



AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN (ARN)

GUÍA DE GESTIÓN DE VULNERABILIDADES

BOGOTÁ D.C. MAYO DE 2026

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

TABLA DE CONTENIDO

	Pág.
1. OBJETIVO	3
2. ALCANCE	3
3. DEFINICIONES	3
4. CONDICIONES GENERALES	7
4.1 PREREQUISITOS	8
4.2 ANÁLISIS DE VULNERABILIDADES	9
4.3 ETHICAL HACKING	9
5. DESARROLLO DE LAS ACTIVIDADES	11
5.1 RECONOCIMIENTO	12
5.2 ESCANEEO	12
5.3 EXPLOTACIÓN	13
5.4 POST EXPLOTACIÓN	13
5.5 GENERACIÓN DE INFORME	14
5.6 REMEDIACIÓN DE VULNERABILIDADES	15
5.7 VERIFICACIÓN DE REMEDIACIÓN (RE-TEST O RE-ESCANEEO DE VULNERABILIDADES)	16
5.8 INFORMES	17

LISTA DE TABLAS

	Pág.
Tabla 1. Informes a entregar a la OTI	17

LISTA DE ILUSTRACIONES

	Pág.
Ilustración 1. Distribución	9
Ilustración 2. Diagrama Caja Negra	10
Ilustración 3. Diagrama Caja Gris	11
Ilustración 4. Metodología	12

	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

1. OBJETIVO

Establecer los lineamientos para evaluar y gestionar el nivel de exposición a vulnerabilidades en los sistemas operativos, servicios, aplicaciones y dispositivos que conforman la infraestructura tecnológica de la Agencia, mediante la identificación, análisis, priorización y seguimiento de los activos de información definidos por la OTI, con el fin de reducir el riesgo asociado, orientar las acciones de remediación y mantener actualizada la matriz de vulnerabilidades con sus respectivas recomendaciones técnicas y medidas preventivas y correctivas durante la vigencia correspondiente.

2. ALCANCE

La gestión de vulnerabilidades inicia con la definición de los activos de información objeto de los ejercicios de escaneos, seguido con la identificación de debilidades a través de los escaneos periódicos de vulnerabilidades programados y las pruebas de Ethical Hacking, conforme al cronograma de ejecución previamente aprobado por esta dependencia. Esta etapa da paso al proceso de remediación, el cual se desarrolla con base en los hallazgos obtenidos y en coordinación con los responsables asignados. También se contempla la atención de vulnerabilidades reportadas por terceros especializados que puedan afectar la infraestructura tecnológica de la Agencia. La actividad finaliza con la presentación de informes técnicos, la socialización de resultados con los líderes de servicio y responsables de los activos analizados, y la entrega de avances documentados sobre la gestión y remediación realizada, teniendo en cuenta que es un proceso continuo debido a la naturaleza.

3. DEFINICIONES

ACTIVO DE INFORMACIÓN: es todo recurso que genera, procesa, transporta y/o resguarda información necesaria para la operación y el cumplimiento de los objetivos del BCE, por lo tanto, se requiere proteger su confidencialidad, integridad y disponibilidad de las amenazas propias de su naturaleza y características.

ANALÍSTA DE CIBERSEGURIDAD: encargado de planificar, implementar, mejorar, o monitorean medidas de seguridad para proteger las redes de computadoras y la información.

AMENAZAS: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

ARN: Agencia para la Reincorporación y Normalización.

ATAQUE DE MOVIMIENTO LATERAL: son técnicas de ataques de hackers informáticos que son utilizadas para propagarse a través de una red buscando assets e información clave

CAJA NEGRA: se refiere a un tipo de pruebas o técnica donde un hacker ético no tiene conocimiento de la información del sistema que se está evaluando.

CAJA GRIS: tipo de prueba de penetración que se sitúa entre las pruebas de caja negra y caja blanca. En este enfoque, el evaluador tiene conocimiento parcial del sistema objetivo.

