TABLA DE CONTENIDO

1. OBJETIVO

Definir los lineamentos que permitan al G.I.T. Tecnologías de la información y las Telecomunicaciones de la ANI, realizar el tratamiento de vulnerabilidades técnicas presentes en los componentes de la infraestructura tecnológica que soporta los procesos de la entidad y que pueden llegar a poner en riesgo los activos de información; lo anterior de manera estándar y organizada.

Con lo anterior se pretende identificar oportunamente los riesgos potenciales de la infraestructura tecnológica de la ANI y proveer un tratamiento preventivo y/o correctivo a los mismos. Dichos lineamientos están enfocados a prevenir y evitar que un atacante logre:

- Acceder y extraer información confidencial
- Modificar información
- Negar un servicio

2. ALCANCE

El alcance de este instructivo contempla todos los componentes de la infraestructura tecnológica de la Agencia Nacional de Infraestructura, está dirigido a los funcionarios y contratistas responsables de la infraestructura tecnológica y de los esquemas de seguridad de la información de la entidad.

Describe las actividades a realizar en el tratamiento de vulnerabilidades, las cuáles inician con la etapa de planeación, continúan con las etapas de disposición del inventario, ejecución de las pruebas, acciones de remediación y pruebas de validación, hasta finalizar con el análisis de resultados.

3. RESPONSABLE

Coordinador G.I.T. Tecnologías de la Información y las Telecomunicaciones de la Vicepresidencia de Planeación, Riesgos y Entorno, quien debe garantizar la adecuada implementación del presente instructivo para el tratamiento de vulnerabilidades técnicas.

El Personal que realiza las actividades de Infraestructura en el l G.I.T. Tecnologías de la Información y las Telecomunicaciones, es responsable de:

i) Tener conocimiento de las vulnerabilidades técnicas de los componentes tecnológicos para gestionarlos de manera preventiva.

ii) Informar al profesional líder del tema de Seguridad de la Información la presencia de alguna vulnerabilidad o cualquier indicio que pueda ser un potencial riesgo para dicha infraestructura, aportando opciones de solución que eliminen o mitiguen los riesgos y acatar las instrucciones que el líder imparta al respecto.

iii) Ejecutar las actividades de respuesta (preventiva / correctiva) frente a la vulnerabilidad identificada. La exposición a esas vulnerabilidades se debe evaluar y se deben tomar las medidas correspondientes para minimizar el riesgo asociado.

iv) Mantener un inventario de activos de información debidamente actualizado y vigente, como base para el tratamiento eficaz de las vulnerabilidades técnicas.
v) Realizar las pruebas de acuerdo con el presente instructivo.
vi) Documentar las evidencias del tratamiento de vulnerabilidades
vii) Tener la base de datos de contacto y especialidad de todos profesionales técnicos (internos/externos), necesarios para apoyar el tratamiento de vulnerabilidades técnicas, esto incluye: proveedores de software, hardware y esquemas de telecomunicaciones, números de versión y las personas responsables.

4. GLOSARIO

ACTIVO: Componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa. La entidad asigna un valor a cada activo que representa el nivel de importancia que tiene el activo en el proceso del negocio.

ACTIVO DE INFROMACIÓN: Se refiere a toda la información o elemento de información que la entidad recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes, que tengan valor para la entidad.

AMENAZA DE SEGURIDAD DE LA INFORMACIÓN: surgen a partir de la existencia de vulnerabilidades, es decir, que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

ANÁLISIS FORENSE DE SEGURIDAD DE LA INFORMACIÓN (Information Security Forensics): Aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información.

ARQUITECTURA DE RED: Descripción, especificación y configuración de los componentes físicos o lógicos en una conexión de dispositivos que comparten recursos.

CIBERATAQUE: En computadoras y redes de computadoras un ataque es un intento de exponer, alterar, desestabilizar, eliminar para obtener acceso sin autorización o utilizar un activo. Está asociado a cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático (ordenador, red privada etc.)

