**GESTIÓN DE VULNERABILIDADES**

|  |  |  |
| --- | --- | --- |
| **REQUISITOS DE LA NORMA:** | ISO 27001-2013: | |
| **ELABORADO POR:**  Fernando Bolívar | **REVISADO POR:**    Carlos Saenz | **APROBADO POR:**  Carlos Saenz |
| **CARGO:** Oficial de Seguridad | **CARGO:**  Coordinador Grupo de Tecnologias de la Informacion y las Radiocomunicaciones | **CARGO:**  Coordinador Grupo de Tecnologias de la Informacion y las Radiocomunicaciones |
| **FECHA:**  28/09/2022 | **FECHA:** | **FECHA:** |

[1.](#_heading=h.2et92p0) OBJETIVO 3

[2.](#_heading=h.tyjcwt) ALCANCE 3

[3.](#_heading=h.3dy6vkm) RELACIONES EXTERNAS 3

[4.](#_heading=h.1t3h5sf) INTERELACION DE PROCEDIMIENTOS 3

[5.](#_heading=h.4d34og8) NORMATIVA APLICABLE 3

[6.](#_heading=h.2s8eyo1) TERMINOS Y DEFINICIONES 4

[7.](#_heading=h.17dp8vu) POLITICAS DE OPERACIÓN 6

[8.](#_heading=h.3rdcrjn) FLUJOGRAMA DE ACTIVIDADES 8

[9.](#_heading=h.26in1rg) PROCEDIMIENTO 8

[10.](#_heading=h.lnxbz9) HERRAMIENTAS 10

# OBJETIVO

Establecer la metodología para la realización de Gestión de Vulnerabilidades a la Plataforma Tecnológica de Parques Nacionales Naturales de Colombia, con el fin de minimizar el riesgo de ataques que puedan comprometer la confidencialidad, integridad y disponibilidad de los sistemas.

# ALCANCE

Este procedimiento aplica para toda la Plataforma Tecnológica de Parques Nacionales Naturales de Colombia, es decir, servidores, equipos de escritorio, portátiles, dispositivos de redes y comunicaciones, bases de datos, aplicaciones web y direcciones IP externas.

# RELACIONES EXTERNAS

* Proveedores de servicios de conectividad
* Proveedores de servicios de plataforma (soporte a infraestructura)
* Clientes

# INTERELACION DE PROCEDIMIENTOS

Procedimiento Gestión Incidentes seguridad de la Información

# NORMATIVA APLICABLE

Norma Técnica Colombiana IEC ISO 27001:2013 Anexo 12

**Ley 1273 de (5 enero 2009)**: Por medio de la cual se modifica el Código Penal. Título VII Bis “De la protección de la información y de los datos”. Artículos 269A a 269J