CENTRO DE OPERACIONES DE SEGURIDAD - SOC: encargado de monitorear la seguridad informática del cliente y generar alertas y eventos en caso de que se identifique situaciones que afecten la seguridad del cliente

CONSECUENCIA: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

DOMINIO: un nombre de dominio (a menudo denominado simplemente dominio) es un nombre fácil de recordar asociado a una dirección IP física de Internet. Se trata del nombre único que se muestra después del signo @ en las direcciones de correo y después de www. en las direcciones web.

EQUIPOS INFORMÁTICOS: son equipos que permiten almacenar y procesar información.

ESCANEO: es la identificación, análisis y reporte de vulnerabilidades (entendida como una falla que permite que una amenaza se convierta en un riesgo).

ESPECIALISTA: persona encargada de desarrollar periódicamente tareas de pentest (penetration testing) y todo tipo de ataque ético (Ethical Hacking) con el fin de identificar y medir vulnerabilidades eliminando los falsos positivos.

ETHICAL HACKING: utilizado para explotar las vulnerabilidades existentes en el sistema que se requiere evaluar, valiéndose de un test de intrusión, que permite verificar y evaluar la seguridad física y lógica de sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, entre otros

 Agencia para la Reinserción y la Normalización - ARN	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

componentes de la infraestructura tecnológica, con la intención de ganar acceso y demostrar que un sistema es vulnerable.

EXPLOIT: en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

EXPLOTACIÓN: es el aprovechamiento de una debilidad o una brecha de seguridad. También es entendido como un código, método o vía, que permite a un atacante informático o a un auditor de seguridad, explotar una vulnerabilidad conocida, para poder comprometer la seguridad de un sistema informático, y tomar posesión y control de este.

FALSOS POSITIVOS: detección de errores o defectos presentados por inestabilidad del sistema, bases de datos corruptas o por alguna causa externa que haga que el entorno no esté funcionando como debería.

HALLAZGO DE SEGURIDAD: vulnerabilidad encontrada en los activos de información y sistemas objeto de los ejercicios de escaneo de vulnerabilidades y ethical hacking.

HTTPS: el Protocolo seguro de transferencia de hipertexto es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

INCIDENTE: evento único o 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.

LAN (Red de área local): son un conjunto de dispositivos electrónicos conectados entre sí que comparten una línea de comunicación común o un enlace inalámbrico con un servidor.

LÍDER DE SERVICIO: profesional designado por la ARN el cual es responsable de la correcta funcionalidad de los servicios y activos de información de la entidad.

	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

MITIGACIÓN: es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

MEDIOS PÚBLICOS: son todos los servicios de la ARN que se encuentran expuestos en internet.

OTI: Oficina de tecnología de la información.

OWASP (Open Web Application Security Project): es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

PLAN DE REMEDIACIÓN: permite identificar los riesgos asociados a cada vulnerabilidad reportada, así como definir los controles que deben ser implementados para mitigar dichos riesgos.

POST EXPLOTACIÓN: es una serie de pasos que se deben seguir posterior a la obtención de penetración en un sistema, estos pasos consisten en entendimiento de la víctima, escalamiento de privilegios, eliminación de logs y procesos de monitorización, recolección de información, establecimiento de puertas traseras, movimiento lateral.

PRUEBAS DE VULNERABILIDAD: las pruebas de vulnerabilidades (también llamadas evaluación de vulnerabilidades o en inglés, "Vulnerability Assessment") son un tipo de prueba de software que se realiza para evaluar los riesgos de seguridad de un software con el fin de reducir la probabilidad de amenazas y futuros ataques que puedan explotar las vulnerabilidades de dicho software.

RECONOCIMIENTO: es la fase de preparación donde el atacante obtiene toda la información necesaria de su objetivo y/o víctima antes de lanzar un ataque.

RED DE SERVIDORES DE DESARROLLO: es el espacio de trabajo donde el programador desarrolla el código de la aplicación, realiza pruebas iniciales y comprueba si la aplicación se ejecuta correctamente con ese código.

RED DE SERVIDORES DE PRODUCCIÓN: el entorno de producción es el

 Agencia para la Reinserción y la Normalización - ARN	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

entorno donde finalmente se ejecuta la aplicación donde acceden los usuarios finales y donde se trabaja con los datos de negocio en sí mismos.

