
	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	<b>Código:</b> MAG-GIT-AS-IF-001
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02	<b>Página No.</b> 1 de 62

# EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 2 de 62

## CONTENIDO

### DEFINICIÓN DEL PROBLEMA

#### 1. JUSTIFICACIÓN

#### 2. OBJETIVO GENERAL

##### 2.1 OBJETIVOS ESPECÍFICOS

#### 3. MARCO REFERENCIAL

- 3.1 ANTECEDENTES
- 3.2 MARCO CONTEXTUAL
- 3.3 MARCO TEORICO
- 3.4 MARCO LEGAL

#### 4. METODOLOGIA

##### 4.1 METODOLOGIA DE LA INVESTIGACIÓN

#### 5. ANÁLISIS DE LA INFORMACIÓN

- 5.1 IDENTIFICACIÓN DE ACTIVOS
- 5.2 IDENTIFICACIÓN DE VULNERABILIADES
- 5.3 ANÁLISIS DE RIESGOS

#### 6. SALVAGUARDAS


##### 6.1 CARACTERIZACIÓN DE LAS SALVAGUARDAS

#### 7. POLÍTICAS Y ESTRATEGIAS

- 7.1 INVENTARIO DE ACTIVOS
- 7.2 PETI, PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN
- 7.3 POLÍTICA DE SEGURIDAD INFORMÁTICA DEL HOSPITAL DEPARTAMENTAL
- 7.4 MANUAL DE USO DE LOS RECURSOS INFORMÁTICOS
- 7.5 MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS
- 7.6 PLAN DE CONTINGENCIA DE FALLOS DEL SISTEMA O PERDIDA DE DATOS

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*


	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 3 de 62

## 8. CONCLUSIONES

- **RECOMENDACIONES**
- **BIBLIOGRAFIA**
- **ANEXOS**

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 4 de 62

## RESUMEN


En el Hospital Departamental San Antonio de Padua, se hace necesario realizar un análisis situacional de la Institución teniendo en cuenta tres pilares fundamentales para la Entidad, como son:

- **INFRAESTRUCTURA TECNOLÓGICA:** Entiéndase por infraestructura tecnológica los componentes de *Hardware, software* y Redes de datos.
- **SISTEMAS DE INFORMACIÓN:** Son las herramientas para el procesamiento de la Información Institucional.
- **SEGURIDAD DE LA INFORMACIÓN:** Proceso orientado a proteger toda la información de una Institución, independiente del modo de creación, procesamiento, almacenamiento, si es física o digital.

Este análisis permitirá proponer la implementación de estrategias para la Gestión de TI (Tecnologías de Información), utilizando marcos de referencia como COBIT, ITIL e ISO 27001, al igual que implementar los lineamientos establecidos por el gobierno "Gobierno Digital", logrando identificar riesgos, vulnerabilidades y amenazas, para establecer los controles necesarios a implementar en la Institución.

***"Hospital Humanizado y Seguro es Nuestro Compromiso"***

*"Documento no valido en medio impreso sin la identificación de Marca de Agua "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital"*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 5 de 62

## INTRODUCCIÓN


El siglo XXI ha sido denominado la nueva era de la información y el conocimiento digital, gracias a la acción transversal de las TI (Tecnologías de Información), los sistemas de Información se pueden aprovechar y desarrollar en diferentes nichos de mercado, optimizando los procesos y tiempos generando las soluciones requeridas para cada sector. Dichos sistemas mejoran la competitividad y desempeña una función clave al permitir la reestructuración y modernización empresarial. La modernización de la industria va de la mano con grandes desafíos institucionales, abriendo las puertas a nuevos mercados, a aumentarla productividad y competitividad, adaptarse a nuevas estrategias de comercialización y sobre todo competir con base en la calidad de los productos y servicios. El sector de las TIC's requiere de un alto nivel de investigación, desarrollo tecnológico y formación de personas capaces de producir soluciones acordes con las necesidades que surgen en la actual coyuntura, necesidades que al ser atendidas eficientemente puede impactar de manera positiva a las organizaciones modernas.

El HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA, conector de estas necesidades está dispuesto a realizar las valoraciones necesarias que permitan apalancar el mejoramiento de su productividad y de su eficiencia corporativa. La información como variable estratégica de la organización, debe estar actualizada soportada en las herramientas necesarias para realizar el análisis estratégico, que le permita a la gerencia tomar decisiones.

En el Hospital Departamental San Antonio de Padua, el proceso de administración de la información dificulta la consolidación de esta, por lo que es necesario en ocasiones utilizar herramientas como hojas de cálculo (Excel) para la integración de datos, adicionalmente los procesos para la gestión de la seguridad de Información son limitados y la infraestructura tecnológica (Redes de datos) es obsoleta en cuanto al tiempo que se realizó las instalaciones.

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 6 de 62

**Palabras clave:** (Amenazas, gestión del riesgo, riesgos, seguridad informática, vulnerabilidades).

## 1. DEFINICIÓN DEL PROBLEMA

Los riesgos informáticos constituyen uno de los factores más preocupantes en seguridad de la información de las Instituciones, por lo tanto, se hace necesario realizar un estudio donde se pueda evidenciar las vulnerabilidades, amenazas y riesgos en el Hospital Departamental San Antonio de Padua y poder establecer como una gestión del riesgo informático contribuye a mejorar la productividad y eficiencia corporativa con el fin de alinearse con los principios estratégicos de la entidad.

Con base en lo anterior se plantea el siguiente interrogante:

¿Cómo el Estudio de vulnerabilidades, amenazas y gestión del Riesgos en el Hospital Departamental San Antonio de Padua, contribuye a mejorar la productividad y eficiencia, alineados con los principios estratégicos?

## 2. JUSTIFICACIÓN

Los riesgos forman parte de la naturaleza del ser humano y están presente en todas sus actividades, más aún cuando la tendencia al uso de la tecnología como factor de desarrollo e innovación, mejora las condiciones de vida minimizando lo que se considera el riesgo asociado al factor humano, pero asumiendo nuevos riesgos derivados de la tecnología y su dependencia.

Es por ello por lo que, de la mano de los avances tecnológicos, vienen también los avances en riesgos informáticos, el auge de nuevas tecnologías lleva al cambio de los procesos

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 7 de 62

empresariales adaptados a estas nuevas herramientas, como son software, sistemas de información y nuevas formas de comunicación.

Adicional el Hospital Departamental San Antonio de Padua, como entidad de salud debe regirse por la normatividad frente al uso y custodia de la Historia Clínica de sus pacientes, garantizando la integridad y el uso adecuado de esta información al considerarse altamente confidencial, el uso de historia clínica sistematizada brinda una gran herramienta para el registro y consolidación de información, pero igualmente genera un factor de riesgo tecnológico a tener en cuenta en la custodia de esta información, igualmente se debe garantizar la confidencialidad, integridad y disponibilidad de toda la información empresarial, comercial y clínica de la Institución.

La tecnología no es ajena a los riesgos y en este escenario es importante identificar los eventos, vulnerabilidades y amenazas que puedan poner en riesgo los activos de información comprometiendo la operación, imagen y credibilidad de la institución. Es por esto por lo que se busca implementar estrategias que puedan mitigar la confidencialidad, integridad y disponibilidad de la información.


### 3. OBJETIVO GENERAL

Realizar un estudio de vulnerabilidades, amenazas y gestión del Riesgo en el Hospital Departamental San Antonio de Padua, para minimizar el impacto provocado por la materialización de riesgos asociados a los activos de información.

#### 3.1 OBJETIVOS ESPECÍFICOS

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 8 de 62

- Identificar los riesgos, amenazas y vulnerabilidades del Hospital Departamental San Antonio de Padua.
- Realizar un estudio de la gestión del Riesgo en el Hospital Departamental San Antonio de Padua.
- Proponer políticas y estrategias que logren mitigar ese riesgo.
- Reducir el impacto de las amenazas
- Implementar y evaluar la gestión de seguridad Informática en la Institución

#### 4. MARCO REFERENCIAL

##### 4.1 ANTECEDENTES

La seguridad informática constituye un marco importante en el alcance de los Objetivos Institucionales, al proteger la integridad, disponibilidad y confidencialidad de los datos del Hospital Departamental San Antonio de Padua, identificar los posibles riesgos y amenazas a los que se puede ver expuesta brinda garantías de protección y mecanismos de prevención.

##### 4.2 MARCO CONTEXTUAL


Dentro de la estructura organizacional el proceso de gestión de la información tiene una incidencia directa en la como se muestra en la siguiente imagen.

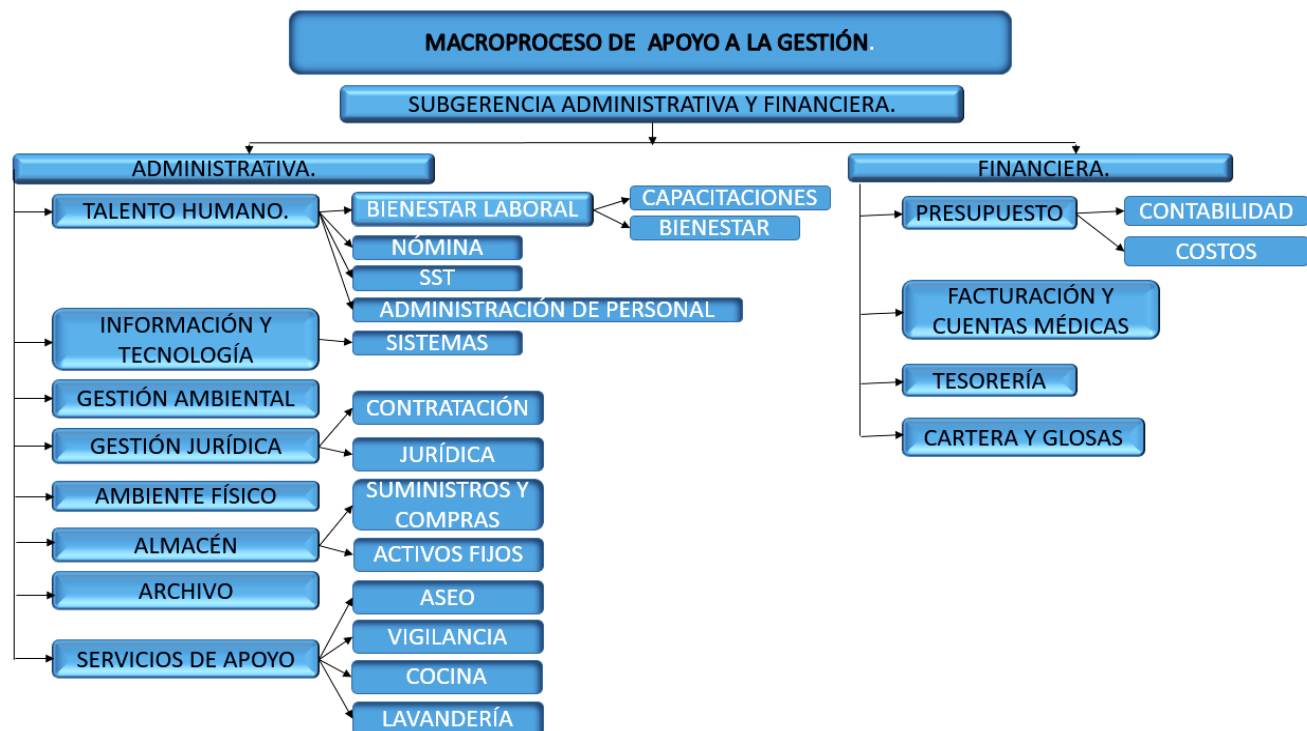
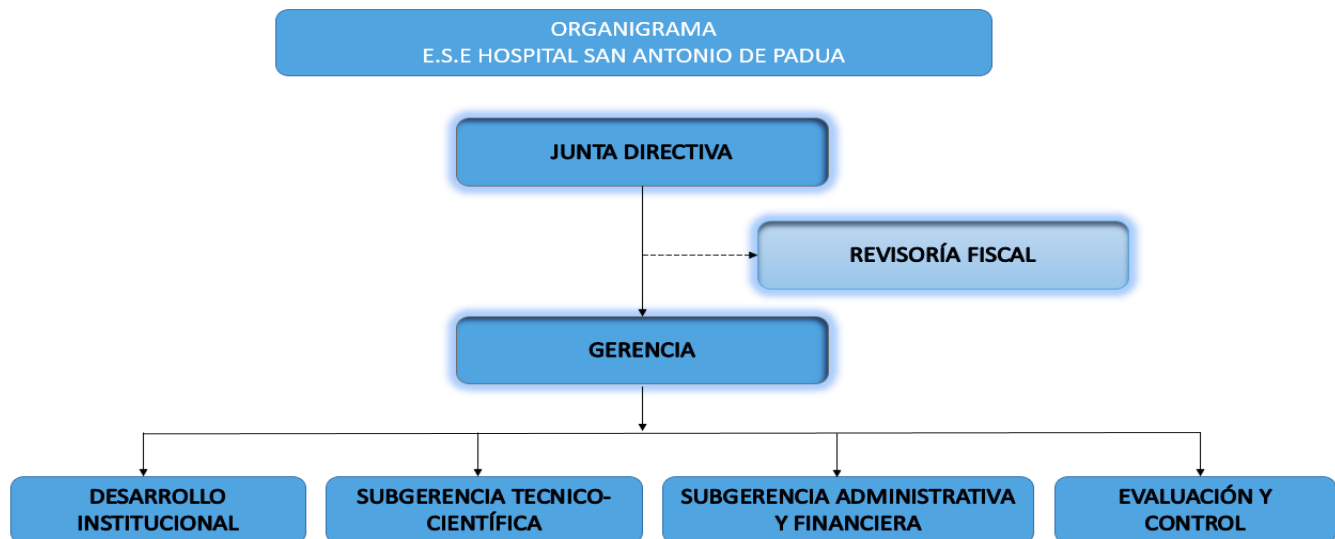
En la figura 1 se observa la estructura organizacional de la entidad, donde se evidencia lo expuesto anteriormente:

Ilustración 1 - Estructura Organizacional

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

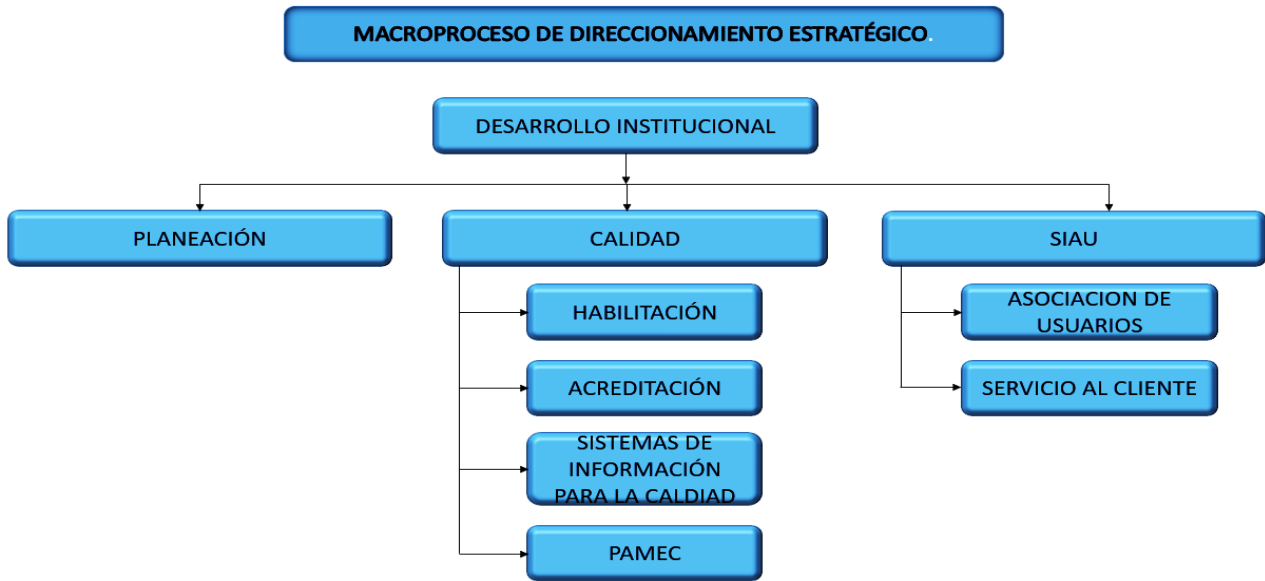
*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	Fecha: 26/04/2024
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	Código: MAG-GIT-AS-IF-001
	<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	Versión: 02
		Página No. 9 de 62




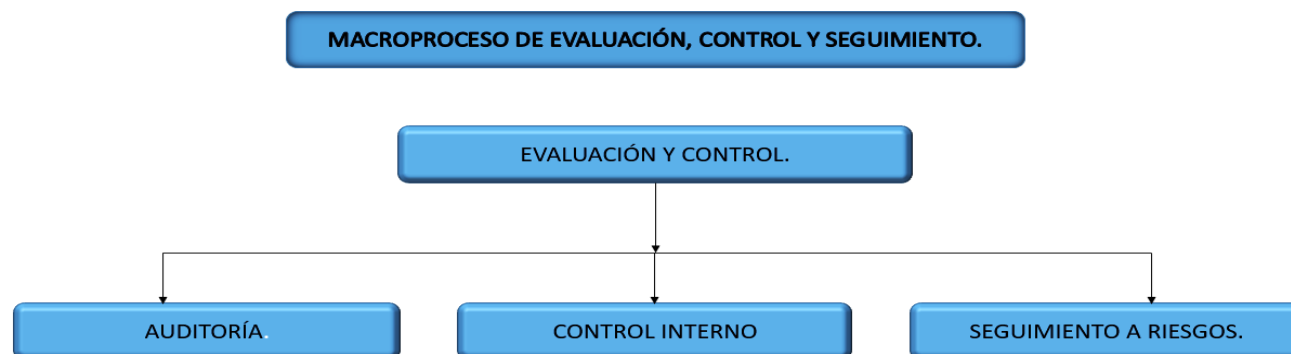
*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”



*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

 <p>E.S.E. Hospital Departamental San Antonio de Padua LA PLATA</p>	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 11 de 62



Fuente: Documento de función pública-Hospital Departamental San Antonio de Padua


La gestión de servicios tecnológicos se encuentra centralizada por el área de sistemas donde se tramitan y se da seguimiento a las solicitudes con usuarios, proveedores y terceros, así como también se hace levantamiento de información de necesidades tecnológicas, las cuales sirven como insumo para la elaboración de los planes anuales de inversión.

Para realizar el proceso de mantenimiento preventivo y correctivo hay una persona autorizada y preparada para realizar el mantenimiento, la cual es supervisada por una persona de planta, que conoce el área de sistema de información.

Se puede decir que se han adelantado algunos procesos de sensibilización y capacitaciones, que tienen en cuenta el componente tecnológico, se hace necesario establecer medidas del impacto cuantitativo y/o cualitativo mediante instrumentos que permitan valorar el nivel de aceptación de la tecnología al interior de la Entidad.

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 12 de 62
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>		

## SISTEMAS DE INFORMACIÓN

De acuerdo con lo dispuesto en el modelo de gestión de TI propuesto por MinTIC los sistemas de información se dividen en: apoyo, misionales y de direccionamiento estratégico. Teniendo en cuenta lo anterior, en el Hospital Departamental San Antonio de Padua se tendría la siguiente categorización:

Sistemas de apoyo:

- Eclipse.
- Gestión Documental

Sistemas Misionales de Gestión


- DINÁMICA GERENCIAL DGH– Asistencial y Administrativo
- Carestream (Imágenes Digitalizadas)

Tabla1. Software Institucional

Servicio	Descripción
<b>Gestión Documental</b>	Se procesa información administrativa y financiera
<b>Dinámica Gerencial</b>	Módulos asistenciales y administrativos como: <ul style="list-style-type: none"> <li>➤ Facturación</li> <li>➤ Inventarios</li> <li>➤ Historia Clínica</li> <li>➤ Contabilidad</li> <li>➤ Activos Fijos</li> <li>➤ Generales</li> <li>➤ Tesorería</li> <li>➤ Presupuesto</li> <li>➤ Nomina</li> <li>➤ Cartera</li> <li>➤ Pagos</li> <li>➤ Compras</li> </ul>

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 13 de 62

	<ul style="list-style-type: none"> <li>➤ Contratos</li> <li>➤ Citas Medicas</li> <li>➤ Hospitalización</li> <li>➤ Admisiones</li> <li>➤ Programación de Cirugías</li> <li>➤ Preauditoria de Cuentas</li> <li>➤ Contratación</li> <li>➤ Gestión Gerencial</li> </ul>
<b>SQL Server 2014</b>	Motor de base de datos administrativo y asistencial
<b>Outlook</b>	Herramienta de correo electrónico
<b>Paquete Office</b>	Paquete de herramientas ofimáticas
<b>Sitio Web</b>	Página web institucional
<b>Gestión de requerimientos TI</b>	Herramienta para gestión de requerimientos de TI

Para la Institución este dominio representa una debilidad dado el número de sistemas de información y en cada uno de ellos se debe brindar un soporte técnico, brindando de manera manual la comunicación entre cada uno de ellos, lo que genera reprocesos administrativos.

#### **Administración de sistemas de información:**

Para la gestión de los sistemas de información en el Hospital Departamental San Antonio de Padua la Entidad cuenta con ambientes de:


- Desarrollo
- Pruebas
- Producción

#### **Ambiente de Desarrollo**

La Institución no realiza procesos de desarrollo, sin embargo, en este ambiente se comprende el entorno de interfaz y conexión de la información entre diferentes aplicativos, herramientas, reportes e informes. A este ambiente, puede acceder solo personal previamente autorizado y

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>		<b>Versión:</b> 02
		<b>Página No.</b> 14 de 62

tienen los privilegios para crear, modificar y eliminar los componentes que componen o compondrán el sistema; se debe restringir los accesos a los usuarios finales o cualquier otro usuario diferente al equipo de desarrollo.

El desarrollo de esta práctica se aplica para los servidores y repositorios de datos.

### **Ambiente de Pruebas:**

Este ambiente es usado para la realización de pruebas del sistema, cada que se desarrolle una nueva función, con el fin de ser probada por los usuarios finales, este es un paso previo a la actualización en ambiente de producción.

Previo a la actualización en ambiente de producción, se debe realizar las validaciones por parte del equipo de *testing* y desarrollo a fin de identificar errores tanto estructurales, funcionales y el manejo de excepciones.

Para la correcta aplicación del entorno de pruebas se debe realizar con casos reales, con el fin de acercarse lo más posible a la realidad a la cual se va a enfrentar el aplicativo, a fin de garantizar el desarrollo y la configuración óptima, además de poder detectar el mayor número de incidentes antes del momento de despliegue en producción.


Se recomienda definir múltiples ambientes de pruebas, para evaluar y determinar el comportamiento de una funcionalidad en diferentes escenarios, este ambiente de pruebas se compone del repositorio de datos reales, datos de pruebas y los componentes a evaluar del software.

### **Ambiente de Producción:**

Este ambiente de producción es donde se despliega las nuevas funcionalidades del software a ejecutar, previa evaluación en el ambiente de pruebas, con un resultado satisfactorio, que se debe formalizar por el representante de la fase y así poder desplegar en producción a fin de ser usadas por los usuarios finales.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 15 de 62

Para realizar el despliegue en producción de los componentes compilados o ejecutables se tomarán las versiones probadas y aceptadas del ambiente de pruebas.

El Grupo de Trabajo de Infraestructura y Servicios de TI, es el responsable de la administración de la aplicación o el sistema en este ambiente.

### Infraestructura:

La infraestructura informática es la base fundamental de todo sistema de información basado en ambiente cliente servidor, por medio de la cual un computador se puede conectar con otro, compartir información y ejecutar aplicativos centralizados desde un servidor de datos. A continuación, se detalla la infraestructura tecnológica dispuesta por el HDSAP y descrita en tres grupos (Servidores, Redes y Telefonía).

### Servidores


Estos componentes se entienden como el hardware y el software que soporta los sistemas de información (misionales y de apoyo), las bases de datos y los servicios de red, los cuales se encuentran distribuidos como servidores físicos, unidades de almacenamiento de información y dispositivos de Backups.

