UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

GESTIÓN DE VULNERABILIDADES

BOGOTÁ D.C. MARZO 2023

USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

TABLA DE CONTENIDO

1. PROCESO

Gestión de Tecnologías de la Información.

2. OBJETIVO

Identificar y mitigar brechas de seguridad a que están expuestos los activos que componen la plataforma tecnológica de la Entidad, a través del análisis y gestión de vulnerabilidades, con el fin de proteger la confidencialidad, integridad y disponibilidad de información institucional.

3. ALCANCE

Aplica para todos los ejercicios de análisis de vulnerabilidades realizados en la Entidad bien sea externos o internos.

4. DEFINICIONES

- **ANÁLISIS DE VULNERABILIDADES:** consiste en definir, identificar, clasificar y priorizar las debilidades de las aplicaciones para proporcionar una evaluación de las amenazas previsibles y reaccionar de manera apropiada.[1]

- **CIBERSEGURIDAD:** es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.[2]

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

- **RESPONSABLE DEL ACTIVO:** Director o Jefe encargado de gestionar las acciones necesarias para proteger los activos de información de la dependencia a la que pertenece.

- **SIEM:** Security Information Event Manager. Es una solución de seguridad que permite detectar y analizar amenazas y responder a ellas antes de que afecten a las operaciones del negocio.

5. DISPOSICIONES GENERALES

Una medida para asegurar la plataforma tecnológica es llevar a cabo una adecuada gestión de vulnerabilidades, con el fin de identificar brechas de seguridad que puedan ser usadas por agentes maliciosos con el propósito de afectar de alguna forma los activos de información de la entidad.

Esta gestión implica realizar periódicamente un escaneo controlado a la red, así como la ejecución de pruebas de penetración especialmente de aquellos activos catalogados como críticos. Así mismo, es necesario generar planes de remediación que permitan mitigar las vulnerabilidades detectadas.

[1] https://saynet.com.mx/que-es-un-analisis-de-vulnerabilidades/

[2] https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

De igual forma, el responsable del activo es el encargado de atender y gestionar, en los términos indicados, todos los requerimientos que se deriven de la identificación de vulnerabilidades técnicas relacionadas con la infraestructura tecnológica, bienes y/o de servicios de TI, y la correspondiente gestión del plan de tratamiento que se estructure.

Es obligatorio cumplir con las mesas de trabajo que se programen asociadas con la valoración de riesgos, la estructuración de ejercicios controlados para identificar amenazas y vulnerabilidades, y las acciones de mitigación. Es responsabilidad de los administradores de la infraestructura tecnológica y los responsables de los activos atender con la oportunidad que se requiera cada uno de los aspectos enmarcados en esta gestión.

6. CONTENIDO

6.1 IDENTIFICAR ACTIVOS

Para llevar a cabo esta gestión se hace necesario mantener los inventarios de activos, de tal manera que se cuente con un registro actualizado de los componentes de la plataforma tecnológica, los bienes y servicios de TI con que cuenta la Entidad.

6.2 PLANIFICAR EL ANÁLISIS DE VULNERABILIDADES

La planificación de este análisis se realiza a través de las siguientes actividades:

- Anualmente la Oficina de Tecnología realiza la gestión para llevar a cabo un análisis de vulnerabilidades, coordinada a través de un tercero. Durante la fase inicial del desarrollo del proceso de contratación, se identifican cuáles son los activos de mayor criticidad que serán foco de la ejecución de los análisis requeridos.

- En la estructuración de los anexos técnicos relacionados con la adquisición de bienes y servicios tecnológicos, se deben incluir obligaciones contractuales que indiquen que las configuraciones cumplan con la implementación de mejores prácticas tendientes a prevenir vulnerabilidades técnicas, de igual manera los proveedores deben mitigar las vulnerabilidades que se generen sobre los productos y/o servicios a su cargo, una vez se realice el análisis de vulnerabilidades por parte de la Entidad. Si durante la ejecución y/o el periodo de soporte o garantía que se establezca contractualmente, se detectan vulnerabilidades estas deben ser tratadas por el contratista y/o administrador del servicio identificado, para lo cual debe adelantarse un análisis de viabilidad de remediación de manera conjunta con la Oficina de Tecnología.

- La Oficina de Tecnología, tiene a cargo la administración del SIEM, herramienta que se encarga de recopilar datos de registro de eventos de varias fuentes sobre los activos de la Entidad, identificando la actividad que se desvía de los parámetros de seguridad, permitiendo al final responder rápidamente a posibles ataques cibernéticos.