**Ley 1581 de (17 octubre 2012):** Por la cual se dictan disposiciones generales para la protección de datos personales.

**CONPES 3701 de (14 julio 2018):** Lineamientos de Política para Ciberseguridad y Ciberdefensa.

**CONPES 3854 de (11 abril 2016)**: Política Nacional de Seguridad Digital.

# TERMINOS Y DEFINICIONES

* **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
* **Escaneo de Aplicaciones Web (WAS)**: Es un servicio que ofrece inspección automática y pruebas para las aplicaciones Web personalizadas con el fin de identificar la mayoría de las vulnerabilidades que aparecen en el Top 10 OWASP, y en la clasificación de amenazas WASC, incluyendo “SQL Injection y “Cross Site Scripting”.
* **Infraestructura tecnológica**: Plataformas de cómputo utilizadas para proporcionar servicios de conexión a funcionarios, ciudadanos y proveedores en un ambiente digital (servidores, computadores de escritorio, computadores portátiles, dispositivos de Internet, etc.), servicios de telecomunicaciones que proporcionan conectividad de datos, voz y video y servicios de administración de datos que almacenan y operan datos.
* **OWASP**: Acrónimo de “Open Web Application Security Project” (Guía para proyectos de seguridad de aplicaciones web abiertas). Es una organización sin fines de lucro especializada en mejorar la seguridad del software de aplicación.
* **Ranking de Vulnerabilidades**: Identificación de nuevas vulnerabilidades de seguridad, como la de fuentes externas para la obtención de información y bases de datos de vulnerabilidades.
* **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
* **Sistema de Información**: (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo).
* **Vulnerabilidad**: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.
* **Web Application Security Consortium (WASC)**: Organización formada por un grupo internacional de expertos, profesionales de la industria y representantes de organizaciones que producen software libre y ampliamente acordados estándares de seguridad de mejores prácticas para la Web
* **MITRE**: Es una organización estadounidense sin ánimo de lucro, provee ingeniería de sistemas, investigación y desarrollo, y soporte sobre tecnologías de la información al gobierno de Estados Unidos de América. <https://cve.mitre.org/>
* **CVE**: Vulnerabilidades y exposiciones comunes (en inglés, Common Vulnerabilities and Exposures, siglas CVE), es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID (año + consecutivo), esta lista es mantenida por MITRE.
* **CVSS**: Sistema de puntuación de vulnerabilidad común (en inglés Common Vulnerability Scoring System). Es un framework abierto y universalmente utilizado que establece unas métricas para la comunicación de las características, impacto y severidad de vulnerabilidades que afectan a elementos del entorno de seguridad IT
* **US-CERT**: Sistema Nacional de Concienciación Cibernética, proporciona información actualizada sobre la actividad de seguridad de alto impacto que afecta a la comunidad en general, información oportuna sobre problemas de seguridad, vulnerabilidades y exploits actuales, resúmenes semanales de nuevas vulnerabilidades junto con información de parches y proporciona un análisis en profundidad sobre una ciberamenaza nueva o en evolución.
* **Plugin**: Script o Test que realiza una función específica de Prueba de seguridad.
* Clasificación de vulnerabilidades:
* **Vulnerabilidad Bajas:** Una vulnerabilidad baja son aquellas confirmadas cuyo CVSS esté entre 0.0 y 3.9. Si estas vulnerabilidades no son corregidas antes de 8 semanas se debe indicar con fechas claramente definidas su remediación, la cual no debe sobrepasar las 16 semanas.
* **Vulnerabilidad Medias**: Una vulnerabilidad media son aquellas confirmadas cuyo CVSS esté entre 4.0 y 7.0. Si estas vulnerabilidades no son corregidas antes de 4 semanas se debe indicar con fechas claramente definidas su remediación, la cual no debe sobrepasar las 12 semanas.
* **Vulnerabilidades Altas**: Las vulnerabilidades altas consideradas de alto riesgo (Críticas-Urgentes) son aquellas confirmadas cuyo CVSS sea superior a 7.0. Estas vulnerabilidades deberán remediarse una vez se haya analizado el impacto que se pueda generar en la Plataforma Tecnológica de RSec. Su plazo no debe ser superior a 4 semanas.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

# POLITICAS DE OPERACIÓN

* El Líder Seguridad de la Información y TI, se encuentran suscritos a boletines de seguridad de Col-Cert u otros Boletines de Reporte de Vulnerabilidades con el fin de comunicar las diferentes vulnerabilidades encontradas y realizar seguimiento de las correcciones y aplicación de parches.
* Es responsabilidad del área de seguridad gestionar las vulnerabilidades de las plataformas tecnológicas, y del Líder de Seguridad el monitoreo de las vulnerabilidades en los diferentes componentes del sistema.
* Trimestralmente se debe hacer el análisis de vulnerabilidades a la infraestructura de Parques Nacionales Naturales de Colombia, con el fin de tomar las acciones correctivas en los componentes del sistema, para garantizar que los controles de seguridad se encuentren conformes, se deberá ejecutar un escaneo de vulnerabilidades cuando se presenten cambios significativos en la infraestructura tecnológica de Parques Nacionales Naturales de Colombia, se realizarán pruebas de vulnerabilidades para determinar su estado.
* Se ejecutará escaneo de vulnerabilidades hasta verificar que las vulnerabilidades críticas hayan sido remediadas.
* Se deberá realizar la revisión de código fuente de las aplicaciones provistas para la operación y solicitar al proveedor dicha revisión, el escaneo de vulnerabilidades de aplicación anualmente y después de cada cambio significativo de las aplicaciones.
* Todas las vulnerabilidades que se presenten en la Infraestructura Tecnológica de Parques Nacionales Naturales de Colombia deben ser corregidas mediante un control de cambios. En caso de que una vulnerabilidad se corrija modificando parámetros o archivos en el sistema operativo (y no implique instalar parches), se debe documentar.
* En caso de no poder corregir una vulnerabilidad crítica y alta por motivos de que requiera implementación en un periodo largo, o altos costos no presupuestados, se deberá hacer la valoración del riesgo y determinar un control compensatorio que deberá contener la forma de mitigar o prevenir cualquier amenaza que se pudiera presentar.
* El análisis y la corrección de vulnerabilidades que pueda generar una afectación en los servicios de la Plataforma Tecnológica de Parques Nacionales Naturales de Colombia, debe ser realizada en horarios que no afecte sustancialmente al usuario final.