Tabla 2– Servidores

Equipo	Aplicativo	Especificaciones
<b>Servidor HP Prolaint 180 Gen 9</b>	Servicios DG	Procesador Intel Xeon CPU E5-2609 V3 @1.90 GHz Velocidad 1900 MHz Discos Duros 2 Total: 1.2 TB Memoria RAM 16 GIGAS Tipo de BIOS: (12/2014)
<b>Servidor HP Prolaint 180 Gen 9</b>	Servicios DHCP Interfaz de Laboratorio Gestión Documental	Procesador Intel Xeon CPU E5-2609 V3 @1.90 GHz Velocidad 1900 MHz Discos Duros 5 Total: 3 TB Memoria RAM 8 GIGAS Tipo de BIOS: (12/2014)

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 16 de 62

Fuente: Manual de uso de los Recursos Informáticos del HDSAP

## Redes

Actualmente el Hospital cuenta con una infraestructura de red LAN basada en tecnología Ethernet 10/100/1000, interconectada en topología tipo cascada, utilizando cable UTP categoría 5e y 6 y 6e, y en algunas conexiones con categoría 7, bajo la norma estándar IEEE 568b. También se cuenta con una conexión de fibra óptica tipo multimodo, para enlazar áreas del hospital alejadas como las áreas de Hospitalización, Ginecología, Pediatría, Cirugía, Urgencias y UCI. La central de cableado está ubicada en el segundo piso del área administrativa del Hospital, y está administrada por equipos de conmutación de alta velocidad como *Switches* de Red, los cuales están apilados para poder administrar la transmisión de datos de todos los puntos conectados.

La red de datos del Hospital está conformada por 132 equipos de cómputo, configurados con sistema operativo Windows de Microsoft, administrados por un servidor de dominio con sistema operativo Windows 2014 Server, por medio del cual se han establecido políticas de configuración de usuario como son:

Validación de acceso por usuario y contraseña.

- Restricciones de acceso al sistema por usuario.
- Restricciones de acceso a información por usuario.
- Política de restricción de servicios.
- Restricciones de acceso a la red.

Se cuenta con un dispositivo de seguridad perimetral Firewall, IDS, IPS, con el fin de gestionar, detectar, prevenir y filtrar el tráfico entrante y saliente que hay entre las diferentes redes de la entidad. Así mismo de acuerdo con la función que realicen estos equipos, ayudan a fortalecer los controles que permiten preservar la confidencialidad, integridad y disponibilidad de la información.

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*


	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 17 de 62

Tabla 3 - Hardware de Redes

Tipo de Equipo (Hardware)	Cantidad
Switch de red	11
Firewall Físico (SONICWALL)	1

Fuente: Manual de uso de los Recursos Informáticos del HDSAP

**Red de corriente Regulada:** El Hospital cuenta UPS (Sistema de poder ininterrumpido), para brindar sistema de corriente regulado a toda la infraestructura tecnológica.

**Canal Internet:** El Hospital dispone de un canal de Internet dedicado de 50 MB de Ancho de banda el cual está contratado con el operador Servisysten S.A.S. y un canal de respaldo de 10 Megas por radio, con ETB.

**Sitio Web:** El Hospital cuenta con su propio sitio web en internet [www.hospitaldelaplata.gov.co](http://www.hospitaldelaplata.gov.co) como herramienta de comunicación para el usuario, donde se describe su portafolio de servicios, programas, proyectos. A demás de darse a conocer nacional e internacionalmente. La página es administrada por el profesional en sistemas de Hospital quien realizara revisiones con el fin de evaluar solicitudes de los usuarios de esta.

**Telefonía:** El Hospital cuenta con un servidor telefónico análogo y digital, para la administración de un primario de 15 líneas, adicional mente se cuenta con línea directas para los servicios de citas médicas, referencia y contra referencia y otras dependencias.

### ESQUEMA FISICO DE LA RED INTERNA

En la siguiente ilustración se muestra la infraestructura de red física de la Entidad:

Ilustración 1–Esquema físico de Red de Administración

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

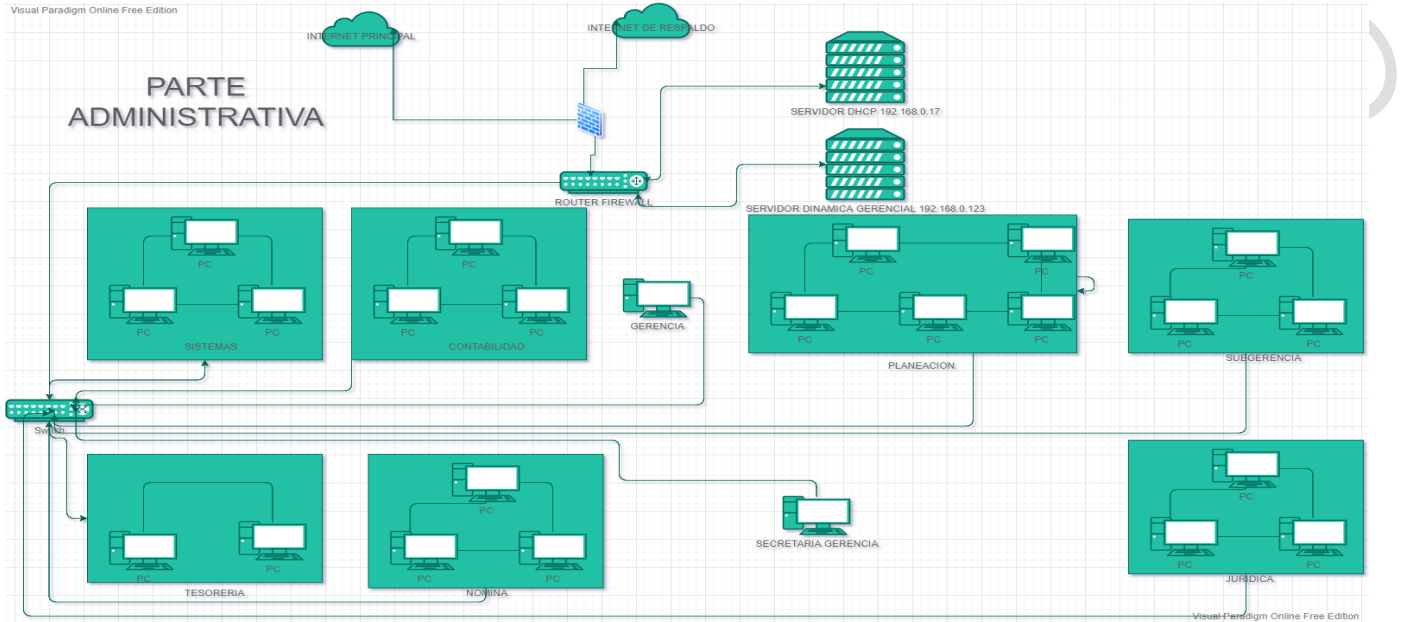


Ilustración 2–Esquema físico de Red de Consulta Externa-Primer piso

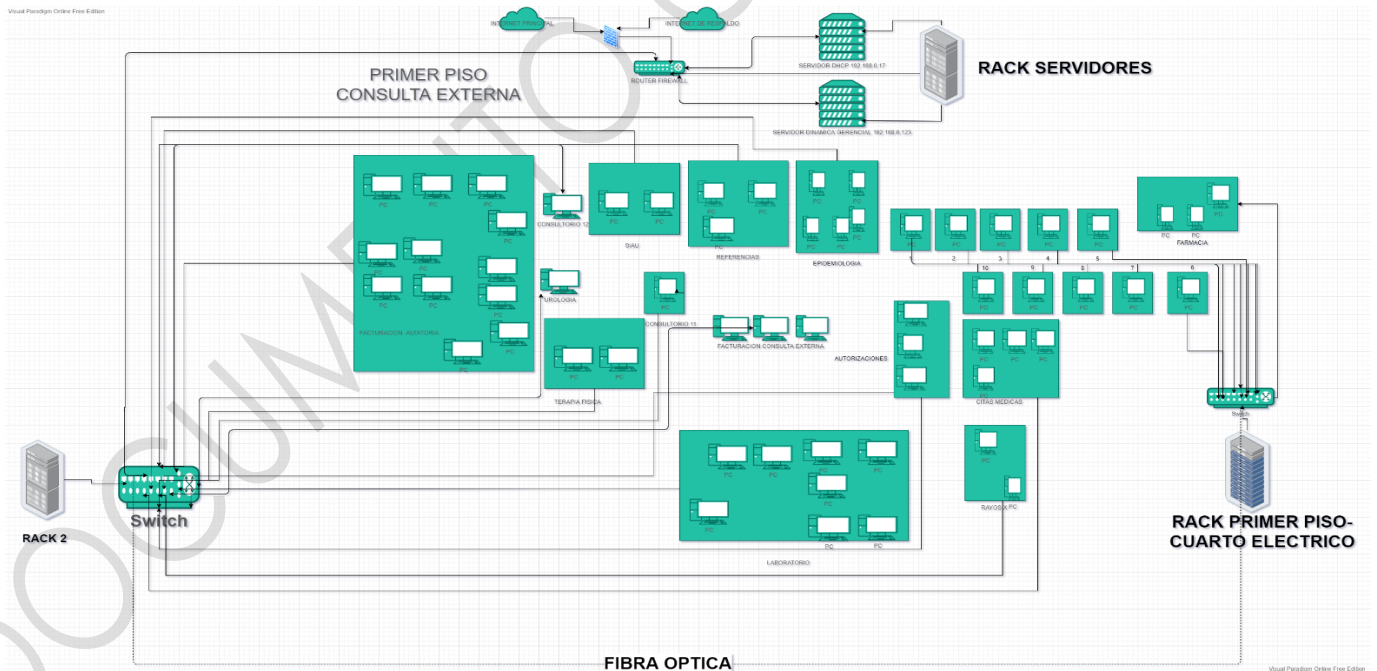


Ilustración 3–Esquema físico de Red de UCI-Urgencias

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital!”

