



## **Documento de Necesidades para el Análisis de Vulnerabilidad**

### **1. Introducción**

El análisis de vulnerabilidad es un proceso crucial para identificar debilidades y riesgos en los sistemas tecnológicos de una institución, en particular aquellos que almacenan o procesan información sensible. Este documento tiene como propósito detallar las necesidades y los requisitos para llevar a cabo un análisis de vulnerabilidad en los sistemas informáticos y de infraestructura tecnológica del **Hospital Departamental San Vicente de Paul**. La implementación de este análisis ayudará a mitigar posibles amenazas, proteger datos críticos y garantizar la disponibilidad, confidencialidad e integridad de los sistemas.

### **2. Objetivo del Análisis de Vulnerabilidad**

El objetivo principal del análisis de vulnerabilidad es identificar, evaluar y priorizar las debilidades de seguridad en los sistemas de TI de la institución. Este análisis permitirá implementar las medidas correctivas y preventivas adecuadas para reducir los riesgos y mejorar la seguridad general de los sistemas informáticos

### **3. Alcance del Análisis de Vulnerabilidad**

El análisis de vulnerabilidad abarcará los siguientes componentes:

Red de TI:

Infraestructura de red (routers, switches, firewalls).

Servidores internos y externos.

Sistemas de comunicaciones y conectividad.

Sistemas y Aplicaciones:

Aplicaciones web y móviles utilizadas para la gestión de datos de salud.

Sistemas operativos de los servidores y estaciones de trabajo.



Base de datos (relacionales y no relacionales).

Seguridad de la Información:

Configuraciones de seguridad (políticas de contraseñas, accesos no autorizados).

Monitoreo y gestión de incidentes de seguridad.

Políticas de encriptación de datos (en tránsito y en reposo).

Equipos y Hardware:

Estaciones de trabajo (PCs, laptops).

Dispositivos móviles utilizados por el personal.

Hardware de almacenamiento (discos duros, unidades de respaldo).

Manejo de Usuarios y Accesos:

Control de accesos y autenticación.

Administración de privilegios y roles de usuarios.

Auditoría de accesos y uso de recursos.

#### **4. Necesidades para la Realización del Análisis de Vulnerabilidad**

El análisis de vulnerabilidad debe abordar varias áreas clave para garantizar que todas las posibles brechas de seguridad sean identificadas y mitigadas. Las necesidades para llevar a cabo este análisis incluyen:

Herramientas de Escaneo de Vulnerabilidades:

Software de pruebas de penetración para simular ataques y evaluar la robustez de los sistemas.

Personal Especializado:

Contar con un equipo de especialistas en ciberseguridad y análisis de vulnerabilidades.



**EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE  
PAÚL GARZÓN - HUILA**  
NIT: 891.180.026-5

Tener expertos en redes, seguridad de bases de datos, y análisis de riesgos informáticos.

Acceso a Infraestructura Crítica:

Acceso autorizado a la infraestructura tecnológica que será evaluada (servidores, redes, bases de datos, aplicaciones).

Permiso para realizar pruebas en entornos productivos y no productivos (si es necesario).

Revisión de Políticas de Seguridad:

Documentación detallada de las políticas de seguridad existentes.

Evaluación de Riesgos y Cumplimiento Regulatorio:

Asegurar que el análisis de vulnerabilidad cumpla con las normativas de seguridad aplicables, tales como la Ley 1581 de 2012 (Protección de Datos Personales), la Ley 1266 de 2008, o las normativas internacionales como ISO/IEC 27001.

Evaluación de riesgos potenciales que puedan derivarse de vulnerabilidades encontradas y su impacto en la organización.

Planificación de Contingencias y Respuesta ante Incidentes:

Crear un plan de respuesta ante incidentes basado en los resultados del análisis de vulnerabilidades.

Establecer un protocolo para remediar las vulnerabilidades críticas identificadas, así como medidas preventivas a largo plazo.

## **5. Metodología del Análisis de Vulnerabilidad**

Para realizar un análisis de vulnerabilidad efectivo, se recomienda seguir una metodología estructurada que incluye las siguientes etapas:



**EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN VICENTE DE  
PAÚL GARZÓN - HUILA  
NIT: 891.180.026-5**

Reconocimiento y Recolección de Información:

Recopilación de datos sobre la infraestructura, redes y sistemas a evaluar.

Identificación de posibles vectores de ataque.

Escaneo de Vulnerabilidades:

Realización de escaneos automatizados para identificar debilidades conocidas en sistemas y aplicaciones.

Evaluación de configuraciones incorrectas o inseguras en la infraestructura de TI.

Pruebas de Penetración (Pentesting):

Simulación de ataques para evaluar la resistencia de los sistemas a accesos no autorizados.

Análisis de vulnerabilidades explotables y riesgos potenciales.

Análisis de Resultados y Generación de Informe:

Evaluación de los resultados obtenidos de los escaneos y las pruebas.

Elaboración de un informe detallado con las vulnerabilidades identificadas y recomendaciones de mitigación.

Remediación y Plan de Mejora:

Definición de las acciones correctivas necesarias.

Implementación de soluciones y medidas de mitigación de los riesgos identificados.



## **6. Resultados Esperados**

Al concluir el análisis de vulnerabilidad, los resultados esperados incluyen:

Identificación completa de las vulnerabilidades en los sistemas y redes de la institución.

Recomendaciones claras de remediación para corregir las debilidades de seguridad.

Informe detallado con los hallazgos, riesgos asociados, y un plan de acción para mitigar las vulnerabilidades.

Mejora en la postura de seguridad de la institución, reduciendo el riesgo de ciberataques y garantizando la integridad de los datos.

## **7. Conclusión**

Este análisis de vulnerabilidad será una herramienta crucial para mejorar la seguridad de la infraestructura tecnológica del hospital Departamental San Vicente de Paul. A través de la identificación temprana de debilidades y su corrección, se pueden prevenir posibles incidentes de seguridad que afecten la confidencialidad, disponibilidad e integridad de los datos, así como la continuidad de los servicios.

**HECTOR LEANDRO RENDON RUIZ**

**Ing. de Sistemas**

**T.P. 70255-412482 TLM**

Coordinador U.F. Gestión Sistemas de Información  
E.S.E. Hospital Departamental San Vicente de Paul