Gestión de Vulnerabilidades de TI

Proceso

Gestión de Servicios de Información y Soporte Tecnológico Tecnológico

Versión 1

12/09/2024

TABLA DE CONTENIDO

INTRODUCCIÓN

El Ministerio de Ambiente y Desarrollo Sostenible, en el proceso de implementación de los lineamientos de la Política de Gobierno y Seguridad Digital continúa haciendo esfuerzos para garantizar la prestación de los servicios al ciudadano, a otras entidades y sectores y mediante los procesos de mejora continua se proponen nuevos retos para lograrlo.

El propósito de este documento es establecer un marco claro y efectivo para la gestión de vulnerabilidades dentro de la organización. La gestión de vulnerabilidades es un proceso crítico que involucra la identificación, evaluación y mitigación de las debilidades de seguridad que podrían ser explotadas por amenazas internas o externas. Este documento define las políticas, procedimientos y responsabilidades necesarios para proteger los activos de información y garantizar la continuidad operativa.

OBJETIVO

El objetivo de este documento es proporcionar directrices detalladas para la identificación, evaluación y tratamiento de las vulnerabilidades de seguridad en los sistemas de información de la organización. Se busca minimizar el riesgo de incidentes de seguridad mediante la implementación de medidas preventivas y correctivas.

ALCANCE

Este documento se aplica a todos los sistemas de información, aplicaciones, redes y dispositivos bajo la gestión de la organización. Incluye tanto los activos tecnológicos como los procesos y políticas relacionados con la seguridad de la información.

ROLES Y RESPONSABILIDADES

Los principales roles y responsabilidades asociadas al procedimiento de **P-A-GTI-11** Gestión de la Operación de servicios tecnológicos - 5.5.11 Análisis Periódico de Vulnerabilidades

- **Profesional de Seguridad OTIC**: Es el responsable de la ejecución del procedimiento para la gestión de vulnerabilidades técnicas, sobre los sistemas de información y equipos informáticos del ministerio. Así mismo, es responsable de presentar anualmente el informe de resultados y llevar el seguimiento sobre los planes de remediación. Por último, también es responsable de definir el alcance para ejecutar el procedimiento de gestión de vulnerabilidades técnicas, sobre los sistemas de información e infraestructura del ministerio.

- **Jefe OTIC**: Es notificado y toma las decisiones ante vulnerabilidades que no pueden ser

remediadas y de las cuales se requiere aceptar el riesgo asociado.

- **Líder Técnico del Activo**: Es responsable del Plan de Remediación, de su implementación y de justificar cuando se asume el riesgo.

MARCO LEGAL Y NORMATIVIDAD

- Decreto 338 de 2022 - Se formaliza la Definición y el alcance de los Equipos de respuesta a Incidentes Cibernéticos.
- Directiva Presidencial 03 del 15 de marzo de 2021, respecto a lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Resolución 500 del 10 de 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.
- Decreto 612 de 2018: Artículo 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Artículo12. Plan de Seguridad y Privacidad de la Información (...)
- NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información
- NTC-ISO/IEC 27001:2015 Código prácticas para la Gestión de Seguridad en la Información.
- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información: Ministerio de Tecnologías de la Información y Comunicaciones de Colombia.

INTEGRACIÓN CON OTROS PROCEDIMIENTOS

- **P-A-GTI-11** "Gestionar la operación de servicios tecnológicos en la etapa – 5.12 Gestión de cambios": La remedición de vulnerabilidades puede requerir realizar cambios tecnológicos en el ambiente productivo y la etapa 5.4. Gestión de incidentes de seguridad y privacidad de la información. cuando una vulnerabilidad es explotada el evento será crítico y posiblemente se presente una caída del servicio, en este caso el evento se debe convertir a un incidente.