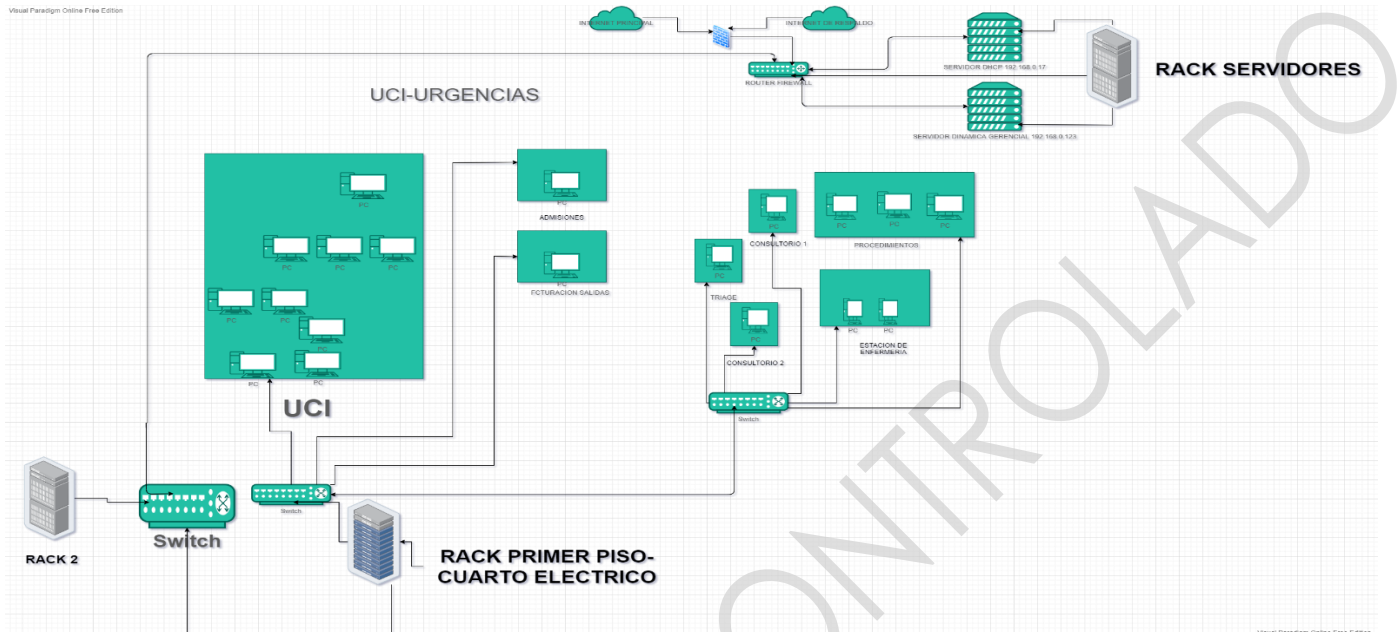


Ilustración 4-Eschema físico de Red de Ginecobstetricia-Cirugía

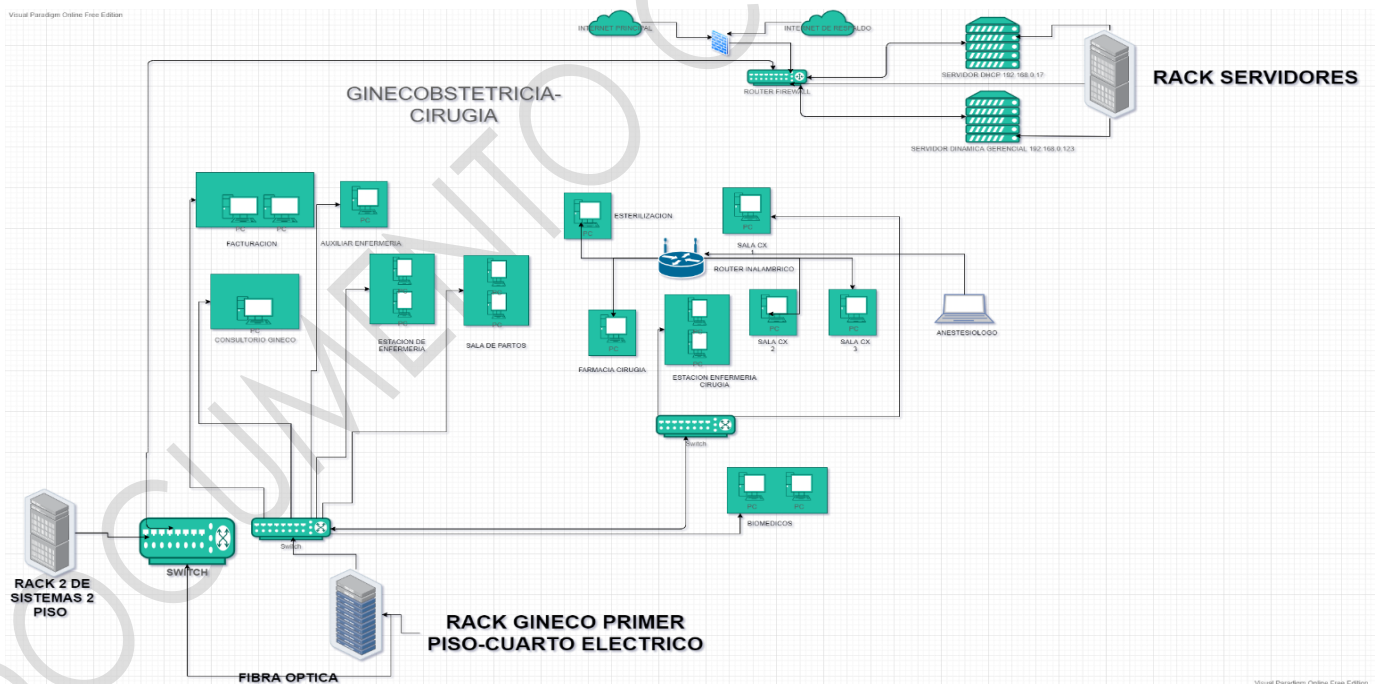


Ilustración 5-Eschema físico de Red de Hospitalización-Observación

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

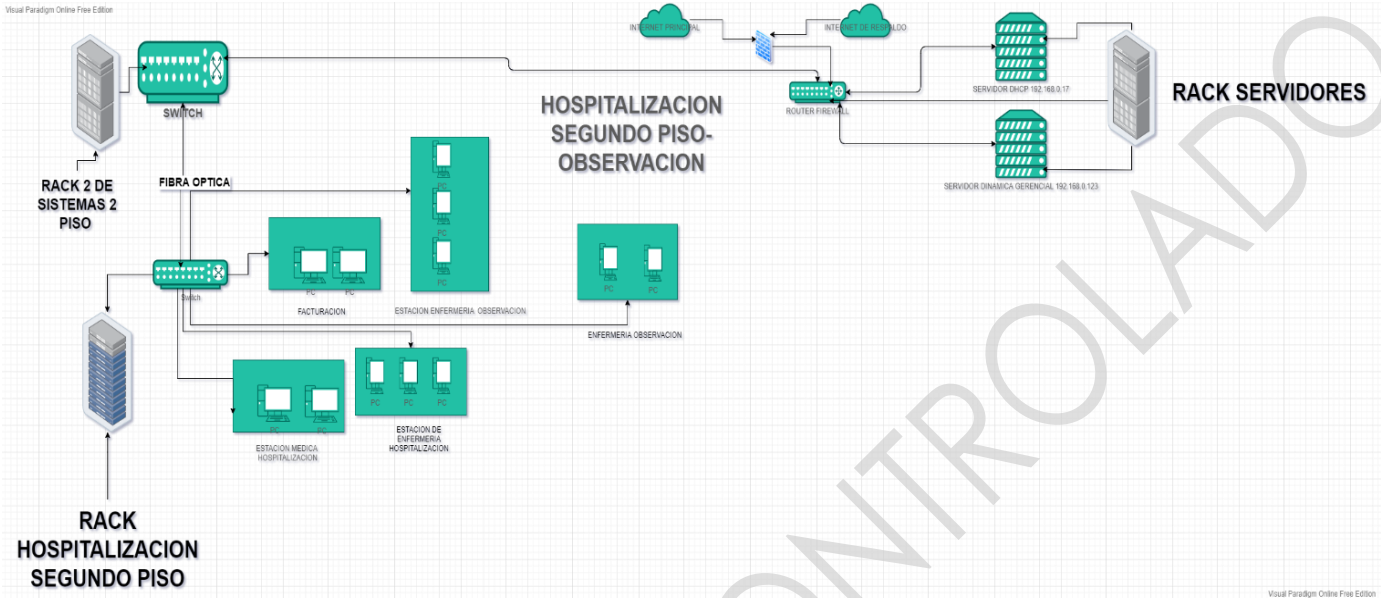
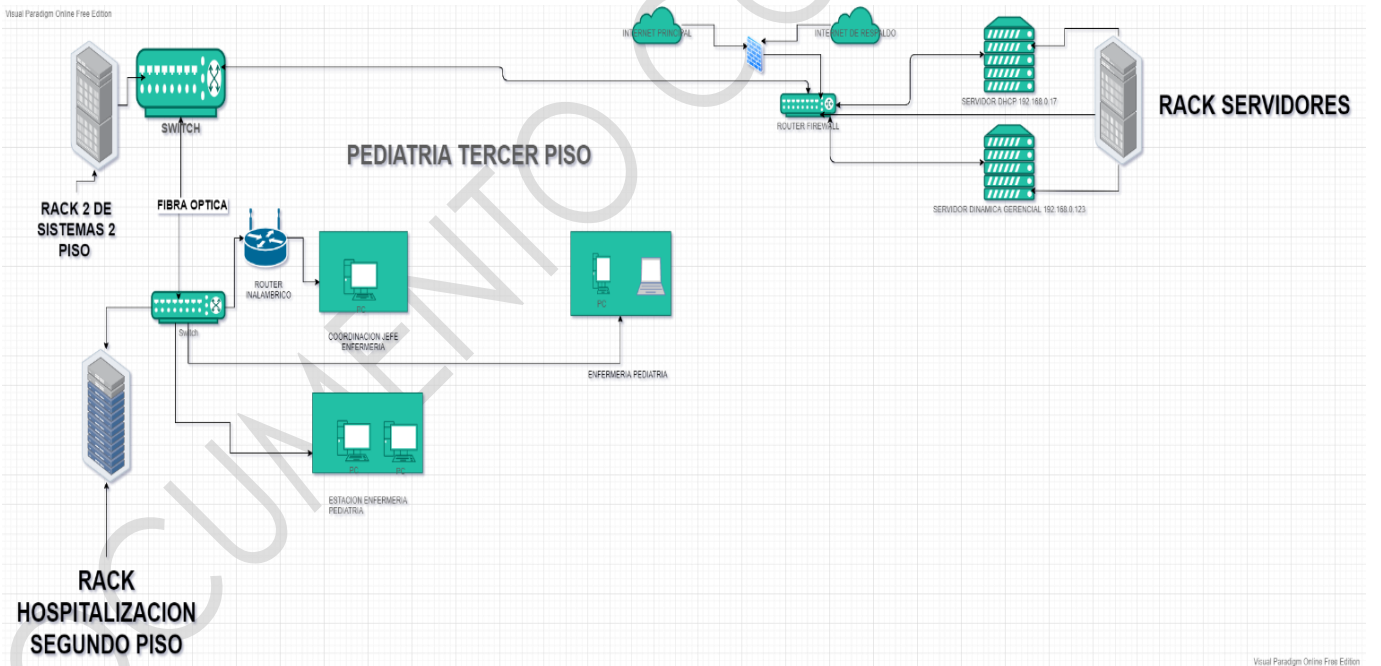



Ilustración 6–Esquema físico de Red de Pediatría



*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 21 de 62

## GESTIÓN DE INFORMACIÓN

El proceso de gestión de la información tiene como base reconocer la información como 'activo' de la organización, gerenciar las fuentes de información dado la responsabilidad en la calidad de los datos suministrados conforme a las necesidades de los clientes y así mismo generar cambios que impacten el negocio positivamente.

Se cuenta con un plan de gerencia de la información donde se ha estandarizado todo el proceso de gestión de la información en la institución.

### Talento Humano Área de Sistemas:

El área de sistemas del Hospital Departamental San Antonio de Padua está compuesta por:

- Profesional Universitario – Sistemas.
- Profesional De Apoyo DGH (Dinámica Gerencial Hospitalaria)
- Técnico administrativo – Sistemas.

### Profesional Universitario:


Presta servicios profesionales en sistemas de información automatizados a la Empresa en procesos operativos de ejecución de acciones de automatización y mantenimiento de los sistemas de información y el soporte al manejo de procesos automatizados en la Institución.

### Funciones Esenciales:

- Participar con los líderes de programas asistenciales y administrativos en la planeación de los servicios en condiciones normales y contingentes, identificando las necesidades de recursos físicos, técnicos y tecnológicos.
- Operar las unidades del equipo de computación y los sistemas centrales y periféricos y asistir a los usuarios en su manejo.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*


*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 22 de 62

- Garantizar el uso legal de software a través de la monitorización de caducidad de licencias.
- Aplicar y hacer cumplir las políticas de uso de los sistemas de información institucional a partir de los criterios planteados en los manuales y procedimientos para tal fin Brindar soporte técnico a todas las áreas de la institución, en la automatización y mantenimiento de los sistemas de información, en el manejo de procesos automatizados y la administración y uso del Software y Hardware utilizado.
- Garantizar la seguridad de la información mediante la consecución de software que evite ingresos maliciosos o dañinos y políticas de acceso seguro a la misma.
- Garantizar la disponibilidad de equipos e insumos técnicos y tecnológicos, de la institución a través de la programación oportuna de mantenimiento preventivo y correctivo.
- Mantener actualizada la infraestructura tecnológica (software y hardware) de la institución de acuerdo con las necesidades de los clientes internos y externos.
- Ejecutar las actividades de su responsabilidad y las resultantes de la elaboración de los planes de acción y de mejoramiento conforme a los Sistemas de Gestión Institucional.
- Proponer acciones de mejoramiento de las áreas de trabajo, atención a los usuarios y desarrollo científico y tecnológico de los procesos en la Empresa.
- Participar en los comités institucionales en los cuales se requiera el apoyo de su disciplina.
- Participar en el plan anual de capacitación institucional a través de la identificación de las necesidades propias relacionadas con la actividad que desempeña, la asistencia a cursos, talleres, reuniones y comités programados por el servicio o la institución y la divulgación de los conocimientos adquiridos.
- Participar como asistente y/o responsable en los procesos de inducción, reinducción y entrenamiento de pares.
- Custodiar, responder y hacer uso racional de los insumos, inventarios y elementos devolutivos bajo su responsabilidad.

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 23 de 62

- Las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, la naturaleza y el área de desempeño del cargo.

### Técnico administrativo:


Prestar servicios de nivel técnico a la Empresa, en procesos y procedimientos que contribuyan a la misión institucional. En la realización de acciones de administración de la infraestructura computacional del hospital.