# FLUJOGRAMA DE ACTIVIDADES



# PROCEDIMIENTO

IDENTIFICAR DISPOSITIVOS Y APLICACIONES WEB

* El área de seguridad identifica y actualiza los elementos de la infraestructura tecnológica (servidores, equipos de escritorio, portátiles, dispositivos de redes, comunicaciones y aplicaciones web e ips externas) a escanear, y los detalla en la herramienta de análisis de vulnerabilidad para ejecutar el escaneo.

EJECUTAR ESCANEO

* El área de seguridad realiza el escaneo de vulnerabilidades a los elementos de la infraestructura tecnológica de Parques Nacionales Naturales de Colombia, con la herramienta destinada para esto

REALIZAR Y REVISAR INFORME

* El área de seguridad realiza y pone a disposición el informe de Vulnerabilidades del trimestre vigente.
* El Líder Seguridad de la Información y TI revisa el informe, verifica que todos los dispositivos se hayan escaneado y analiza la criticidad de las vulnerabilidades encontradas en los diferentes componentes del sistema. Para el análisis de las Aplicaciones Web, se genera un “Informe de Aplicaciones WEB”, este informe aborda todas las vulnerabilidades del TOP 10 de OWASP.

NOTIFICAR REMEDIACIONES

* El Líder Seguridad de la Información y TI entrega el informe del escaneo de vulnerabilidades a los encargados de las plataformas y sistemas de información y solicita el “Plan de corrección de las Vulnerabilidades”.

CORREGIR

* El área de seguridad cumple el “Plan de corrección de las Vulnerabilidades” para la solución, luego de realizadas las tareas de corrección, se debe enviar el informe al Líder Seguridad de la Información y TI para su verificación.
* En el caso de las aplicaciones Web, los encargados de la corrección realizan los ajustes en las aplicaciones Web corrigiendo las vulnerabilidades según la clasificación de las vulnerabilidades y lo regresaran al Líder Seguridad de la Información y TI para la revisión y re-escaneo de la aplicación Web.
* Nota: Antes de corregir las vulnerabilidades se debe realizar un análisis de las posibles incidencias que se puedan generar a la Plataforma Tecnológica de Parques Nacionales Naturales de Colombia, con el fin de tomar acciones preventivas.

REALIZAR SEGUIMIENTO

* El Líder de Seguridad debe realizar seguimiento del “Plan de corrección de Vulnerabilidades” y el área de seguridad realiza el re-escaneo, con el fin de validar que las vulnerabilidades hayan sido corregidas. Este ciclo deberá ejecutarse hasta que hayan sido corregidas todas las vulnerabilidades o se evalué y se apruebe el riesgo residual.
* El Líder Seguridad de la Información y TI recibe del Col-CERT notificaciones de posibles vulnerabilidades que puedan afectar la infraestructura tecnológica de Parques Nacionales Naturales de Colombia y las reportará a los responsables de los componentes del sistema para su revisión, quienes las solucionarán de acuerdo con la clasificación de las vulnerabilidades.

# HERRAMIENTAS

Todas las herramientas automatizadas de Análisis de Vulnerabilidades se basan en Plugins, por lo tanto, es importante siempre tener la base de datos de Plugins actualizada.

Para un análisis adecuado se debe configurar de forma correcta el perfil del análisis de vulnerabilidades de acuerdo con la infraestructura de Parques nacionales Naturales de Colombia, teniendo en cuenta la información de pruebas anteriores.

La experiencia de configuración de la herramienta de acuerdo con el entorno se adquiere con el tiempo cada vez que se realiza un análisis de vulnerabilidades (“Pruebas + Pruebas + Pruebas”)

Las vulnerabilidades se pueden presentar en:

* Hosts: Sistemas Operativos (Windows, Linux, IOS, etc.), Servicios de Red (FTP, HTTP, DNS, NTP, etc.), Aplicaciones (WordPress, Apache, etc.)
* Dispositivos: Router, Switch, Firewall, PLC, IoT, OT
* Personas: Todos tenemos vulnerabilidades

Las herramientas de análisis de vulnerabilidades para Hosts, Aplicaciones y dispositivos más utilizadas son:

* Tenable IO
* NMAP - <https://nmap.org/>

Para las personas no utilizamos como tal una herramienta automatizada de detección de vulnerabilidades, pero si se utiliza otras técnicas que consisten en engañar a los usuarios.

|  |  |  |
| --- | --- | --- |
| **NOVEDADES Y ACTUALIZACIONES** | | |
| **FECHA** | **DESCRIPCIÓN** | **VERSIÓN** |
| 28/09/2022 | Creación del documento | 01 |