GESTIÓN DE LAS VULNERABILIDADES

La gestión de vulnerabilidades es un proceso esencial para la seguridad informática, el cual consiste en la planificación del análisis de vulnerabilidades, la ejecución de dicho análisis, y la implementación de un plan de remediación. Además, incluye la realización de pruebas de verificación posteriores para asegurar que las debilidades o fallos detectados, que podrían afectar a los sistemas, redes o aplicaciones, hayan sido efectivamente resueltos. Este proceso no solo ayuda a identificar y corregir

las vulnerabilidades, sino que también contribuye a la prevención de incidentes de seguridad, fortaleciendo así la postura defensiva de una organización frente a las amenazas cibernéticas.
Para atender las vulnerabilidades, MinAmbiente estableció el **P-A-GTI-11** Procedimiento Gestión de la operación de servicios tecnológicos etapa 5.11 Análisis Periódico de Vulnerabilidades que incluye la ruta a seguir en cuanto a las actividades que se deben seguir.

CLASIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades identificadas se clasifican según su criticidad en; críticas, altas, medias y bajas, basándose en el impacto potencial y la probabilidad de explotación. Esta clasificación ayuda a priorizar las acciones de mitigación.

- **Críticas:** este tipo de vulnerabilidades suelen permitir un compromiso total en la integridad y confidencialidades de los datos, por lo que es importante establecer medidas correctivas de inmediato.
- **Altas:** este tipo de vulnerabilidades suelen suponer un riesgo elevado para la integridad y confidencialidad de los datos, por lo que es importante establecer medidas correctivas de inmediato.
- **Medias:** este tipo de vulnerabilidades suelen suponer un riesgo para la integridad o la confidencialidad de los datos
- **Bajas:** este tipo de vulnerabilidades suelen suponer, en situaciones determinadas, un riesgo para la integridad o la confidencialidad de los datos.

METODOLOGÍA

Etapa - Planificar el Análisis de Vulnerabilidades

Esta fase se compone de tres componentes principales, los cuales permiten la correcta ejecución de análisis de vulnerabilidades:

El profesional de seguridad debe diseñar el plan de trabajo para la ejecución del escaneo de vulnerabilidades, el líder técnico del activo debe ejecutar el plan de remedición y re-test, el cual incluya, objetivos, alcance, metodología, el listado de elementos de la infraestructura tecnológica, cronograma de actividades, fecha de re-test, responsables, riesgos y acciones de mitigación a implementar.

- Definir el alcance: se refiere a definir concretamente los objetivos (hosts) a analizar, en el cual está especificado que se entrega un inventario de elementos y credenciales, donde están identificados objetivos críticos con una dirección IP específica, rangos de red, nombres de dominio, entre otros.
  Los activos seleccionados a ser analizados en cada una de las fases están basados en su criticidad y deben estar incluidos en la línea base de la operación del ministerio y alojados en

el data center principal.
Es importante aclarar que si existen objetivos con proveedores de servicios en la nube (*Cloud*) o fuera de la data center principal, estos **no** entran dentro del alcance del análisis de vulnerabilidades.

- Línea de tiempo: En este componente se define la periodicidad en la cual se ejecutará los análisis en la herramienta, es decir la frecuencia de ejecución.

- Objetivo de orientación: Se debe definir la herramienta necesaria para el análisis a ejecutar.

Etapa - Ejecutar el Análisis de Vulnerabilidades e Implementar Plan de Remediación.

El profesional de seguridad OTIC informa al Administrador de la herramienta de análisis de vulnerabilidades sobre el escaneo según lo establecido en el plan de trabajo aprobado por el Jefe OTIC.

El Administrador de la herramienta de análisis de vulnerabilidades inicia el escaneo de vulnerabilidades los resultados arrojados por las herramientas son puntualizados y clasificados de acuerdo con el informe que arroja la herramienta de vulnerabilidades Tenable IO.

Una vez finalizado el escaneo de vulnerabilidades, se organizan los resultados emitidos por las herramientas, incluyendo: lista de las vulnerabilidades según el nivel de criticidad, asociar los elementos afectados, CVE, sistema de información asociado, descartar falsos positivos. Lo anterior es materia prima para el diligenciamiento del **F-A-GTI-11** Registro de pruebas y remediación de vulnerabilidades técnicas

Cuando se realice un VAS se requiere:

- Evaluar los sistemas desde una perspectiva externa.
  Ej. desde Internet, así como desde una perspectiva interna, asumiendo que el diseño del sistema diferencia entre estas dos ubicaciones.