### Funciones Esenciales:

- Brindar soporte técnico a todas las áreas de la institución en el manejo de los equipos de cómputo de la empresa.
- Participar en la elaboración y actualización de los procedimientos relacionados con el área de sistemas acordes al procedimiento establecido por el área de calidad.
- Apoyar en la ejecución de las actividades del plan de acción del proceso en lo referente con el área de sistemas de la institución.
- Elaborar y presentar informes sobre las actividades desarrolladas en las distintas unidades funcionales sobre soporte técnico en sistemas.
- Presentar recomendaciones cuando aplique en la mejora continua de los procesos y procedimientos de sistemas.
- Realizar actividades tendientes a controlar virus informáticos, y problemas relacionados con hardware y software institucional.
- Atender a los usuarios internos y externos en los requerimientos relacionados con el área de sistemas.
- Asistir a las capacitaciones designadas y retroalimentar al personal que le aplique para el correcto desarrollo del proceso.
- Responder, custodiar y velar por los Inventarios de los elementos devolutivos asignados y velar por la actualización permanente.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 24 de 62

- Participar en la conformación, la capacitación y las actividades de las brigadas de emergencia para dar cumplimiento al Plan de Emergencia Hospitalario.
- Las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, la naturaleza y el área de desempeño del cargo.

### 4.3 MARCO TEORICO

**Seguridad informática:** Proceso orientado a proteger todo lo que tiene que ver con la infraestructura tecnológica (hardware - software), como columna vertebral de los sistemas de información. Para ello es importante definir los activos críticos que hacen parte de dicha infraestructura, con el fin de identificar amenazas, vulnerabilidades y gestionar los riesgos asociados.

**Seguridad de la información:** Proceso orientado a proteger toda la información de una institución, independiente mente del modo de creación, procesamiento, almacenamiento, si es física o digital, incluso la memoria de las personas con información institucional. Para la gestión del riesgo se tiene en cuenta las personas, los procesos y la operación del negocio, así como también los aspectos físicos y tecnológicos.

Dentro de esta se definen tres principios fundamentales como son:

**Integridad:** Es la salvaguarda con precisión y totalmente completa de la Información.


**Confidencialidad:** Es la protección de los datos, que siempre estén seguros.

**Disponibilidad:** Es la garantía del acceso a la información siempre que sea necesitada.

**Análisis de riesgos informáticos:** Es el proceso mediante el cual se identifican los activos de la Organización las vulnerabilidades y amenazas a las que se puedan ver expuestas, así como la probabilidad de que ocurran estos hechos y el impacto que puede generar con el fin de mitigar, aceptar o transferir el riesgo.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 25 de 62

**Riesgo:** Es la probabilidad de que ocurra algo con consecuencias e impacto, igualmente la incertidumbre frente a la realización de un evento que afecte nuestra seguridad informática.

**Amenazas:** Es la potencial probabilidad que ocurra algún hecho que afecte nuestra seguridad, es decir la materialización del riesgo.

**Vulnerabilidades:** Son las debilidades o exposición del sistema, igualmente son las fallas ya sea por omisión o deficiencia de seguridad, que puedan ser aprovechadas por terceros.

**Gestión del riesgo:** Son los lineamientos dados para el manejo de la incertidumbre dada por una amenaza, eso se logra a través del estudio de los riesgos, generación de salvaguardas y controles necesarios para mitigar el riesgo.

**COBIT (Objetivos de control para tecnologías de la información):** Es un marco de referencia que adopta las mejores prácticas para gobernar y gestionar efectivamente la información y tecnología, lo cual incide en la toma efectiva de decisiones relacionadas con TI, realizar mejores inversiones, y poder generar más valor a los servicios o productos a partir de la información y los activos tecnológicos.


Características:

- Satisfacer las necesidades de los colaboradores.
- Se alinean las tecnologías de la información con las estrategias del negocio.
- Mejora los procesos de gobernanza y gestión de TI.
- Permite a los gerentes cubrir las brechas entre los requisitos de control, los aspectos técnicos y riesgos del negocio.

**ITIL (biblioteca de infraestructura de tecnologías de la información):** Es un marco de referencia que adopta las mejores prácticas para la gestión de servicios de TI y la relación con los procesos operativos de una empresa.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 26 de 62

Características:

- Creación de valor a través del servicio.
- Gestión del riesgo.
- Gestión de inversión y presupuesto para TI.
- Integra la estrategia para el servicio con estrategia de negocio y necesidades de clientes.
- Mejora la interacción con los clientes.

**ISO 27000:** Esta norma brinda un conjunto de estándares diseñados y desarrollados por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), proporcionando un marco de gestión de la seguridad de la información que sirve para cualquier organización, sin importar su naturaleza (pública o privada) o tamaño (grande o pequeña).

**ISO 27001:** Norma certificable que brinda todos los requisitos para el desarrollo, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información.


Características:

- Compromiso de la alta dirección.
- Análisis y tratamiento de riesgos.
- Definición de objetivos y estrategias.
- Recursos y competencias.

**MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información:** Esta herramienta permite evaluar y abordar los riesgos informáticos en busca de promover la eficacia en las comunicaciones en la organización y sus colaboradores, con el fin de dar

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 27 de 62

cumplimiento a los últimos estándares de la ISO 27001, 27005 y 31000 para la gestión de riesgos y brindar las justificaciones necesarias para la toma de decisiones gerenciales.

**CRAMM, CCTA – Risk – Analysis – and Management Method.** Se puede utilizar siempre que sea necesario para identificar la seguridad y/o requisitos de contingencia para un sistema de información o de la red.

**EBIOS,** Expresión de las necesidades e Identificación de los objetivos de seguridad. Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Adicional a esto, apoya a la preparación de la organización para procesos de evaluación, auditoría, certificación o acreditación según corresponda.


**NIST SP 800 – 30, National Institute of Standards and Technology.** Guía de gestión de riesgo para sistemas de tecnología de la información. Propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información; sin embargo, esto no es suficiente, pues se necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito.

**ISO//IEC 27005 – MEHARI,** Método armonizado de análisis de riesgos. Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgo, evaluando cuantitativamente, de acuerdo con la situación de la organización, dónde se requiere el análisis; acopla los objetivos estratégicos existentes con los nuevos métodos de funcionamiento de la empresa mediante una política de seguridad y mantenimiento de los riesgos a un nivel convenido.

**CORAS, Construct a Platformfor Risk Analysis of Security Critical Systems,** Su aplicación permite la detección de fallas de seguridad, inconsistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad, exploradas en siete etapas: presentación, análisis de alto nivel,

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 28 de 62

aprobación, identificación de riesgos, estimación de riesgo, evaluación de riesgo y tratamiento del riesgo

**OCTAVE, Operationally Critical Threat, Asset, and Vulnerability Evaluation, Octave**, evalúa los riesgos de seguridad de la información y propone un plan de mitigación de estos dentro de una organización. Sus objetivos se encuentran enfocados básicamente en concientizar a la organización en cuanto a que la seguridad informática no es un asunto solamente técnico, y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos.

**COBIT, Control Objectives Control Objectives for Information and related Technology**, Sus conceptos se aplican en los niveles operacional y táctico y permiten que la estructura departamento de TI el ciclo de vida de sus servicios en su conjunto, con el fin de alcanzar la excelencia operativa.

#### 4.4 MARCO LEGAL


**Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

**Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

**Ley 1437 de 2011:** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 29 de 62

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

**Ley 1753 de 09 de junio de 2015:** Por la cual se expide el Plan Nacional de Desarrollo, 2014-2018. "Todos por un nuevo país"

**Decreto 3816 de 2003:** "Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública".

**Decreto 235 DE 2010:** Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones.

**Decreto 019 de 2012:** Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

**Decreto 2609 de 2012:** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.


**Decreto 1078 de 2015:** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

**Decreto 415 de 2016:** "Por el cual se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".

**Decreto 2094 de 2016:** Por el cual se modifica la estructura del Departamento Administrativo para la Prosperidad Social - Prosperidad Social.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 30 de 62

**Decreto 1499 de 2017:** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

**Documento CONPES No. 3854 de 2016:** Política Nacional de Seguridad Digital.

Acuerdo 003 de 2015 del AGN: "Por el cual se establecen los lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.

## 5. METODOLOGIA

### 5.1 METODOLOGIA DE LA INVESTIGACIÓN


La metodología de análisis y gestión de riesgos de los sistemas de Información, define los riesgos como la posibilidad que suceda un daño, tiene dos objetivos claros: el estudio de los riesgos que soportan los sistemas de información y realizar las recomendaciones de las medidas que se deben adoptar para conocer, prevenir, impedir, reducir o controlar los riesgos encontrados, realiza análisis sobre sus principales elementos los cuales define como activo, amenaza, vulnerabilidades, impacto, riesgo y salvaguarda, maneja las etapas de planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas, sus guías se dividen en tres libros: Métodos, Catalogo de Elementos y Guías Técnicas.

Los cuales contemplan el siguiente catálogo de elementos:

- Tipos de Activos

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 31 de 62

- Dimensión de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de Información
- Salvaguardas por considerar para proteger sistemas de Información

Aplicada esta metodología al estudio que se realiza en el desarrollo de este proyecto se recolecta la información pertinente mediante recorridos en la Institución donde se identifican los activos físicos y se plasman en la ficha técnica de activos, adicional se realizará entrevistas con el personal encargado del área informática para conocer el área y su infraestructura, las políticas ya implementadas, la documentación pertinente y el plan de seguimiento y medición, finalmente se realizará observación de las prácticas de los usuarios.

## 6. ANÁLISIS DE LA INFORMACIÓN

Teniendo en cuenta la metodología que hace énfasis en la identificación de activos categorizados en grupos, con el fin de identificar riesgos y realizar controles frente a estos, se realiza la identificación de activos informáticos en el Hospital Departamental San Antonio de Padua.

### 6.1 IDENTIFICACIÓN DE ACTIVOS


Ver anexo No. 1 Inventarios de Activos

### 6.2 IDENTIFICACIÓN DE VULNERABILIDADES

Una vulnerabilidad es una debilidad o falla en un activo de información, la cual puede ser explotada por una amenaza, poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 32 de 62


Para la identificación de vulnerabilidades se priorizaron los activos de información más sensibles de la Institución los cuales fueron analizados con software especializado como Nmap ("Network Mapper") que es una herramienta de distribución libre utilizada para el análisis de redes y auditorías de seguridad, esta aplicación utiliza técnicas especializadas de escaneo para identificar equipos activos en una red, sistemas operativos, puertos abiertos, protocolos y servicios en ejecución, adicionalmente contiene scripts para identificación de vulnerabilidades, lo que significa información valiosa para estructurar un ataque por parte de un ciberdelincuente.