REMEDIACIÓN: acción que permite minimizar el impacto de las vulnerabilidades en la organización.

RIESGO: efecto que se causa sobre los objetivos de la entidad, debido a eventos potenciales.

SEGMENTO DE RED: refiere a un LAN el cual hace referencia a un conjunto o agrupación de varios equipos informáticos (computadoras y/o periféricos que están conectados entre sí en una red, a través de realizar una segmentación de red se obtienen ventajas de aumento en el rendimiento y favorece la seguridad.

SISTEMAS DE INFORMACIÓN: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

SUBDOMINIO: un subdominio es un subgrupo o subclasificación del nombre de dominio el cual es definido con fines administrativos u organizativos, que podría considerarse como un dominio de segundo nivel. Normalmente es una serie de caracteres o palabra que se escriben antes del dominio.

VULNERABILIDAD: representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. CONDICIONES GENERALES

La gestión de vulnerabilidades es un proceso continuo que consistente en la identificación, evaluación y remediación de vulnerabilidades en los activos de información de la entidad, que de acuerdo con las buenas prácticas, atraviesa por un ciclo de vida el cual va desde la identificación de la debilidad, hasta que es remediada, ofreciendo a la ARN un panorama real sobre el estado de seguridad en los diferentes activos de información definidos y analizados, para con esto, poder determinar el nivel de exposición y las medidas que se implementan o fortalecen en la postura de seguridad de la agencia.

Para el cubrimiento de los activos de información definidos por la OTI y descritos en el alcance, se definieron los siguientes ítems de ejecución:

	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

- Ejecución de las pruebas de vulnerabilidades, Ethical Hacking.
- Documentación de los hallazgos.
- Realizar los entregables que correspondan según el numeral de 5.9 INFORMES.
- Realizar la presentación de los resultados a los responsables técnicos, administradores de plataformas, líderes de servicios tecnológicos y demás actores involucrados, según corresponda.
- El SOC presenta el cronograma de ejecución de vulnerabilidades, Ethical Hacking para revisión y evaluación de la OTI, el cual contiene la metodología que se describe en esta guía.

4.1 PREREQUISITOS

Es necesario contar con los siguientes requerimientos antes de ejecutar la actividad:

4.4.1 Pruebas de Vulnerabilidad

- Definir con el líder del servicio de la ARN, los activos de información a ser objeto del análisis de vulnerabilidades.
- Socializar la prueba con los dueños de los activos o servicios de TI de la ARN que fueron definidos previamente.
- Asegurar que el sensor de la herramienta a utilizar para las pruebas alcance los activos de información definidos por la ARN.
- Programar escaneos periódicos de vulnerabilidades, los cuales son acordados en conjunto entre el proveedor de servicios y la ARN.

4.1.2 Ethical Hacking

- Definir con la entidad el tipo de prueba a realizar (caja blanca, negra o gris).
- Definir con el líder del servicio de la ARN, los activos de información a ser objeto del análisis del Ethical Hacking.
- Para pruebas internas se requiere puntos de red o conexión inalámbrica, según se defina, para dar conectividad a los especialistas que ejecutarán las pruebas y acceso al segmento de red de los activos de información a

	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

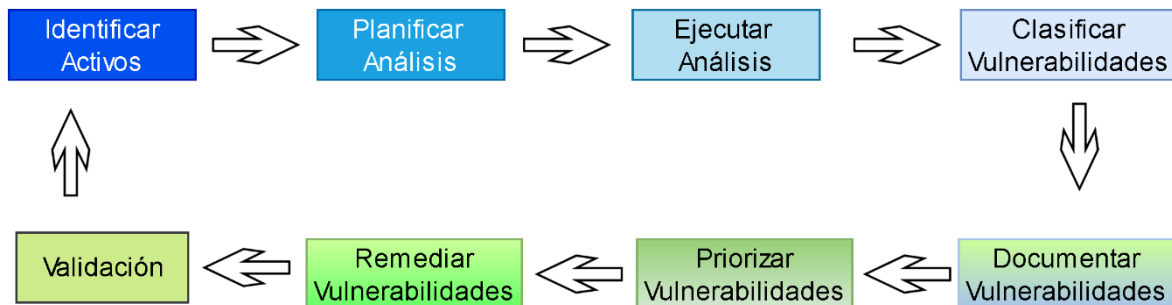
ser evaluados.

