



Superintendencia de Notariado y Registro



MANUAL PARA LA GESTIÓN DE VULNERABILIDADES TÉCNICAS

Gestión de Tecnologías de la Información

**SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO**

Código: CTI - MN - 001	Versión: 1	Fecha: 3/Oct/2025
-------------------------------	-------------------	--------------------------

JOSÉ RICARDO ACEVEDO SOLARTE
JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
JUAN CARLOS VALENZUELA BUITRAGO
PROFESIONAL OFICINA DE TECNOLOGIA DE LA
INFORMACIÓN
SANTIAGO CAMPO VICTORIA
JEFE OFICINA ASESORA DE PLANEACIÓN

SEPTIEMBRE/ 2025



República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro



TABLA DE CONTENIDO

INTRODUCCIÓN	4
OBJETIVO	4
GLOSARIO DE TÉRMINOS	4
MARCO LEGAL	4
MANUAL PARA LA GESTIÓN DE VULNERABILIDADES TÉCNICAS	7
1. PLANEACIÓN DE LA GESTIÓN DE VULNERABILIDADES TÉCNICAS	7
2. EJECUCIÓN DE LAS PRUEBAS DE VULNERABILIDAD	7
3. ASPECTOS PARA DEFINICIÓN DE ESPECIFICACIONES PARA PRUEBAS CONTRATADAS	8
4. EJECUCIÓN DE PRUEBAS DE VULNERABILIDAD	8
5. REMEDIACIÓN DE VULNERABILIDADES	9
6. VERIFICAR LA MITIGACIÓN DE LAS VULNERABILIDADES Y AMENAZAS TÉCNICAS	10
7. SISTEMAS DE INFORMACIÓN PUBLICADOS EXTERNAMENTE	10
8. REVISIONES PERIÓDICAS DE ALERTAS DE SEGURIDAD	10
BIBLIOGRAFÍA	11
DOCUMENTOS ASOCIADOS	12



Superintendencia de Notariado y Registro

INTRODUCCIÓN

La gestión de las vulnerabilidades técnicas consiste en proteger los activos de información y tecnológicos que pueden ser afectados por amenazas internas y externas derivadas del uso de los sistemas y aplicaciones, mediante la realización de diferentes actividades que permiten identificar, analizar y mitigar las brechas de seguridad. Lo anterior permite robustecer los pilares de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad generando un ecosistema digital seguro y confiable.

El presente documento referencia fases importantes a tener en cuenta antes, durante y después de la gestión de vulnerabilidades técnicas como son la planeación, en donde se deben identificar los tipos de pruebas; la reunión inicial y contextualización, en la cual se identifican los responsables, administradores de sistemas, canales de comunicación, entre otros; la ejecución de pruebas, basadas en marcos de trabajo nacionales e internacionales; la entrega de informes; exposición de los hallazgos y el seguimiento de los resultados. Lo anterior busca dar una hoja de ruta que permita a la entidad mantener un proceso preventivo, proactivo y de buenas prácticas en la ciberseguridad de los activos de información y tecnológicos.

OBJETIVO

Establecer lineamientos que permitan la gestión adecuada de las vulnerabilidades técnicas de los activos de información y tecnológicos de la Superintendencia de Notariado y Registro, mediante pruebas de vulnerabilidades y penetración, verificación de código, análisis de los hallazgos, mitigación y seguimiento.

GLOSARIO DE TÉRMINOS

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).

Amenaza: acto malicioso o un evento inesperado que daña los sistemas de información u otros recursos de la organización relacionados. (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).

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. (MAGERIT – versión 3.0, libro I – Método).



Superintendencia de Notariado y Registro

Ciberseguridad: es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio. (CISCO).

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).

Integridad: propiedad de exactitud y completitud. (NTC-ISO/IEC 27000).

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

Pruebas de vulnerabilidad: consiste en realizar escaneos en una red o aplicación web para identificar problemas potenciales y proceder con la evaluación de lo hallado para determinar el nivel del riesgo y el plan de mitigación.