Tabla 4 - Activos de Información Analizados

Equipo	Aplicativo	Especificaciones
<b>Servidor HP Prolaint 180 Gen 9</b>	Servicios DG IP: 192.168.0.123	Procesador Intel Xeon CPU E5-2609 V3 @1.90 GHz Velocidad 1900 MHz Discos Duros 2 Total: 1.2 TB Memoria RAM 16 GIGAS Tipo de BIOS: (12/2014)
<b>Servidor HP Prolaint 180 Gen 9</b>	Servicios DHCP Interfaz de Laboratorio Gestión Documental IP: 192.168.0.17	Procesador Intel Xeon CPU E5-2609 V3 @1.90 GHz Velocidad 1900 MHz Discos Duros 2 Total: 1.2 TB Memoria RAM 8 GIGAS Tipo de BIOS: (12/2014)
<b>Firewall</b>	Firewall de seguridad de red	MAC Address: 2C:B8:ED:3D:3E:9C (SonicWall) DIRECCION IP : 192.168.0.24
<b>Servidor de Imágenes diagnosticas</b>	Carestream	IP: 192.168.0.91 MAC Address: 70:10:6F:BC:C1:8C (Hewlett Packard Enterprise)

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	Fecha: 26/04/2024
		Código: MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	Versión: 02
		Página No. 33 de 62
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>		

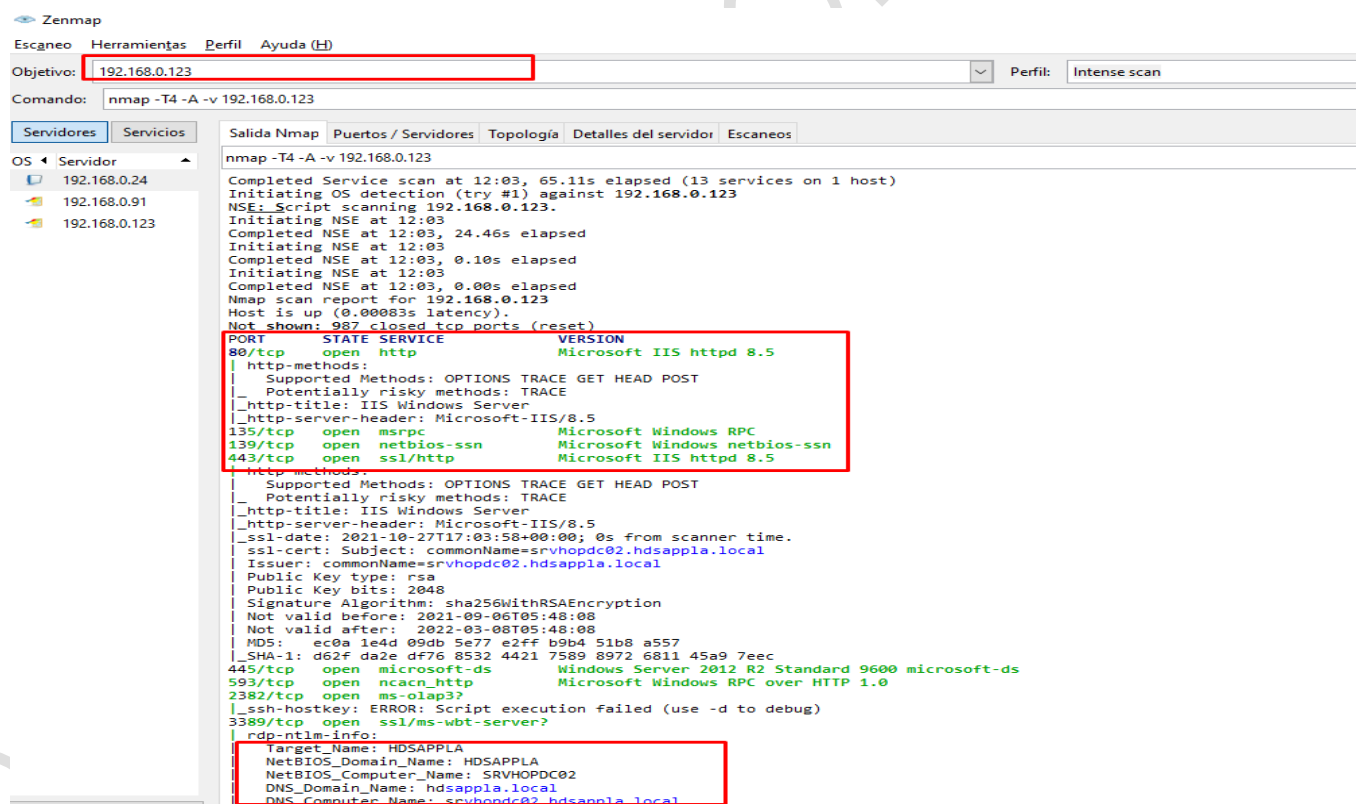
## Resultados NMAP

Se ejecuta la interfaz gráfica de Nmap la cual presenta varias opciones de escaneo, en este caso se toma la opción "Intense Scan", que utiliza el comando `nmap -T4 -A -v <dirección IP>` para escanear los puertos TCP más comunes, servicios en ejecución, sistema operativo y su versión; de igual forma se ejecuta `script` para identificación de vulnerabilidades.

### • Servidor HP Prolaint DL 180 DGH:

Se realiza el análisis con el aplicativo nmap al servidor HP Prolaint DL 180 con dirección IP 192.168.0.123, con el objetivo de obtener los datos que lleve a identificar las vulnerabilidades.

Ilustración 1 – Análisis servidor - HP Prolaint DL 180



```

Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: 192.168.0.123 Perfil: Intense scan
Comando: nmap -T4 -A -v 192.168.0.123

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos
OS Servidor
192.168.0.24
192.168.0.91
192.168.0.123

nmap -T4 -A -v 192.168.0.123
Completed Service scan at 12:03, 65.11s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.123
NSE: Script scanning 192.168.0.123.
Initiating NSE at 12:03
Completed NSE at 12:03, 24.46s elapsed
Initiating NSE at 12:03
Completed NSE at 12:03, 0.10s elapsed
Initiating NSE at 12:03
Completed NSE at 12:03, 0.00s elapsed
Nmap scan report for 192.168.0.123
Host is up (0.00083s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 8.5
|_ http-methods:
|_ Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ http-title: IIS Windows Server
|_ http-server-header: Microsoft-IIS/8.5
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
443/tcp   open  ssl/http         Microsoft IIS httpd 8.5
|_ http-methods:
|_ Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ http-title: IIS Windows Server
|_ http-server-header: Microsoft-IIS/8.5
|_ ssl-date: 2021-10-27T17:03:58+00:00; 0s from scanner time.
|_ ssl-cert: Subject: commonName=srvhopdc02.hdsappla.local
|_ Issuer: commonName=srvhopdc02.hdsappla.local
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2021-09-06T05:48:08
|_ Not valid after: 2022-03-08T05:48:08
|_ MD5: ec0a 1e4d 09db 5e77 e2ff b9b4 51b8 a557
|_ SHA-1: d62f da2e df76 8532 4421 7509 8972 6811 45a9 7eec
445/tcp   open  microsoft-ds     Windows Server 2012 R2 Standard 9600 microsoft-ds
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
2382/tcp  open  ms-olap3?
|_ ssh-hostkey: ERROR: Script execution failed (use -d to debug)
3389/tcp  open  ssl/ms-wbt-server?
|_ nmap-ntlm-info:
|_ Target_Name: HDSAPPLA
|_ NetBIOS_Domain_Name: HDSAPPLA
|_ NetBIOS_Computer_Name: SRVHOPDC02
|_ DNS_Domain_Name: hdsappla.local
|_ DNS_Computer_Name: srvhopdc02.hdsappla.local

```

Fuente: Aplicativo NMAP

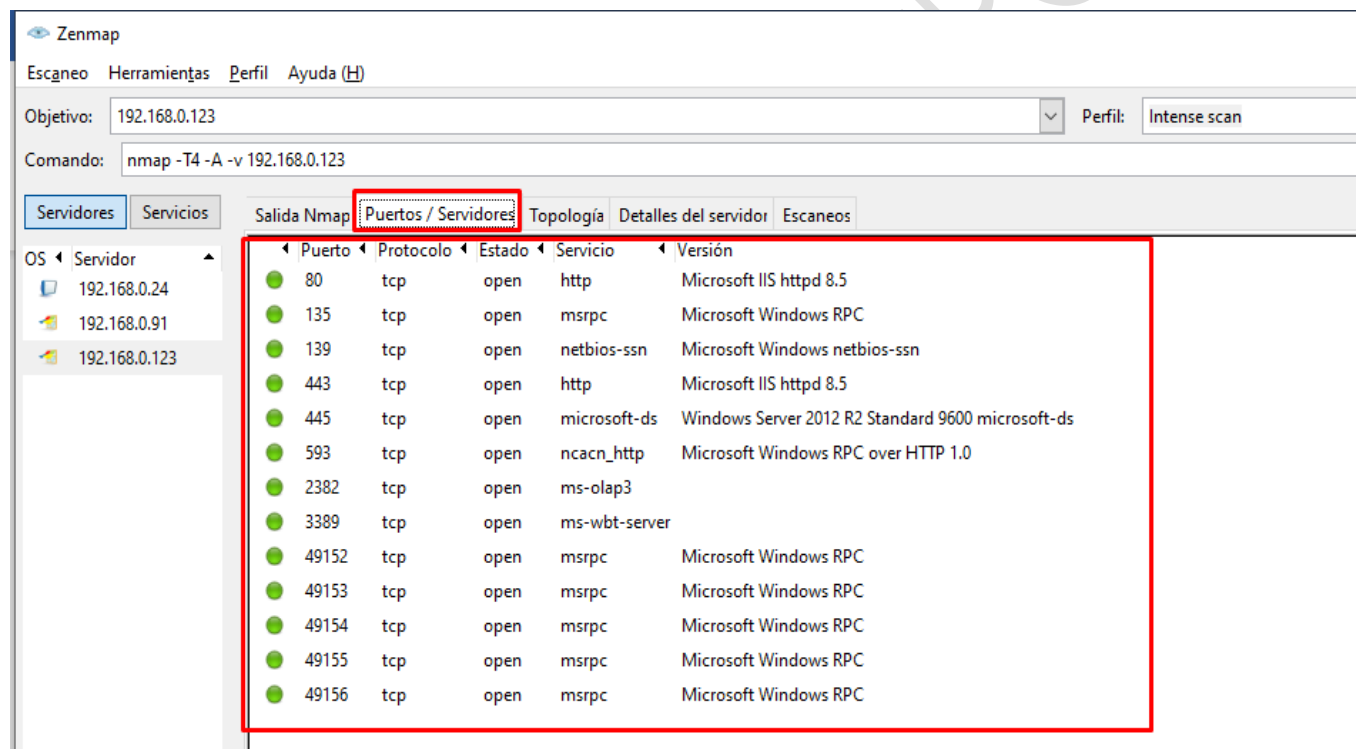
*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

Una vez realizado el escaneo al Activo de información con IP 192.168.0.123, La herramienta muestra en diferentes pestañas la información recolectada.

En la pestaña puertos/servidores se observa un recopilatorio de todos los puertos abiertos, el número de puerto, protocolo, estado, servicio, dependiendo del tipo de escaneo que se realice, mostrando más o menos puertos.

Ilustración 2- Escaneo de Puertos y servicios - HP Prolaint DL 180



Fuente: Análisis con el aplicativo NMAP

El equipo escaneado se puede ver en la pestaña Detalles del servidor donde se encuentra cada uno de los datos correspondientes al mismo.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*


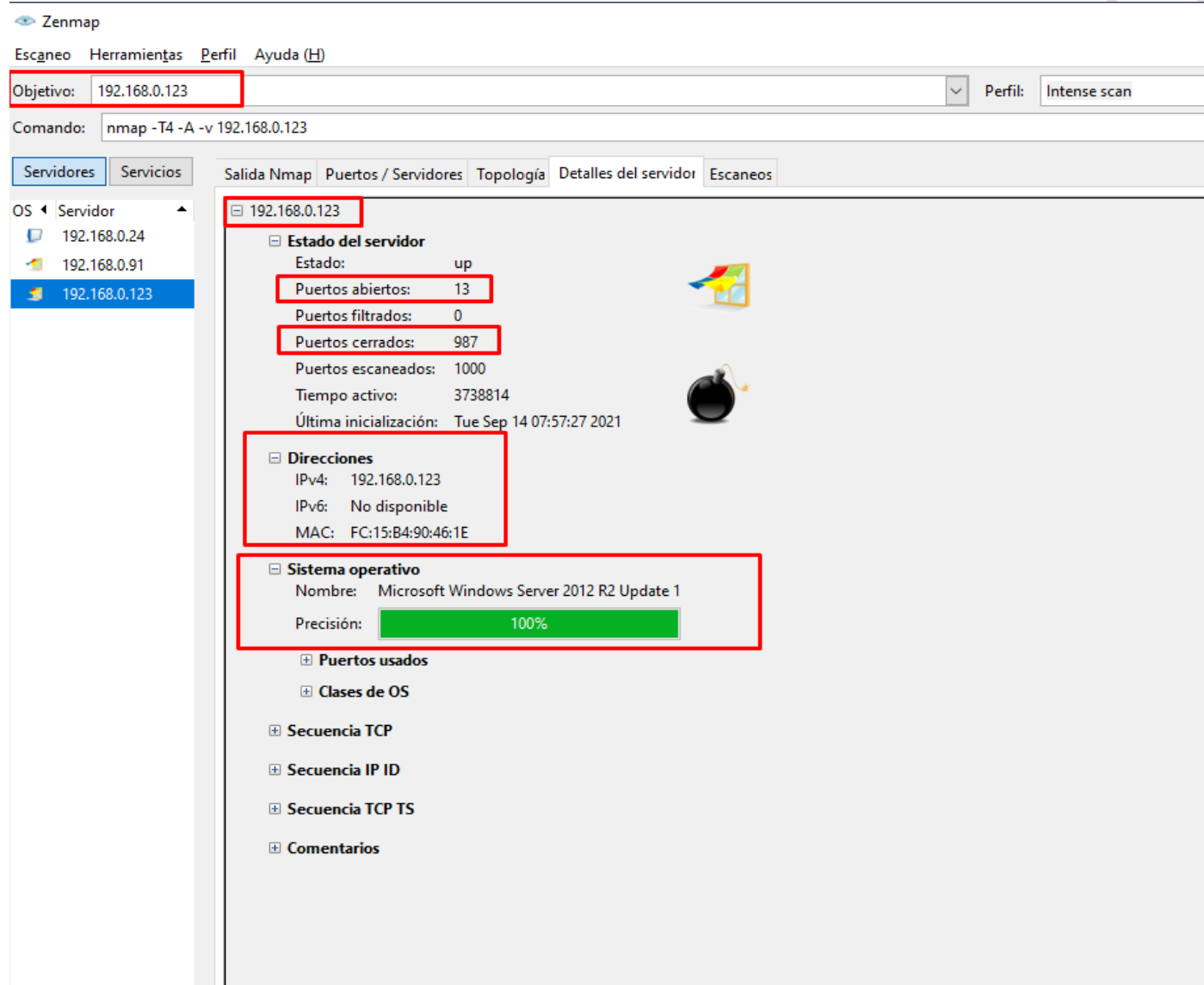
	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	<b>Código:</b> MAG-GIT-AS-IF-001
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02	<b>Página No.</b> 35 de 62