6.3 EJECUTAR EL ANÁLISIS DE VULNERABILIDADES

Teniendo en cuenta los requerimientos contractuales, se procederá con la ejecución de las pruebas de vulnerabilidad sobre aquellos activos previamente establecidos por la OTEC. Los requerimientos para su correcta ejecución se establecen a través del proceso contractual.

En el caso del SIEM, de manera constante se realiza el monitoreo a la herramienta con el fin de identificar posibles amenazas y tomar las medidas a que haya lugar de manera oportuna.

6.4 CLASIFICAR LAS VULNERABILIDADES ENCONTRADAS

Para llevar a cabo esta gestión se debe vincular tanto personal con conocimiento en ciberseguridad, como los administradores de la infraestructura tecnológica y responsables de los activos encargados de su funcionamiento. Aunque las herramientas especializadas generan unos valores de clasificación, es importante que la misma se realice con el personal involucrado, evaluando el impacto que tendría la vulnerabilidad para la operación de la Entidad. Esta clasificación se realiza por niveles en función de su impacto en la operación de la Entidad o probabilidad.

La clasificación de las vulnerabilidades detectadas a través de los ejercicios de seguridad o de inspecciones internas que se realicen a los componentes de la infraestructura tecnológica, se deben registrar en la Matriz de Control y Gestión de Vulnerabilidades. A través de esta gestión se deben establecer las fechas y los responsables de su remediación de acuerdo a su rol frente al activo afectado.

Con el fin de determinar la viabilidad para abordar las gestiones de mitigación de vulnerabilidades en cuanto a esfuerzo, requerimientos técnicos, financieros o de capacidad operativa, es necesario llevar a cabo mesas de trabajo entre el personal encargado de administrar la plataforma tecnológica y el personal especializado del contratista.

Dentro de las opciones de tratamiento de las vulnerabilidades se encuentran las siguientes:

a. **Corregir**: realizar las acciones que no permitan el aprovechamiento de la vulnerabilidad, Ejemplo: aplicar un parche o actualización.

b. **Reconocer:** son aquellas que no requieren una solución inmediata. En este caso es necesario realizar la justificación en la Matriz de Control y Gestión de Vulnerabilidades y adicionar una fecha de revisión con el fin de evaluarla nuevamente.

c. **Investigar**: las vulnerabilidades a investigar deben usarse solo como un estado temporal mientras no puedan ser categorizados como “corregir” o “reconocer”. Esto puede deberse a que se desconoce el costo de resolver el problema o que hay varias soluciones posibles y se requiere más tiempo para identificar cuál funciona mejor. Requiere incluir una fecha de revisión con el fin de evaluarla nuevamente.

d. **Aceptar**: convivir con la vulnerabilidad aceptando el riesgo de materialización, probablemente debido a la imposibilidad de tratamiento.

Posteriormente, se debe realizar una sesión con los responsables de los activos y el personal encargado de la Oficina de Tecnología para determinar y coordinar el tiempo de ejecución estimado (fecha de inicio y fin) de las actividades y gestiones para dar tratamiento a las vulnerabilidades que correspondan. Esta sesión debe integrar en la medida de lo posible a los contratistas o proveedores de servicios tecnológicos involucrados para tener claro el horizonte de las gestiones que se decidan afrontar.

6.5 REMEDIAR

En esta etapa se implementa el plan de mitigación establecido, las acciones se registran en la Matriz de Control y Gestión de Vulnerabilidades y los soportes se almacenan en el recurso compartido establecido por la Oficina de Tecnología. Cada tres meses se realiza el seguimiento a la ejecución del plan con el fin de evaluar el cumplimiento de las actividades propuestas.

Ante las gestiones de tratamiento de vulnerabilidades que impliquen ventanas de mantenimiento, se debe tener en cuenta los protocolos establecidos para dichas actividades a través del procedimiento Control de Cambios TI-PR-013.

6.6 VALIDAR

Una vez ejecutadas las actividades de remediación es necesario realizar actividades de retest con el fin de identificar la efectividad de las acciones de mitigación, de acuerdo al cronograma establecido por la Oficina de Tecnología.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	31/03/2023	Todos	Se crea el documento.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Nombre: Mayra Alexandra Agudelo Carvajal	Nombre: Diana Paola Cárdenas Huertas	Nombre: Imelda Muñoz Mancipe
Cargo: Profesional Especializado	Cargo: Profesional Universitario	Cargo: Jefe Oficina de Tecnología
Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología
	Nombre: Álvaro Camargo Barbosa	
	Cargo: Analista de Sistemas	
	Dependencia: Oficina de Tecnología	
	Nombre: Camilo Alejandro Romero González	
	Cargo: Coordinador de Comunicaciones	
	Dependencia: Oficina de Tecnología	