- Para Pruebas Externas: aprobación de parte de la entidad para la ejecución.
- Dos (2) ciclos de evaluación, sobre los cuales se realizará la fase de identificación de vulnerabilidades de Ethical Hacking, correspondiente una en cada semestre del año.

4.2 ANÁLISIS DE VULNERABILIDADES

Para la ejecución de las pruebas de análisis de vulnerabilidades, se tiene como referencia el siguiente enfoque que permite determinar metodológicamente como realizarlas a sistemas operativos, aplicaciones, redes inalámbricas y/o infraestructura tecnológica de la agencia.

Ilustración 1. Distribución



Fuente: SOC

El análisis de vulnerabilidades se realiza mediante el uso de herramientas para la detección de estas con el apoyo especialistas que permitan tipificar los resultados eliminando los falsos positivos. El servicio de análisis de vulnerabilidades se diferencia del Ethical Hacking por la fase de explotación la cual requiere el uso de varias herramientas y el conocimiento del especialista para su ejecución.

Finalizados los ejercicios, se realizará entrega de la información según lo descrito en el numeral "5.8. INFORMES".

4.3 ETHICAL HACKING

El Ethical Hacking es un conjunto de pruebas de seguridad, en donde un profesional de seguridad ejecuta ataques reales controlados con técnicas

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

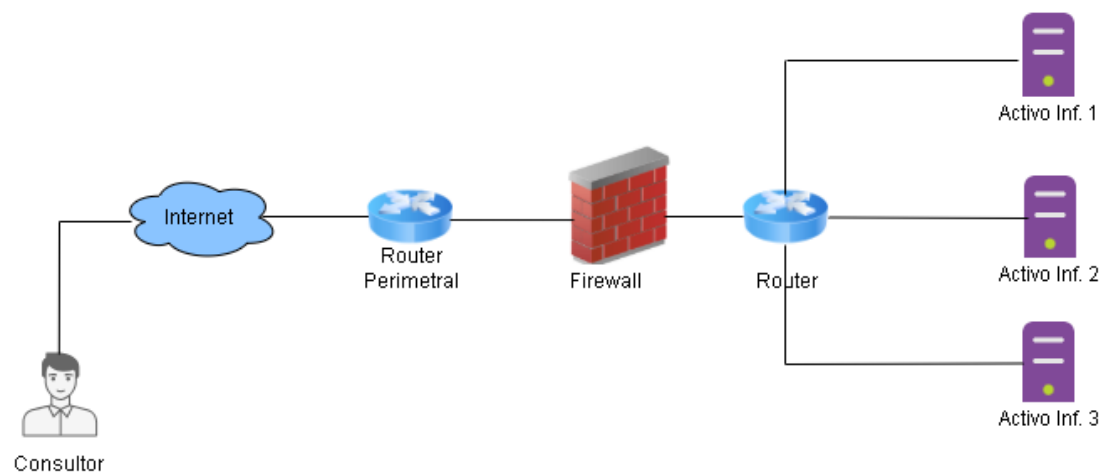
especializadas para la detección y explotación de vulnerabilidades que poseen los activos de la agencia, sin afectar la disponibilidad del activo de información. En este servicio el especialista toma el rol de un atacante real que busca explotar y aprovecharse de las vulnerabilidades detectadas para comprometer los sistemas de información y ganar acceso en los sistemas y activos de información de la agencia.

Al finalizar la ejecución de las pruebas, se realizará entrega de la información según lo descrito en el numeral “5.8 INFORMES”.