Ilustración 3– Detalles del servidor - HP Prolaint DL 180



Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: 192.168.0.123 Perfil: Intense scan

Comando: nmap -T4 -A -v 192.168.0.123

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS Servidor

- 192.168.0.24
- 192.168.0.91
- 192.168.0.123

192.168.0.123

Estado del servidor

Estado: up

Puertos abiertos: 13

Puertos filtrados: 0

Puertos cerrados: 987

Puertos escaneados: 1000

Tiempo activo: 3738814

Última inicialización: Tue Sep 14 07:57:27 2021

Direcciones

IPv4: 192.168.0.123

IPv6: No disponible

MAC: FC:15:B4:90:46:1E

Sistema operativo

Nombre: Microsoft Windows Server 2012 R2 Update 1

Precisión: 100%

Puertos usados

Clases de OS

Secuencia TCP

Secuencia IP ID

Secuencia TCP TS

Comentarios

Fuente: Análisis aplicativo Nmap

En la ilustración 7, se visualizan resultados de ejecución del *scriptVuln* para la identificación de vulnerabilidades del servidor espejo HP Prolaint DL 180 con IP 192.168.0.123 desde el aplicativo Nmap, **se encuentra que no hay ninguna vulnerabilidad.**

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”


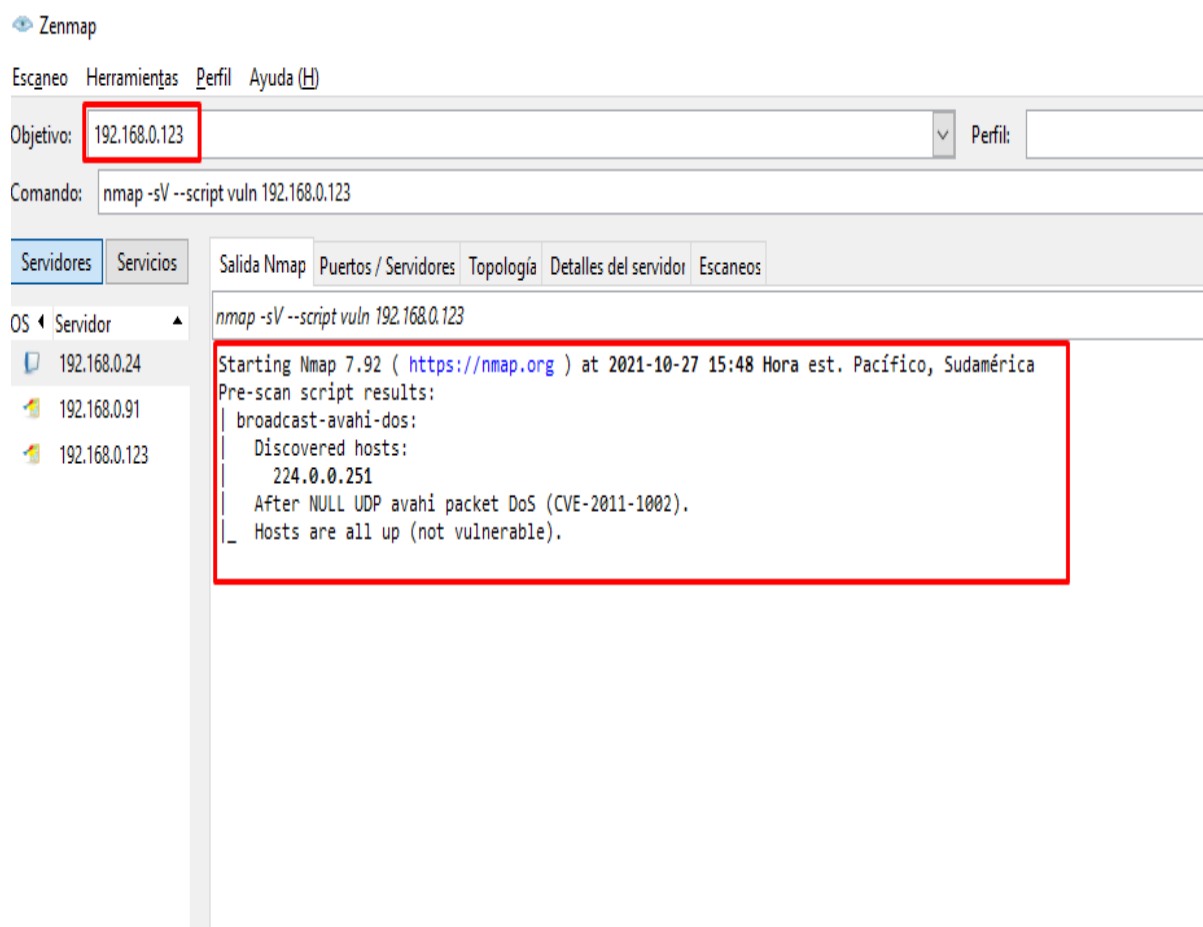
	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 36 de 62

Ilustración 4 – Identificación de vulnerabilidades 1- HP Prolaint DL 180  
 No se encuentra ninguna vulnerabilidad



Fuente: Análisis aplicativo Nmap

- **Servidor HP Prolaint DL 180**

Se realiza el análisis con el aplicativo nmap al servidor HP Prolaint DL 180 con dirección IP 192.168.0.17, con el objetivo de obtener los datos que lleven a la identificación de las vulnerabilidades.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*


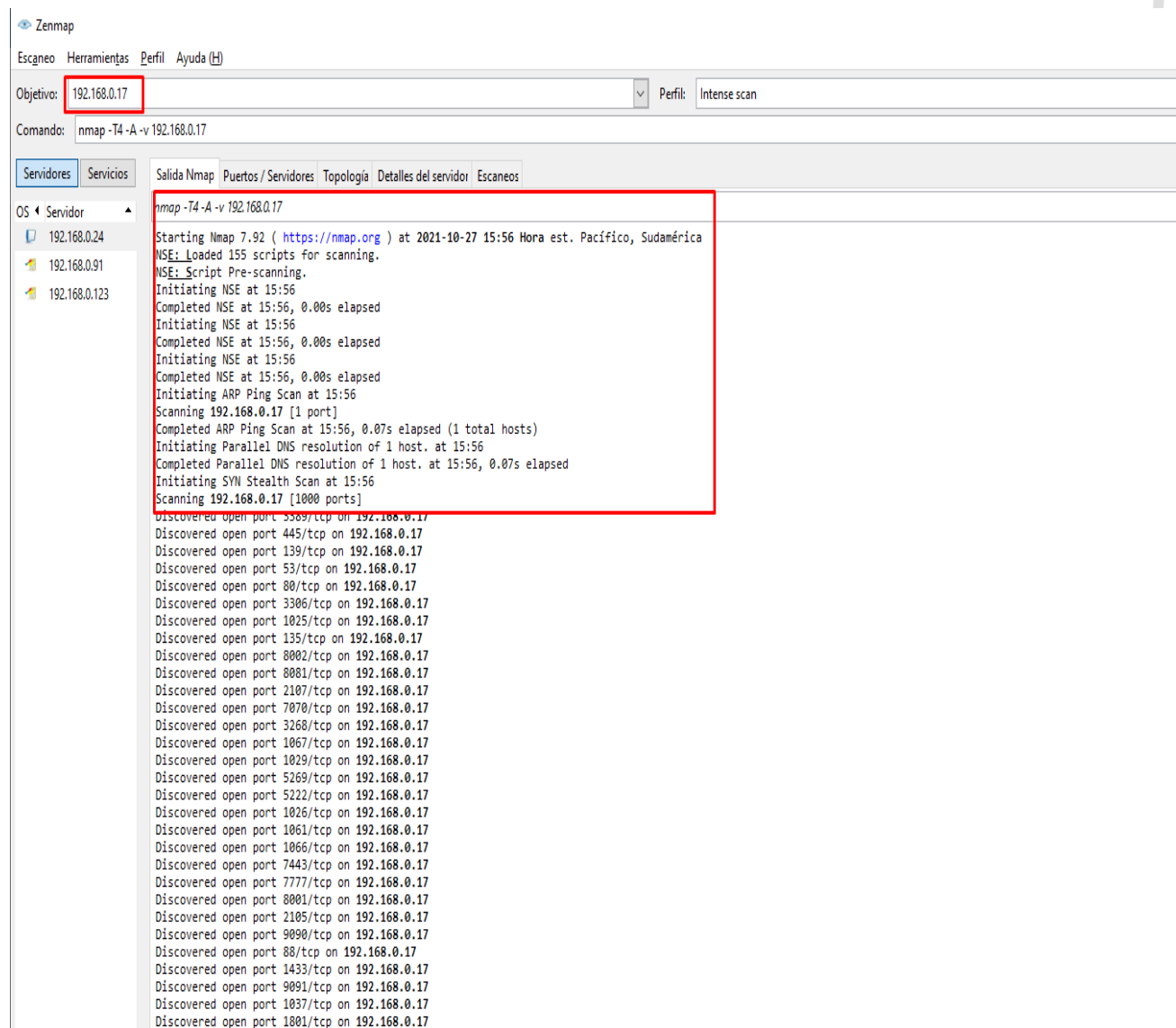
	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	Fecha: 26/04/2024
		Código: MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	Versión: 02
		Página No. 37 de 62
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>		

Ilustración 1- Análisis Servidor - HP Prolaint DL 180



Objetivo: 192.168.0.17 Perfil: Intense scan

Comando: nmap -T4 -A -v 192.168.0.17

```

nmap -T4 -A -v 192.168.0.17
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-27 15:56 Hora est. Pacífico, Sudamérica
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Initiating ARP Ping Scan at 15:56
Scanning 192.168.0.17 [1 port]
Completed ARP Ping Scan at 15:56, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:56
Completed Parallel DNS resolution of 1 host. at 15:56, 0.07s elapsed
Initiating SYN Stealth Scan at 15:56
Scanning 192.168.0.17 [1000 ports]
Discovered open port 5589/tcp on 192.168.0.17
Discovered open port 445/tcp on 192.168.0.17
Discovered open port 139/tcp on 192.168.0.17
Discovered open port 53/tcp on 192.168.0.17
Discovered open port 80/tcp on 192.168.0.17
Discovered open port 3306/tcp on 192.168.0.17
Discovered open port 1025/tcp on 192.168.0.17
Discovered open port 135/tcp on 192.168.0.17
Discovered open port 8002/tcp on 192.168.0.17
Discovered open port 8081/tcp on 192.168.0.17
Discovered open port 2107/tcp on 192.168.0.17
Discovered open port 7070/tcp on 192.168.0.17
Discovered open port 3268/tcp on 192.168.0.17
Discovered open port 1067/tcp on 192.168.0.17
Discovered open port 1029/tcp on 192.168.0.17
Discovered open port 5269/tcp on 192.168.0.17
Discovered open port 5222/tcp on 192.168.0.17
Discovered open port 1026/tcp on 192.168.0.17
Discovered open port 1061/tcp on 192.168.0.17
Discovered open port 1066/tcp on 192.168.0.17
Discovered open port 7443/tcp on 192.168.0.17
Discovered open port 7777/tcp on 192.168.0.17
Discovered open port 8001/tcp on 192.168.0.17
Discovered open port 2105/tcp on 192.168.0.17
Discovered open port 9090/tcp on 192.168.0.17
Discovered open port 88/tcp on 192.168.0.17
Discovered open port 1433/tcp on 192.168.0.17
Discovered open port 9091/tcp on 192.168.0.17
Discovered open port 1037/tcp on 192.168.0.17
Discovered open port 1801/tcp on 192.168.0.17

