcciones mediante correo electrónico.	Jefe OTI Especialista de seguridad	Correo electrónico
3. NOTIFICAR LA APROBACIÓN	3.1 Notificar la aprobación a los interesados para que se cumpla con el escaneo de vulnerabilidades o prueba de penetración. Nota: Tener en cuenta los activos que se van a proteger según su criticidad.	Especialista de seguridad	Correo electrónico

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GIT-PR-003
		Versión: 1
	PROCEDIMIENTO: GESTIÓN DE VULNERABILIDADES TÉCNICAS	Fecha: 03/Oct/2025

4. REALIZAR ESCANEADO DE VULNERABILIDADES O PENTESTING	4.1 Realizar escaneo de vulnerabilidades o pentesting El escaneo de vulnerabilidades o las pruebas de penetración deben ejecutarse de acuerdo con el alcance previamente definido y aprobado. Para la correcta ejecución de las pruebas, se debe consultar el Manual de Gestión de Vulnerabilidades Técnicas de la SNR.	Especialista de seguridad y/o Proveedor	Correo electrónico
5. REALIZAR LOS INFORMES	5.1 Elaborar informes gerenciales y técnicos detallados sobre los resultados de las pruebas, priorizando las vulnerabilidades identificadas. Los informes deberán incluir recomendaciones claras para la remediación de cada amenaza o vulnerabilidad detectada.	Especialista de seguridad y/o Proveedor	Informe gerencial y técnico
6. INFORMAR LAS VULNERABILIDADES Y AMENAZAS TÉCNICAS	6.1 Informar las vulnerabilidades y amenazas técnicas con sus respectivas sugerencias de mitigación a los administradores de sistemas probados, realizando el plan de mitigación con su correspondiente cronograma. Nota: Es una fase en conjunto por parte de los responsables del proceso de vulnerabilidades de la SNR con el fin de mostrar resultados de las fases anteriores con las partes interesadas de la OTI.	Especialista de seguridad y/o Proveedor Administrador del sistema jefe OTI	E-mail. Reunión con las partes
7. REMEDIAR LAS VULNERABILIDADES Y AMENAZAS TÉCNICAS	7.1 Remediar las vulnerabilidades y amenazas técnicas conforme al plan de mitigación y la priorización de las vulnerabilidades.	Administrador del sistema Especialista de seguridad	Herramienta de control de cambios
8. VERIFICAR LA MITIGACIÓN DE LAS VULNERABILIDADES Y AMENAZAS TÉCNICAS	8.1 Verificar la mitigación de las vulnerabilidades y amenazas técnicas mediante un retest de vulnerabilidades, cuyo resultado será enviado al administrador del sistema OTI / Oficial de seguridad. Nota: El administrador del sistema solicitará por correo electrónico la realización del retest.	Administrador del sistema Especialista de seguridad y/o Proveedor	Correo electrónico. Informe técnico de retest
9. VALIDAR QUE LAS VULNERABILIDADES Y AMENAZAS HAYAN SIDO REMEDIADAS CONFORME A LOS RESULTADOS DEL RETEST	9.1 Se valida que las vulnerabilidades y amenazas hayan sido remediadas conforme los resultados del retest. ¿Se remedian vulnerabilidades? Sí: Generar el informe de remediación de vulnerabilidades. Avanza a la actividad 10. No: Ir actividad 7. Remediar las vulnerabilidades técnicas, devolver mediante correo electrónico.	Administrador del sistema Especialista de seguridad y/o Proveedor Oficial de seguridad	Correo electrónico Informe remediación de vulnerabilidades
10. ORGANIZACIÓN DE DOCUMENTOS FIN	10.1 Archivar conforme los parámetros de gestión documental para archivos físicos y digitales	Personal OTI	Repositorio documental OTI

 Superintendencia de Notariado y Registro	PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GIT-PR-003
		Versión: 1
	PROCEDIMIENTO: GESTIÓN DE VULNERABILIDADES TÉCNICAS	Fecha: 03/Oct/2025

4. DOCUMENTOS ASOCIADOS:

4.1. Documentos internos: Manual de Vulnerabilidades

4.2. Documentos externos: No aplica

VERSIÓN DE CAMBIOS			
Código:	Versión:	Fecha:	Motivo de la actualización:
	1	3 de Octubre de 2025	Se hace necesario ajustar la documentación en el marco del fortalecimiento institucional con el fin de alinearlos al Sistema Integrado de Gestión y el nuevo modelo por procesos de la Entidad.

ELABORACIÓN Y APROBACIÓN			
ELABORÓ	APROBÓ	REVISIÓN METODOLOGICA	Vo. Bo. Oficina Asesora de Planeación
Robinson Vallejo Cortes Juan Carlos Valenzuela Johan Lorenzo Contreras Flórez	José Ricardo Acevedo Solarte	Juan Sebastián Ávila	Santiago Campo Victoria
Oficina de Tecnologías de la Información	Jefe Oficina de Tecnologías de la Información	Contratistas OAP	Jefe Oficina Asesora de Planeación
Fecha: 22 de septiembre 2025	Fecha: 25 de septiembre 2025	Fecha: 30 de septiembre 2025	Fecha de Aprobación: 3 de Octubre 2025