Open Web Application Security Project (OWASP): es una comunidad libre y gratuita a nivel mundial centrada en la mejora de la seguridad del software de aplicación.

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 activos causando daños o perjuicios a la Organización. (MAGERIT – versión 3.0, libro I – Método).

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. (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).



MARCO LEGAL

- 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”.



MANUAL PARA LA GESTIÓN DE VULNERABILIDADES TÉCNICAS

1. PLANEACIÓN DE LA GESTIÓN DE VULNERABILIDADES TÉCNICAS

Las pruebas de vulnerabilidad en la infraestructura tecnológica deben centrarse en identificar y mitigar cualquier brecha de seguridad presente.

De acuerdo con lo anterior, el equipo de seguridad de la información liderado por el Oficial de Seguridad de la Información debe definir un Plan de Evaluación de Vulnerabilidades para la infraestructura tecnológica y los sistemas de información vulnerados. Este Plan debe incluir los siguientes elementos:

- Dispositivos a cubrir en las pruebas.
- Alcance de las pruebas, que abarcará los sistemas de información y los equipos en la red de datos.
- Tipo de pruebas a realizar (externas, internas, con o sin conocimiento previo del dispositivo).
- Nivel de explotación de vulnerabilidades (detección, explotación intrusiva, denegación de servicio, entre otros).
- Implicaciones y consideraciones antes, durante y después de las pruebas a los dispositivos y aplicaciones.

El plan propuesto por el equipo de seguridad y el Oficial de Seguridad de la Información será revisado y aprobado por el Jefe de la Oficina de Tecnologías de la Información.

Nota: En el caso que para el periodo en cuestión las pruebas sean contratadas con un tercero, en el Plan se deberá establecer las actividades de generación de anexos técnicos de acuerdo con el alcance que se defina. Así mismo, se deberá establecer una proyección de inicio de ejecución de las actividades.

2. EJECUCIÓN DE LAS PRUEBAS DE VULNERABILIDAD

Las pruebas de vulnerabilidad pueden ser realizadas ya sea por el equipo de la SNR encabezado por el Oficial de Seguridad de la Información de la Entidad, o por un proveedor externo seleccionado. Se recomienda que las pruebas sean realizadas por diferentes ejecutores (proveedores externos - especialista de seguridad de la SNR) de un periodo al otro. Esta práctica permite obtener una evaluación más objetiva y completa de la seguridad, facilitando la identificación de posibles vulnerabilidades desde diversas perspectivas.



3. ASPECTOS PARA DEFINICIÓN DE ESPECIFICACIONES PARA PRUEBAS CONTRATADAS

Para las pruebas que sean contratadas con terceros, se debe establecer claramente el alcance del tipo de pruebas a realizar. Lo anterior, acorde con el tipo de información que se entregará, del conocimiento que se tiene de la Entidad y de su estructura, se pueden realizar 3 tipos de prueba:

Pruebas de caja negra: No se tiene información del funcionamiento del sistema a probar, simulando pruebas como si fuera un usuario habitual. Toma poco tiempo su realización.

Pruebas de caja gris: Se cuenta con información limitada sobre el funcionamiento del sistema a probar, lo cual le da cierta ventaja al simular la prueba de penetración.

Pruebas de caja blanca: Se tiene información sobre el funcionamiento del sistema a probar, lo cual le permite simular una prueba de penetración como si fuera un funcionario de la entidad o alguien que obtuvo la información con anterioridad mediante el reconocimiento del objetivo. Lleva más tiempo su realización.

Se recomienda que, para las pruebas contratadas se incluyan pruebas de caja negra como primera fase, esto permitirá identificar un análisis de superficie de información expuesta por la SNR como insumo de posibles brechas de seguridad. Una vez finalizadas, se debe incluir pruebas de caja blanca al alcance definido de activos.

Aunado a lo anterior, se debe tener en cuenta que tipos de pruebas de penetración se requiere realizar:

- Pruebas de penetración de red.
- Prueba de penetración de aplicaciones web.
- Prueba de penetración de red inalámbrica.
- Prueba de penetración física.
- Ingeniería social.