Ambiente: Externo

Tipo Prueba: Penetración de Caja Negra

Ilustración 2. Diagrama Caja Negra



Fuente: SOC

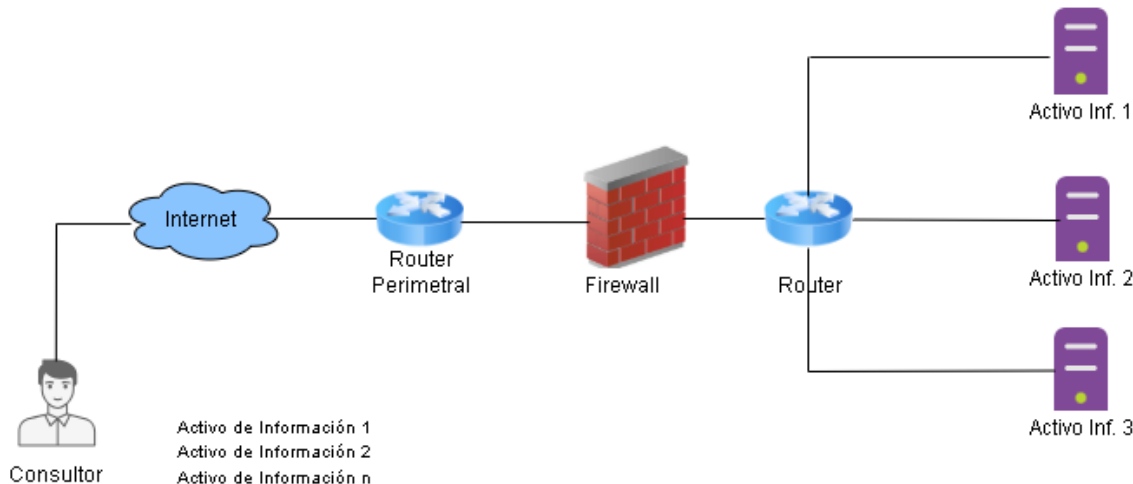
Las pruebas son realizadas por los especialistas desde cualquier punto fuera de la ARN. El objetivo de este tipo de pruebas es simular el accionar de un atacante remoto hacia los activos de información, que se encuentran expuestos en Internet. Este tipo de pruebas permite valorar la visibilidad que tiene el atacante externo y el impacto asociado a la explotación de las vulnerabilidades detectadas.

Ambiente: Interno

Tipo de Prueba: Penetración Caja Gris

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

Ilustración 3. Diagrama Caja Gris



Fuente: SOC

Este tipo de pruebas de seguridad se sitúa entre caja blanca y caja negra. En este enfoque, los especialistas en seguridad tienen un nivel de acceso parcial a la información y a los sistemas de la agencia. Esto significa que se les proporciona cierta información sobre los activos de información y los sistemas a evaluar, pero no cuentan con un conocimiento completo y detallado.

El objetivo de este tipo de pruebas es simular el accionar de un atacante remoto hacia los activos de información, que se encuentran expuestos en Internet. Este tipo de pruebas permite valorar la visibilidad que tiene el atacante externo y el impacto asociado a la explotación de las vulnerabilidades detectadas. De acuerdo con lo anterior los especialistas se limitan a ejecutar las pruebas sobre el inventario de activos definido y entregado por la agencia, de los cuales no recibe información adicional. Este tipo de pruebas son realizadas desde fuera de las instalaciones de la Entidad.

5. DESARROLLO DE LAS ACTIVIDADES

La gestión de vulnerabilidades constituye una práctica fundamental para propender por la seguridad de la información en las entidades del Estado colombiano. Su implementación en la ARN permite identificar y corregir debilidades tecnológicas que podrían ser aprovechadas por actores maliciosos, reduciendo así el riesgo de incidentes que afecten la confidencialidad, integridad y disponibilidad de la información. Así mismo, propende por el cumplimiento de las normativas nacionales e internacionales en materia de seguridad de la

	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

información, optimiza los recursos institucionales al priorizar riesgos críticos, altos y medias fortaleciendo la continuidad de la operación misional. De esta manera, la ARN consolida una postura proactiva frente a las crecientes amenazas en el entorno digital.