- Supervisar las cuentas utilizadas para ejecutar análisis de evaluación de vulnerabilidades en busca de cualquier actividad inusual. Cuando no se esté realizando una evaluación, hay que considerar deshabilitar la cuenta o cambiar las credenciales asociadas a ella.

- Realizar escaneos de las redes, además de escaneos específicos de sistemas conocidos, con el objetivo de descubrir dispositivos potencialmente desconocidos o no autorizados.

Tener en cuenta que un VAS puede provocar resultados inesperados, que pueden incluir la corrupción de datos.

Ejecutar el VAS con las credenciales (típicamente usuario y contraseña) necesarias para realizar una evaluación en el host (computadora, servidor o sistema) no simplemente un escaneo no autenticado (sin credenciales).

Es importante aclarar que:

- El resultado del análisis de vulnerabilidades se tomará y analizará en primera instancia para identificar y eliminar "falsos positivos", dejando únicamente las vulnerabilidades que efectivamente se encuentran en los elementos de la infraestructura tecnológica analizada.

- Se analizarán las vulnerabilidades con criticidades críticas y altas para de esta forma identificar y recomendar un mecanismo de:

    - Asumir
    - Mitigar o Corregir

Con los resultados del escaneo de vulnerabilidades técnicas arrojados por la herramienta Tenable IO, el Líder Técnico del Activo debe generar el plan de remedición, teniendo en cuenta la clasificación **(Crítico, Alto, Medio o Bajo)** presentada y socializada en el informe **F-A-GTI-11** Registro de pruebas y remediación de vulnerabilidades técnicas, dando prioridad a las vulnerabilidades de nivel crítico y alto, así como a aquellos elementos de la infraestructura tecnológica que soporten aplicaciones críticas.

El Plan de remediación debe gestionar las acciones definidas. En caso de identificar incidencias o requerimientos asociados a la vulnerabilidad se debe realizar la solicitud por medio de la plataforma de gestión y mesa de asistencia (GEMA).
Si se identifican necesidades de cambios asociados al plan de remediación se debe realizar la solicitud conforme al procedimiento **P-A-GTI-11** Gestionar la operación de servicios tecnológicos en la etapa-5.12 Gestión de cambios.

El Profesional de Seguridad OTIC debe socializar a los interesados el informe del resultado del análisis de vulnerabilidades una vez implementado el plan de remediación, con el fin de analizar las acciones a tomar.

- Mitigar o Corregir
- Asumir

Las vulnerabilidades por **Mitigar o corregir** son aquellas para las cuales es necesario aplicar un parche, una reconfiguración o una mitigación. Se debe dar prioridad a estas correcciones y otorgarles una fecha en la cual se implementarán.

Las vulnerabilidades por **Asumir** Si la vulnerabilidad no se puede remediar se deberá Justificar la razón por la cual se asume el riesgo en el plan de remediación, con el fin de documentar la decisión tomada en caso de que la vulnerabilidad vuelva a aparecer.

Etapa - Re-tes de Vulnerabilidades

Informar al administrador de la herramienta

Según lo previsto en el plan de trabajo aprobado, el administrador de la herramienta de análisis de vulnerabilidades solicita autorización al profesional de seguridad OTIC para ejecutar el re-test, cuyo alcance busca comprobar si las vulnerabilidades fueron subsanadas, según el plan de remediación y procede a ejecutar el re-test para evidenciar si la vulnerabilidad se mitigó.

Analizar informe de vulnerabilidades y generar acta

Se debe analizar que las vulnerabilidades fueron subsanadas según lo programado en el plan de remedición. De encontrarse que las vulnerabilidades persisten o que se encontraron nuevas vulnerabilidades, el profesional de seguridad OTIC actualiza el informe de vulnerabilidades y actualizar el formato **F-A-GTI-11** Registro de pruebas y remediación de vulnerabilidades técnicas.

Socializar informe Re-test a interesados

El profesional de Seguridad OTIC socializa el informe del Re-test a interesados y el comparativo de la gestión realizada en el cierre de las vulnerabilidades.

TÉRMINOS Y DEFINICIONES

Escaneo de vulnerabilidades: Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.
Impacto: Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza.

Parche de seguridad: Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.

Re-test PRUEBA de FIABILIDAD que consiste en aplicar una misma prueba en dos momentos distintos.

Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.