4. EJECUCIÓN DE PRUEBAS DE VULNERABILIDAD

El ejecutor de las pruebas, para el cumplimiento del Plan de Evaluación de Vulnerabilidades deberá establecer un cronograma detallado de fechas y horario de las actividades. Así mismo, debe entregar un informe de pruebas de vulnerabilidad, recomendaciones y pruebas finales de verificación.



Superintendencia de Notariado y Registro

De evidenciarse alguna vulnerabilidad crítica en la ejecución de la prueba, se debe reportar inmediatamente al Jefe de la Oficina de Tecnología o al Oficial de Seguridad de la Información, para tomar acción inmediata sobre la misma.

Una vez finalizada la etapa de pruebas, el ejecutor debe consolidar la información recopilada y generar un informe técnico que debe ser socializado al administrador del sistema de información o colaborador encargado del activo.

El informe técnico presentado debe contemplar los siguientes aspectos:

- Dispositivos cubiertos en las pruebas.
- Evidencia recopilada.
- Vulnerabilidades identificadas e impacto estimado.
- Recomendaciones para cierre de vulnerabilidades.

Si el proceso de análisis de vulnerabilidades es realizado por la Entidad, quedará bajo responsabilidad de la Oficina Tecnología de la Información la generación de los Planes de Acción para la implementación de las recomendaciones realizadas. Cuando haya sido contratado con un tercero, se realizará proceso de remediación, conforme a lo establecido en el anexo técnico.

El informe deberá ser remitido al responsable de la Gestión de Riesgos de Seguridad de la Información o al líder de seguridad de la información para alimentar las debilidades o vulnerabilidades detectadas en incluirlas como riesgos de seguridad digital en la Matriz de Riesgos del sistema de gestión de seguridad de la información y con lo anterior documentar el Plan de Tratamiento de riesgos de seguridad de la información.

NOTA: El informe de vulnerabilidades se deberá tratar como información RESERVADA, únicamente estará bajo custodia del responsable del equipo de seguridad de la información y el jefe de la Oficina Tecnología información.

Una vez culmine la ejecución de pruebas a la infraestructura o información definida en el alcance, se deberá generar un informe con un resumen gerencial para ser presentado al Jefe de Tecnología de la Información.

5. REMEDIACIÓN DE VULNERABILIDADES

Toda identificación de vulnerabilidades deberá ser remediada o se le deben implementar medidas compensatorias. El responsable del activo de información que presente vulnerabilidades será encargado de desplegar, coordinar o ejecutar las acciones y recomendaciones que se requieran, y deberá retroalimentar el avance.



En dado caso que para la implementación de acciones compensatorias o de remediación se requiera hacer un cambio en la infraestructura, se deberá proceder conforme al PROCEDIMIENTO CONTROL DE CAMBIOS DE TI.

6. VERIFICAR LA MITIGACIÓN DE LAS VULNERABILIDADES Y AMENAZAS TÉCNICAS

El equipo de seguridad de la información o colaborador encargado del equipo de seguridad de la información realizará seguimiento periódico de los avances de remediación y establecerá una fecha máxima para la aplicación de estas.

- Clasificación	- Código	- CVSS o equivalente	- Tiempo para remediación
- Critica	- C	- 9.0-10.0	- 30 días
- Alta	- A	- 7.0-8.9	- 30 días
- Media	- M	- 4.0-6.9	- 45 días
- Baja	- B	- 0.0-3.9	- 90 días

Con el fin de realizar seguimiento y verificar que las vulnerabilidades y amenazas técnicas se hayan mitigado, una vez ejecutadas las remediaciones por parte del colaborador responsable o cumplidos los tiempos pactados para la remediación, se realizará un retest; el cual consiste en repetir la prueba de vulnerabilidad o penetración, generando un informe de remediación de vulnerabilidades con los hallazgos en donde se analiza si el Plan de Mitigación tuvo éxito o si debe implementar controles o actualizaciones.