CÓDIGO MALICIOSO: Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONTENIDO MALICIOSO: Hace referencia a la difusión de contenido que ataca en forma maliciosa a personas o a la Agencia, por ejemplo, bromas pesadas y acoso.

NEGACION DE SERVICIO (DDS): Es causada por el uso voraz de recursos de red y de sistemas de información tales como CPU, memoria, espacio en disco o ancho de banda de red, y de esta manera afecta la operación normal de los sistemas de información.

DESBORDAMIENTO DE BUFFER (buffer overflow o buffer overrun): es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer).

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando se requiera por los roles autorizados.

ESCÁNEO DE REDES: Software para adquirir información acerca de las configuraciones de red, puertos, servicios y vulnerabilidades existentes.

ESCÁNEO DE VULNERABILIDADES: Mecanismo que permite identificar los fallos de seguridad de un sistema operativo y de sus servicios. Dicho procedimiento puede ser realizado de forma manual o utilizar herramientas que automatizan el proceso.

INGENIERIA SOCIAL: Consiste en la recolección de información de una persona utilizando estrategias y acciones que no involucran instrumentos físicos, por ejemplo, mentiras, trampas, sobornos o amenazas.

LOG (REGISTRO): es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

PUERTAS TRASERAS: Hace referencia a la utilización e instalación de programas y/o códigos de programación dentro de un software o hardware para evadir los sistemas de seguridad y así lograr acceso de manera indebida a estos.

RECOLECCIÓN Y ANÁLISIS DE EVIDENCIA: Actividad referente a la toma, preservación, documentación y análisis de datos o información que pueda usarse como prueba o evidencia.

PRUEBAS DE VALIDACIÓN: Repetición del mismo test aplicado en el análisis de vulnerabilidades. Este procedimiento sirve sobre todo para medir la fiabilidad (o confiabilidad) de la prueba en cuestión.

SISTEMA DE DETECCIÓN DE INTRUSOS: (Intrusion Detection System(IDS)): es un programa de detección de accesos no autorizados a un computador o a una red.

SISTEMA DE INFORMACIÓN: Cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales, así como el software, firmware o hardware que forme parte del sistema.

SOLUCIÓN DE ERRORES CONOCIDOS: Serie de pasos previamente establecidos que permiten resolver un problema en un equipo tecnológico o un Software.

VULNERABILIDAD DE SEGURIDAD DE LA INFORMACIÓN: Debilidad de un activo o de un grupo de activos que podría permitir que una amenaza se materialice y genere un impacto no deseado a la Entidad.

Nota: Las definiciones anteriores fueron tomadas de fuentes oficiales en cada una de las ramas a las que corresponden en el ámbito técnico de tecnologías de la información y las comunicaciones.

5. NORMATIVIDAD

El presente instructivo se encuentra soportado por las normas y lineamientos del gobierno nacional en el campo de seguridad de la información, a continuación, se listan algunos de ellos:

- Ley 1581 de 2012 de protección de datos personales
- Ley 1712 de 2014 de acceso a la información pública
- Manual de Políticas específicas de Seguridad y Privacidad de la información de la ANI.
- Norma Técnica Colombiana NTC ISO/IEC 27001:2013 Anexo A12.1.2 [1]Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afecten la seguridad de la información.

6. DESCRIPCIÓN DEL TRATAMIENTO DE VULNERABILIDADES

El tratamiento de vulnerabilidades abarca una serie de actividades agrupadas en 4 principales etapas:

- **Planear el tratamiento de vulnerabilidades:** Elaborar el plan de recursos, logística y responsables alrededor de las actividades a realizar.
- **Disponer del Inventario de activos y clasificación**: identificar claramente el inventario que puede ser objeto de vulnerabilidades.
- **Ejecutar las pruebas de vulnerabilidad:** involucra escaneos y agentes autenticados, proporciona riqueza de datos sobre vulnerabilidades.