Se tiene como referencia el siguiente enfoque que permite determinar metodológicamente la realización de las pruebas independientemente si se trata de unas pruebas de vulnerabilidades, Ethical Hacking internas/Externas a los activos de información definidos por la agencia.

La ejecución y validación de estas actividades está a cargo de un equipo de especialistas en ciberseguridad, con experiencia en gestión y remediación de vulnerabilidades y Ethical Hacking, trabajando en conjunto con los líderes funcionales y técnicos de la ARN.

Ilustración 4. Metodología



Fuente: SOC

5.1 RECONOCIMIENTO

En esta fase busca la recolección de la mayor cantidad de información a través de medios públicos y servicios expuestos (levantamiento de información activa y pasiva).

En la fase de recolección pasiva, se analizaron fuentes abiertas (OSINT) como motores de búsqueda, registros públicos, redes sociales, sitios web institucionales y repositorios públicos, obteniendo información relacionada con nombres de dominio, subdominios, direcciones IP asociadas, metadatos embebidos en documentos públicos y huellas tecnológicas.

En la fase activa, se realizaron escaneos controlados sobre los sistemas identificados, permitiendo descubrir servicios, puertos abiertos, banners de servicios, tecnologías utilizadas y posibles configuraciones inseguras.

Lo anteriormente mencionado, permite identificar posibles puntos de entrada iniciales que podrían ser aprovechados en etapas posteriores de un ataque dirigido.

5.2 ESCANEO

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

Una vez identificados los activos de información pertenecientes a la agencia y que se encuentren dentro del alcance, los especialistas realizan la ejecución de técnicas con el uso de herramientas que permitan identificar activos expuestos, tales como: servidores, sistemas operativos, puertos, versiones de servicios, aplicaciones web, portales de autenticación, entre otros. También, durante esta etapa, se realizará el escaneo y análisis de vulnerabilidades asociadas a los activos de información encontrados, la validación de los hallazgos y la investigación de las vulnerabilidades, los cuales son alojados en la carpeta definida por la entidad.

5.3 EXPLOTACIÓN

Esta fase tiene como objetivo validar de forma práctica el aprovechamiento de las vulnerabilidades identificadas y priorizadas para dimensionar el impacto real sobre los activos de información evaluados.

Las pruebas simulan el comportamiento de un atacante real dentro de un entorno debidamente autorizado, bajo controles que garantizan la continuidad operacional. En ningún caso se ejecutarán acciones que comprometan la disponibilidad de los servicios, tales como ataques de denegación de servicio (DoS/DDoS).

Las actividades se limitan estrictamente al acceso inicial, mediante la explotación de vulnerabilidades en sistemas, aplicaciones o configuraciones inseguras, haciendo uso de exploits, shells, payloads u otras técnicas ofensivas controladas.

El éxito de esta etapa se determina al obtener un punto de entrada válido al sistema objetivo, sin avanzar hacia acciones posteriores al compromiso. Todo ello priorizando la integridad y disponibilidad de los activos de información de la entidad.

Las actividades de explotación deberán ejecutarse únicamente sobre los activos definidos dentro del alcance previamente aprobado para la ejecución del ejercicio de análisis de vulnerabilidades o pruebas de Ethical Hacking. En caso de requerirse la validación de impacto en ambientes productivos, estas deberán contar con autorización previa, expresa y documentada por parte de la Oficina de Tecnologías de la Información o del responsable del activo tecnológico evaluado, garantizando que su ejecución no genere afectaciones sobre la disponibilidad de los servicios institucionales.

5.4 POST EXPLOTACIÓN

Esta fase inicia una vez confirmado el acceso inicial de la etapa anterior, y tiene como propósito evaluar el alcance real del compromiso, simulando las acciones

"Toda impresión física de este documento se considera Documento no Controlado.