7. SISTEMAS DE INFORMACIÓN PUBLICADOS EXTERNAMENTE

Todos los sistemas de información que sean modificados o adquiridos y que vayan a ser publicados externamente, deberán someterse a un análisis de vulnerabilidades antes de su paso a producción. Esta actividad podrá ser realizada por un proveedor contratado o por el equipo de seguridad de la información, liderado por el Oficial de Seguridad de la Información.

El Coordinador de servicios tecnológicos o quien haga sus veces o el servidor público delegado por ese grupo de coordinación, deberá asegurarse de que, antes de la liberación y publicación del servicio, se hayan realizado las pruebas de vulnerabilidades y se hubieran mitigado aquellas que hayan sido detectadas.

8. REVISIONES PERIÓDICAS DE ALERTAS DE SEGURIDAD

El personal del equipo de Seguridad de la Información de la Oficina de Tecnología de la Información realizará la verificación de las alertas de seguridad emitidas por organizaciones y foros de seguridad de la información



Superintendencia de Notariado y Registro

de orden nacional e internacional, con el fin de verificar vulnerabilidades y eventos de seguridad que se hayan presentado o que sean susceptibles de ocurrencia.

En caso de encontrar información crítica respecto a amenazas o vulnerabilidades que puedan afectar la infraestructura tecnológica de la Entidad, se deberá comunicar de forma inmediata, por medio de correo, al encargado del activo con copia al Jefe de la Oficina Tecnología de la Información y comunicar la debilidad conforme al PROCEDIMIENTO GESTIÓN DE INCIDENTES, EVENTOS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN, con el fin de que se tomen inmediatamente las acciones preventivas necesarias para evitar algún impacto a las infraestructura tecnológica de la Entidad.

BIBLIOGRAFÍA

Instituto Colombiano de Normas Técnicas y Certificación. (2017). NTC-ISO-IEC 27000 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Visión general y vocabulario. Bogotá: ICONTEC. Recuperado el 23 de julio de 2024.

Instituto Colombiano de Normas Técnicas y Certificación. (2022). NTC-ISO-IEC 27001 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. Bogotá: ICONTEC. Recuperado el 25 de julio de 2024.

Instituto Colombiano de Normas Técnicas y Certificación. (2022). NTC-ISO-IEC 27005 Seguridad de la información, ciberseguridad y protección de la privacidad. Orientaciones sobre la gestión de los riesgos para la seguridad de la información. Bogotá: ICONTEC. Recuperado el 25 de julio de 2024.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2016). Guía Metodológica de Pruebas de Efectividad. Bogotá: MINTIC. Recuperado el 03 de julio de 2024.

MITRE ATT&CK. (2024). Adversarial Tactics, Techniques, and Common Knowledge. Estados Unidos: MITRE ATT&CK. Recuperado el 03 de julio de 2024.

National Institute of Standards and Technology. (2008). Special Publication 800-115 Technical Guide to Information Security Testing and Assessment. Estados Unidos: NIST. Recuperado el 04 de julio de 2024.

National Institute of Standards and Technology. (2021). NIST Publicación especial 1271. Estados Unidos: NIST. Recuperado el 08 de julio de 2024.



Superintendencia de Notariado y Registro

Open Web Application Security Project. (2014). OWASP Web Security Testing Guide v4. Estados Unidos: OWASP. Recuperado el 05 de julio de 2024.

Open Web Application Security Project. (2016). Threat Modeling. Estados Unidos: OWASP. Recuperado el 16 de julio de 2024.

The Institute for Security and Open Methodologies. (2010). OSSTMM 3 The Open-Source Security Testing Methodology Manual. Estados Unidos: ISECOM. Recuperado el 04 de julio de 2024.

DOCUMENTOS ASOCIADOS.

Procedimiento Gestión de Vulnerabilidades Técnicas.

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	Alberto Higueta Goetz Sandra Milena Niño Camacho	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