[1] http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

- **Analizar las vulnerabilidades y reportes:** ante un gran hallazgo de vulnerabilidades, será necesario definir cuáles son las primeras que deben repararse y centrarse en los activos con mayor probabilidad de ser explorados.
- **Remediar (Acciones Preventivas/Correctivas)**: Una vez identificados y priorizados los hallazgos se ejecuta el plan de acción que mitigará o eliminará las vulnerabilidades.

Las actividades antes mencionadas consisten en procesos cíclicos, debido a que la tecnología y las amenazas nunca dejan de evolucionar y cada vez más se generan nuevos riesgos para las organizaciones; por tanto, en la ANI se realizarán de acuerdo con la planeación que se proyecte periódicamente o las necesidades identificadas durante el cumplimiento de las funciones de administración de la infraestructura tecnológica de la Agencia.

6.1. PLANEAR EL TRATAMIENTO DE VULNERABILIDADES

En esta etapa se establecen los requerimientos, actividades, prioridades del tratamiento de vulnerabilidades. El objetivo es identificar todos los requerimientos del análisis y definir el alcance teniendo en cuenta aspectos como:

- Las ubicaciones desde donde se ejecutarán las pruebas.
- Cantidad de áreas, numero de dispositivos por cada área y tecnologías empleadas.
- Tipo de pruebas que se ejecutaran (Escaneos con credenciales, pruebas de penetración caja negra, caja gris o caja blanca).
- Las solicitudes explicitas de escaneo de vulnerabilidades (solicitud del área responsable, cumplimientos regulatorios, solicitudes de auditoría, apoyo a proyectos previo a su puesta en producción, etc.)
- Resultados de análisis de vulnerabilidades o pruebas de penetración realizados con anterioridad.
- Validar con cada uno de los administradores de los sistemas el alcance del análisis y de las pruebas de vulnerabilidad con el fin de determinar los tiempos de ejecución, horarios, recursos, restricciones, requisitos o cualquier tema relacionado con la disponibilidad o criticidad de los dispositivos seleccionados.
- Identificar la herramienta que se empleará para la realización de las pruebas, esta debe ser una herramienta específica para la detección de vulnerabilidades, pueden ser tanto de software para correr sobre sistemas operativos tradicionales o poseer un hardware especifico (appliances). Se recomienda la utilización de Nessus[2], Acunetix[3] y Kali Linux[4]. A nivel de Hardware, los principales fabricantes que comercializan este tipo de tecnología son: Fortinet , Astaro, Symantec , McAfee , Panda Security .

[2] https://www.seaq.co/nessus.html
[3] https://www.north-networks.com/acunetix/
[4] https://es.wikipedia.org/wiki/Kali_Linux

El resultado de esta actividad es el plan de implementación de alto nivel, que se irá actualizando de acuerdo con el resultado del inventario de activos y análisis de vulnerabilidades que se realizan posteriormente.

6.2. DISPONER DEL INVENTARIO DE ACTIVOS Y CLASIFICACIÓN

Esta etapa está enfocada en la protección total de los recursos (redes, aplicaciones, dispositivos móviles) que estén dispuestos a un posible ataque por parte de personas internas o externas a la entidad.

Se debe identificar cada uno de los dispositivos de hardware o software residentes en la infraestructura que soportan los procesos del negocio; para tal fin, debe iniciarse con el inventario de los servicios prestados, continuar con la relación de los procesos asociados a estos servicios y de allí, determinar el listado de los activos o dispositivos que soportan estos procesos.

La lista de Equipos, aplicativos y App_server Azure es reserva de la entidad y está administrada por del G.I.T. Tecnologías de la Información y las Telecomunicaciones.

Se debe contar con inventario base permanentemente actualizado y una relación completa de la infraestructura y artefactos tecnológicos que son la base para el análisis y el tratamiento de las vulnerabilidades.