La versión vigente se encuentra en el software para la administración de la planeación y la gestión"

Página 13 de

	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

que un atacante ejecutaría para maximizar el impacto de su intrusión. A diferencia de la explotación, esta fase opera desde el interior del entorno comprometido e incluye actividades como: escalamiento de privilegios, movimientos laterales, enumeración interna, recolección de credenciales, creación de backdoors, persistencia y exfiltración simulada de datos, etc. Esto permite medir el impacto máximo potencial y evaluar la capacidad de detección y respuesta de la entidad.

Todas las pruebas y hallazgos serán tratados con estricta confidencialidad, priorizando la protección de la integridad y disponibilidad de los activos de información de la agencia de tal modo que las técnicas usadas permitan evidenciar el impacto y alcance del ataque sin afectar los servicios. Cualquier técnica que implique el uso de algún Payload, script o artefacto, debe ser eliminado al terminar el desarrollo de esta fase

Las actividades de post-explotación que impliquen validación de acceso a información sensible, escalamiento de privilegios o verificación de movimiento lateral, entre otras actividades propias del ejercicio, dentro de los activos tecnológicos deberán contar obligatoriamente con autorización previa, expresa y documentada por parte de la Oficina de Tecnologías de la Información o del responsable del activo de información involucrado, y deberán ejecutarse exclusivamente dentro del alcance aprobado del ejercicio, garantizando en todo momento la no afectación de la integridad de la información ni la continuidad de los servicios institucionales.

5.5 GENERACIÓN DE INFORME

Debido a la importancia del reporte, se definió esta etapa para la generación de los reportes y/o informes según lo descrito en el numeral “5.8 INFORMES”, que facilita su comprensión tanto para equipos técnicos como para la alta dirección, de esta manera, el reporte no solo identifica las áreas de mejora, sino que también ofrece una hoja de ruta práctica para reducir la superficie de ataque y mejorar la postura de seguridad global de la agencia.

El reporte técnico contiene información sobre el alcance de las pruebas, los activos que se evaluaron, la metodología empleada, los detalles técnicos de hallazgos de seguridad, la criticidad de las vulnerabilidades encontradas, los datos técnicos de los activos que presentan cada vulnerabilidad, la descripción y CVE asociado a cada vulnerabilidad, recomendaciones para la mitigación de las vulnerabilidades, los hallazgos, la evidencia de la intrusión y las conclusiones.

Mientras que el reporte ejecutivo contiene un breve resumen, evitando utilizar lenguaje técnico, sobre los activos evaluados, los hallazgos más relevantes de

	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

seguridad, evidencias de intrusión y conclusiones, los cuales serán presentados a los líderes de cada servicio.

5.5.1 Socialización de resultados

Una vez generados los informes de análisis de vulnerabilidades y pruebas de Ethical Hacking y que estos hayan sido verificados por parte del profesional de Seguridad y redes y el líder de Ciberseguridad, el proveedor de servicios a través de la Oficina de Tecnologías de la Información realizará la socialización de los resultados con los responsables técnicos, administradores de plataformas, líderes de servicios tecnológicos y demás actores involucrados, según corresponda.

5.6 REMEDIACIÓN DE VULNERABILIDADES

Con base en los reportes de vulnerabilidades de los activos de información por medio de pruebas Ethical Hacking y/o escaneo de vulnerabilidades, al igual que las vulnerabilidades identificadas y/o comunicadas por terceros especializados, que impacten los activos de información de la infraestructura tecnológica de la ARN, se realiza el tratamiento para la remediación de vulnerabilidades en conjunto entre la gestión de vulnerabilidades y la gestión de seguridad de la información, la ejecución de las actividades para la remediación de vulnerabilidades será realizada por parte de los Líderes del Servicio (administradores de las plataformas); en el caso que sea una remediación compleja, el Líder del Servicio (Administrador de plataforma) creará un plan de trabajo para la remediación. El profesional de Seguridad y redes y el líder de Ciberseguridad, con base en sesiones de seguimiento e informes mensuales, verifican que las acciones del plan de remediación se cumplan de acuerdo con lo concertado o si existe alguna desviación justificada.