En las actividades antes mencionadas es importante revisar que no se haya descartado ningún componente del inventario. Los elementos de la infraestructura más sensibles y potencialmente más expuestos que pudieran albergar vulnerabilidades son:

- Servidores
- Aplicaciones (Orfeo, Pagina Web, Aniscopio entre otras)
- Estaciones de trabajo
- Bases de datos
- Firewalls
- Enrutadores
- Switches

6.3. EJECUTAR LAS PRUEBAS DE VULNERABILIDAD

En esta etapa se preparan los detalles puntuales para realizar la prueba, se realiza la prueba, se analizan los resultados de esta y se finaliza con un análisis y entrega de reportes técnicos de la ejecución de la prueba, a continuación, se desagregan:

6.3.1. Aspectos de negocio a considerar para las pruebas

Antes de iniciar las pruebas se deben considerar aspectos a nivel de detalle tales como:

- Fecha y hora adecuada de pruebas
  - Horas de bajo tráfico de red
  - Preferiblemente horarios de no prestación de servicios.

- Análisis de riesgo cualitativo sobre la prueba
  - Análisis sobre la no disponibilidad de activos críticos de la prueba
  - Estimar una probabilidad
  - Estimar un impacto

- Medidas de contingencia
  - Definir estrategias de contingencia para activos críticos
  - Involucrar al oficial de seguridad y coordinador o responsable del plan de continuidad de negocio y del plan de recuperación de desastres (si los hay)
  - Realizar respaldos de la información de los activos involucrados
  - Guardar en formato electrónico y físico configuraciones de equipos involucrados

- Monitoreo de los servicios durante las pruebas
  - Tiempos de respuesta excesivos
  - Eventos o incidentes de seguridad

- Informar al responsable o profesionales de la seguridad de la información la realización de las pruebas.

- Monitorear el tráfico de la red
  - Utilización de los segmentos críticos
  - Condiciones de error (CRC, Bad checksum)
  - Utilización de CPU en servidores críticos

- Informar a los dueños de los activos.

- Verificar si las medidas adoptadas han disminuido la exposición y el nivel de riesgo.

6.3.2. Aspectos técnicos a considerar para las pruebas.

- Hacer análisis de los posibles riesgos al nivel de negocios, identificar las amenazas y las vulnerabilidades tanto físicas como lógicas.
- Revisar configuración de los sistemas operativos, las aplicaciones misionales, archivos de registros y los dispositivos que hacen parte de la arquitectura de red.
- Autentificación de los usuarios y controlar sus accesos. Monitorear las actividades de los usuarios.
- Utilizar scripts propias, revisión de códigos, pruebas de vulnerabilidad manual, herramientas propietarias, comerciales y de código abierto para hacer evaluación de la

vulnerabilidad de la aplicación y de base de datos, de la red, equipos de la red y dispositivos móviles.
- Hacer pruebas de caja negra y caja blanca para encontrar los agujeros de seguridad.

6.3.3. Pruebas

Se debe iniciar la clasificación de activos o dispositivos con base en la confidencialidad de la información que guardan y la importancia del activo para la continuidad del proceso.

Luego se debe identificar la base de datos de vulnerabilidades aceptadas por la industria (CERT, SANS) la más actualizada y completa a la fecha de realización del análisis y con un criterio común de clasificación como el CVE (common vulnerabilities and exposure). Se busca por medio del uso de esta práctica poder identificar cualquier elemento activo presente en la red, siempre y cuando posea una dirección IP, con el fin de detectar sus vulnerabilidades presentes a nivel de software y evitar futuros incidentes de seguridad.

Posteriormente se debe crear un esquema de priorización teniendo en cuenta los impactos sobre la continuidad del servicio agrupando los servidores o estaciones de trabajo, siempre y cuando se cuente con la certeza que aquellos seleccionados para esta agrupación, comparten más de un 90% de similitud en su configuración con los otros que no serán inspeccionados. Si no se tiene esta certeza, necesariamente se debe aumentar el universo de la prueba, hasta que este universo comprenda al menos un elemento de todas las categorías de activos críticos para la operación continua y segura de los procesos.

A continuación, se deben seleccionar la(s) aplicaciones y artefactos tecnológicos que, por su sensibilidad e impacto pudieran tener una consecuencia negativa para la entidad en caso de que pudiese materializarse una vulnerabilidad.

Finalmente, en esta etapa se realizan análisis de los datos, redes, aplicaciones, bases de datos y dispositivos móviles con servicios de escaneo de vulnerabilidades.

6.3.4. Análisis y reportes

Basado en los resultados de las diferentes herramientas utilizadas sobre las pruebas y/o la extracción de información obtenida de las mismas, se deben desarrollar informes tanto técnicos como ejecutivos teniendo en cuenta aspectos definidos en el plan de trabajo y aspectos como los descritos a continuación:

- Se debe analizar cada uno de los resultados teniendo en cuenta los activos de información y el nivel de criticidad establecidos por la ANI.
- Se debe realizar análisis y validación de resultados con el objetivo de identificar falsos positivos; este ítem aplica exclusivamente sobre el análisis de vulnerabilidades debido a que las pruebas de penetración garantizan la confirmación de la vulnerabilidad.
- Realizar comparaciones con los análisis anteriormente realizados.

- Se deben organizar las vulnerabilidades de acuerdo con su nivel de criticidad conforme a la escala mostrada a continuación y el impacto para el negocio de lo cual se obtiene la priorización de las vulnerabilidades más críticas:
  - **Urgente (5):** Intrusos pueden fácilmente obtener el control de un dispositivo lo cual puede conducir al compromiso de toda la red de seguridad.
  - **Crítico (4):** Los intrusos pueden posiblemente obtener el control del dispositivo o estos posiblemente pueden tener fugas de información altamente sensible.
  - **Serio (3):** Los intrusos pueden tener acceso a información específica almacenada sobre el dispositivo, incluyendo configuraciones de seguridad. Esto puede resultar en el aprovechamiento de esta falencia por parte de un atacante.
  - **Medio (2):** Los intrusos pueden ser capaces de recolectar información sensible desde un dispositivo como por ejemplo la versión específica de un software instalado posibilitando la explotación de vulnerabilidades conocidas de este software.
  - **Mínimo (1):** Los intrusos pueden reunir información acerca de puertos abiertos y servicios y puede ser capaz con esta información de buscar otras vulnerabilidades.
- Realizar recomendaciones y elaborar informes para cada uno de los grupos o seccionales identificadas en el plan de trabajo.
- Realizar presentaciones y entrega de informes con las partes interesadas.

6.4. REMEDIACIÓN

En esta etapa se debe proponer las acciones de remediación específicas para las vulnerabilidades, las cuales podrían ser parte del plan de tratamiento general de riesgos, una vez claro está, se haya hecho un análisis formal y detallado de los resultados obtenidos tanto de las pruebas de vulnerabilidades como de las de explotación.

Estas acciones de remediación deben ser documentadas en donde se clasifica (con ayuda de la herramienta de vulnerabilidades y de explotación) la criticidad de cada una de las vulnerabilidades encontradas y se sugiere cuáles deben ser solucionadas en el corto, mediano o largo plazo. Esta decisión conlleva a definir actividades de control respectivo a las vulnerabilidades analizadas también debe contemplar costo del control, capacidad, administración y facilidad de implementación.

Cada uno de los administradores de las diferentes plataformas deben entender el informe técnico el cual describe los problemas de seguridad concernientes a la plataforma, y de esa manera ejecutar las actividades de remediación de dichos problemas de seguridad, algunas de esas actividades pueden ser:

- Instalación masiva de parches de seguridad que estén presentes en el informe y que afecten en gran porcentaje a los activos.
- Clasificación y agrupación de los problemas de seguridad a nivel de sistemas operativos, software específico, aplicaciones web, bases de datos etc.
- Top de dispositivos con la mayor cantidad de vulnerabilidades.