Para lo anterior, el SOC creará un caso padre en la herramienta de gestión, asociando a este los casos hijo respectivos, estos casos hijo serán agrupados dependiendo de las vulnerabilidades encontrada (críticas, altas y medias), para posteriormente generar el caso con esta categoría y asignar al administrador de la plataforma o dueño de servicio según corresponda encargado de la remediación de las vulnerabilidades. La remediación de las vulnerabilidades medias y bajas, se trabajarán en la medida de lo posible, toda vez que se da prioridad a la gestión de las vulnerabilidades críticas y altas.

Una vez se realice la asignación del caso se inicia el seguimiento a las remediaciones por parte del Líder técnico de vulnerabilidades, con el fin de

 Agencia para la Reincorporación y la Normalización - ARN	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

propender al cierre de los casos asignados. La gestión de vulnerabilidades realizada será comunicada en los informes mensuales.

Es importante aclarar que, una vez se disponga de los resultados del nuevo escaneo vulnerabilidades y/o del informe de Ethical Hacking correspondientes al siguiente semestre, se creará un nuevo caso padre y nuevos casos hijo para estos, por lo anterior, los casos (padre e hijo) que no fueron gestionados en el periodo anterior se cerrarán, dejando constancia sobre el caso que la gestión continuará bajo el nuevo caso padre y sus casos hijos correspondientes. Las vulnerabilidades pendientes por remediación del semestre anterior serán incluidas junto a las nuevas vulnerabilidades observadas si estas se presentan.

NOTA: Los casos asociados se cerrarán conforme avance la gestión de remediación correspondiente. Es importante considerar que estas actividades pueden depender de procesos adicionales propios de los servicios involucrados, lo que podría generar la necesidad de extender la fecha de remediación, lo cual, es debidamente sustentado y documentado en cada caso relacionado. El seguimiento al estado de estos casos será realizado por el gestor de remediación de vulnerabilidades y por el líder SOC.

5.7 VERIFICACIÓN DE REMEDIACIÓN (RE-TEST O RE-ESCA NEO DE VULNERABILIDADES)

Una vez implementadas las acciones de remediación por parte de los responsables de los activos tecnológicos sobre los activos reportados, el equipo de ciberseguridad o el SOC deberá realizar un proceso de verificación técnica con el fin de confirmar que la vulnerabilidad reportada ha sido efectivamente remediada o eliminada.

Esta verificación se llevará a cabo mediante la ejecución de re-escaneos manuales y focalizados o pruebas de re-test de la vulnerabilidad en gestión, utilizando las mismas herramientas o metodologías empleadas durante la fase de identificación inicial, con el objetivo de validar que la debilidad ya no se encuentra presente en los activos evaluados.

En caso de que la vulnerabilidad persista, se deberá notificar nuevamente al responsable del activo para que en conjunto con el líder de remediación se analice el análisis pertinente y se generen e implementen acciones correctivas adicionales, manteniendo el caso abierto en la herramienta de gestión, documentando el mismo y realizando el respectivo seguimiento dentro de la matriz de vulnerabilidades hasta que se confirme su cierre,

	GUÍA DE GESTIÓN DE VULNERABILIDADES	CÓDIGO: TI-G-10	
		FECHA 2026-05-22	VERSIÓN V- 2

5.8 INFORMES

Para los servicios de análisis de vulnerabilidades y/o Ethical Hacking se presentan los siguientes informes:

Tabla 1. Informes a entregar a la OTI

ENTREGABLE	DESCRIPCIÓN	SERVICIO	
		Análisis de Vulnerabilidades	Ethical Hacking
Matriz de Vulnerabilidades	Se registran las vulnerabilidades de los activos de información, permite hacer seguimiento de cierre de brechas de seguridad.	Aplica	Aplica
Informe Ejecutivo	Se presentará archivo en formato no editable (PDF), en donde se realizará la presentación ejecutiva con los resultados y recomendaciones más relevantes.	N/A	Aplica
Informe Técnico	Contiene la descripción del escenario en el que se hicieron las pruebas, descripción de la vulnerabilidad, nivel de criticidad, activo de información afectado, recomendaciones, evidencias, información adicional.	N/A	Aplica

Fuente: SOC