- Top de vulnerabilidades más comunes.

Posterior a la selección de la estrategia de remediación se procederá a ejecutar la solución de seguridad, sin embargo, para sistemas que sean críticos para la organización se deben implementar ambientes de prueba.

Estos ambientes de prueba serán instalados en sistemas virtualizados y en ambientes semejantes al de producción de tal forma que las versiones de software instaladas en el ambiente de producción serán las mismas que en el ambiente de pruebas.

En caso de existir incompatibilidad con la implementación de la solución de seguridad se debe informar al área de seguridad de dicha incompatibilidad, el área de riesgos y seguridad deberán tomar la decisión sobre los controles alternativos y deben llegar a un acuerdo sobre el riesgo expuesto, así mismo para futuros análisis, estos casos puntuales deberán ser tenidos en cuenta para las respectivas excepciones sobre las herramientas utilizadas.

6.4.1. Pruebas de validación

Finalizado el plan de remediación y la implementación de los respectivos cambios sobre las plataformas evaluadas, se ejecutarán las pruebas de validación con el objetivo de identificar la correcta implementación de la solución de seguridad o la aparición de nuevas vulnerabilidades.

Sobre la validación se deben tener en cuenta las excepciones de las vulnerabilidades acordadas con el área de seguridad de la información.

La evidencia de las actividades realizadas debe quedar registrada dentro de los soportes del plan de implementación en donde al menos se registre actividades realizadas, resultados de las pruebas y acciones de remediación.

6.5. ANÁLISIS DE RESULTADOS FINALES

Una vez realizadas las pruebas, la remediación y las pruebas de validación, se debe, con base en la información obtenida realizar una reunión técnica para informar de estos resultados y la revisión general de las vulnerabilidades encontradas y la clasificación emitida por la herramienta.

En dicha reunión deben participar:

- El responsable de implementar el tratamiento de vulnerabilidades técnicas
- Los profesionales de la seguridad de la información
- Los dueños de procesos relacionados con el análisis realizado

Los resultados y decisiones de esta reunión deben quedar plasmadas dentro de documentación de las lecciones aprendidas del tratamiento de vulnerabilidades.

6.6. DOCUMENTACION Y LECCIONES APRENDIDAS

Con el fin de conservar un histórico de las vulnerabilidades encontradas, así como las acciones de remediación implementadas y poder contar con un repositorio y base de conocimiento para la ANI, se deben documentar todas las actividades realizadas y las lecciones aprendidas de cada etapa descrita en el presente instructivo, dicha documentación se alojará en medio digital en el repositorio del G.I.T. Tecnologías de la información y las Telecomunicaciones de la ANI.

Algunos ejemplos de lecciones aprendidas de incidentes de SI
Requisitos nuevos o modificados para los controles de seguridad de la información técnicos o de otro tipo.
Información nueva o modificada sobre vulnerabilidades y/o amenazas, en consecuencia, cambios en la valoración de los riesgos de la Entidad.
Aplicación de medidas de corrección efectivas.

Algunos ejemplos de decisiones a partir de lecciones aprendidas
Actualizaciones rápidas de configuraciones de componentes de Hardware y/o software.
Entrega de instrucciones asociadas a la toma de conciencia sobre la seguridad de la información

7. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
001	15/04/2020	Creación del instructivo

8. APROBACIÓN

	Nombre	Cargo	Fecha	Firma
Elaboró	Guillermo Cadena Ronderos	Contratista	15/04/2020	Aprobado mediante memorando radicado No. 20206070055883
Revisó	Erika Díaz Abella	Contratista	15/04/2020	
Aprobó	Andrés Francisco Boada	Coordinador G.I.T. Tecnologías de la información y las Telecomunicaciones	15/04/2020	
Vo.Bo. SIG	Daniela Mendoza	Contratista	15/04/2020	