```

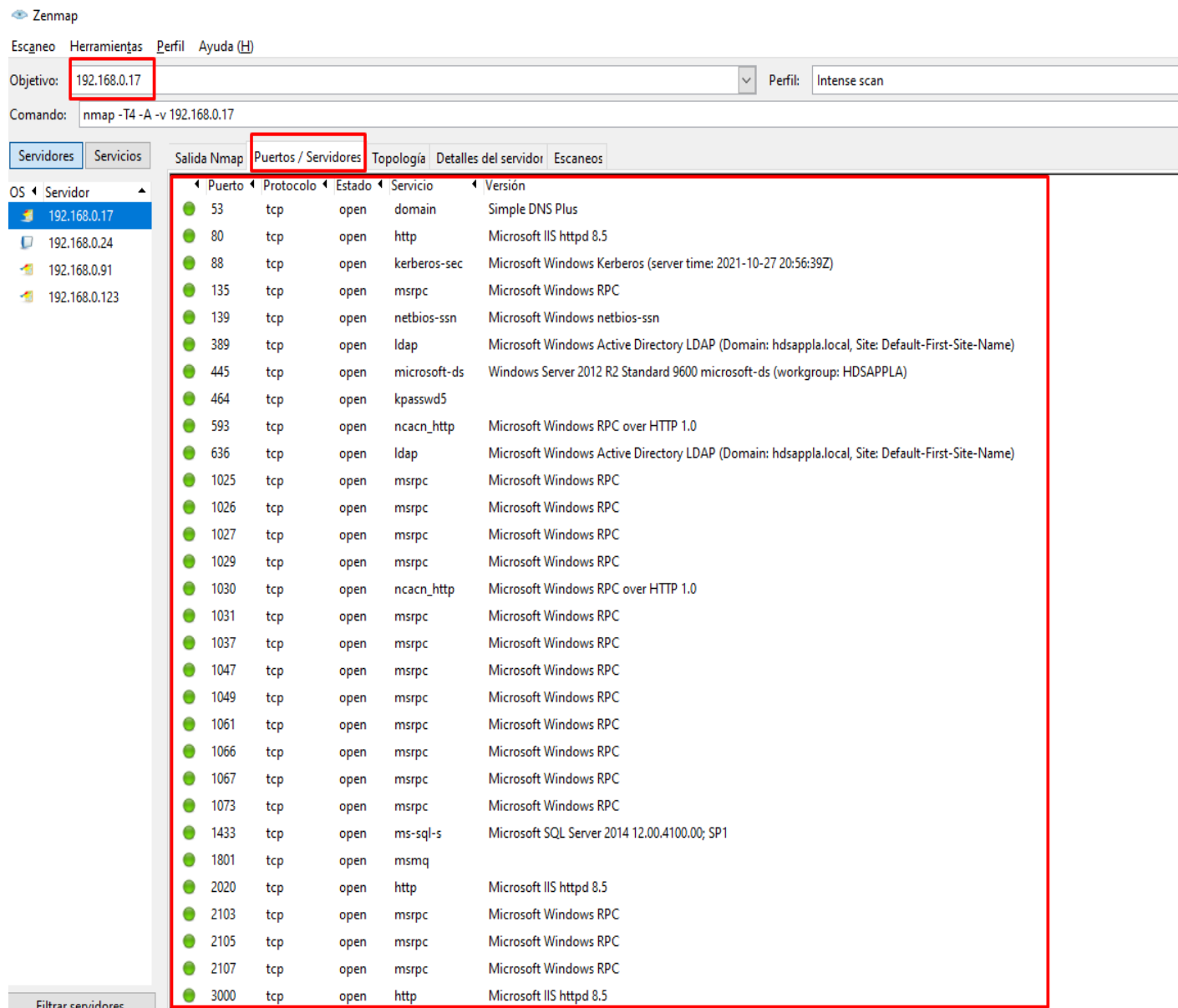
Fuente: Análisis aplicativo Nmap

En la pestaña puertos/servidores se observa un recopilatorio de todos los puertos abiertos, el número de puerto, protocolo, estado, servicio, dependiendo del tipo de escaneo que realicemos, se muestra más o menos puertos.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

Ilustración 2 –Escaneo de puertos y servicios - HP Prolaint DL 180



Objetivo: 192.168.0.17 Perfil: Intense scan

Comando: nmap -T4 -A -v 192.168.0.17

Puerto	Protocolo	Estado	Servicio	Versión
53	tcp	open	domain	Simple DNS Plus
80	tcp	open	http	Microsoft IIS httpd 8.5
88	tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2021-10-27 20:56:39Z)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
389	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: hdsappla.local, Site: Default-First-Site-Name)
445	tcp	open	microsoft-ds	Windows Server 2012 R2 Standard 9600 microsoft-ds (workgroup: HDSAPPLA)
464	tcp	open	kpasswd5	
593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: hdsappla.local, Site: Default-First-Site-Name)
1025	tcp	open	msrpc	Microsoft Windows RPC
1026	tcp	open	msrpc	Microsoft Windows RPC
1027	tcp	open	msrpc	Microsoft Windows RPC
1029	tcp	open	msrpc	Microsoft Windows RPC
1030	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1031	tcp	open	msrpc	Microsoft Windows RPC
1037	tcp	open	msrpc	Microsoft Windows RPC
1047	tcp	open	msrpc	Microsoft Windows RPC
1049	tcp	open	msrpc	Microsoft Windows RPC
1061	tcp	open	msrpc	Microsoft Windows RPC
1066	tcp	open	msrpc	Microsoft Windows RPC
1067	tcp	open	msrpc	Microsoft Windows RPC
1073	tcp	open	msrpc	Microsoft Windows RPC
1433	tcp	open	ms-sql-s	Microsoft SQL Server 2014 12.00.4100.00; SP1
1801	tcp	open	msmq	
2020	tcp	open	http	Microsoft IIS httpd 8.5
2103	tcp	open	msrpc	Microsoft Windows RPC
2105	tcp	open	msrpc	Microsoft Windows RPC
2107	tcp	open	msrpc	Microsoft Windows RPC
3000	tcp	open	http	Microsoft IIS httpd 8.5

Fuente: Análisis aplicativo Nmap

El equipo escaneado se puede ver en la pestaña Detalles del servidor donde se encuentra cada uno de los datos correspondientes al mismo.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*


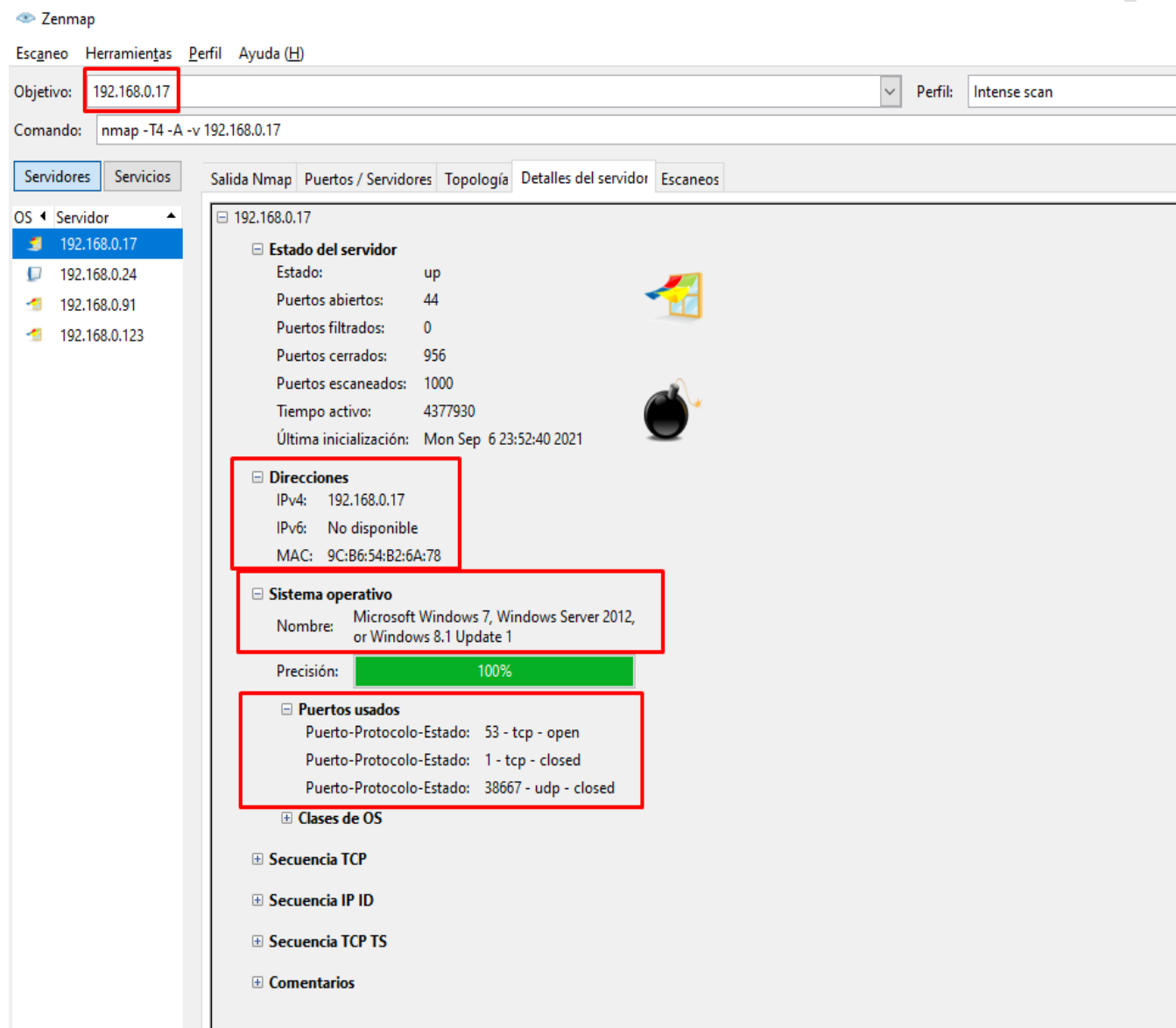
	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 39 de 62
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>		

Ilustración 3– Detalles del servidor- HP Prolaint DL 180



Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: 192.168.0.17 Perfil: Intense scan

Comando: nmap -T4 -A -v 192.168.0.17

Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS Servidor

- 192.168.0.17
- 192.168.0.24
- 192.168.0.91
- 192.168.0.123

192.168.0.17

- Estado del servidor
  - Estado: up
  - Puertos abiertos: 44
  - Puertos filtrados: 0
  - Puertos cerrados: 956
  - Puertos escaneados: 1000
  - Tiempo activo: 4377930
  - Última inicialización: Mon Sep 6 23:52:40 2021
- Direcciones
  - IPv4: 192.168.0.17
  - IPv6: No disponible
  - MAC: 9C:B6:54:B2:6A:78
- Sistema operativo
  - Nombre: Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
  - Precisión: 100%
- Puertos usados
  - Puerto-Protocolo-Estado: 53 - tcp - open
  - Puerto-Protocolo-Estado: 1 - tcp - closed
  - Puerto-Protocolo-Estado: 38667 - udp - closed
- Clases de OS
- Secuencia TCP
- Secuencia IP ID
- Secuencia TCP TS
- Comentarios

Fuente: Análisis aplicativo Nmap

En la ilustración 15, se visualizan resultados de ejecución del *scriptVuln* para la identificación de vulnerabilidades del servidor espejo HP Prolaint DL 180 con IP 192.168.0.17 desde el aplicativo Nmap. **No se encuentran ninguna vulnerabilidad.**

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”


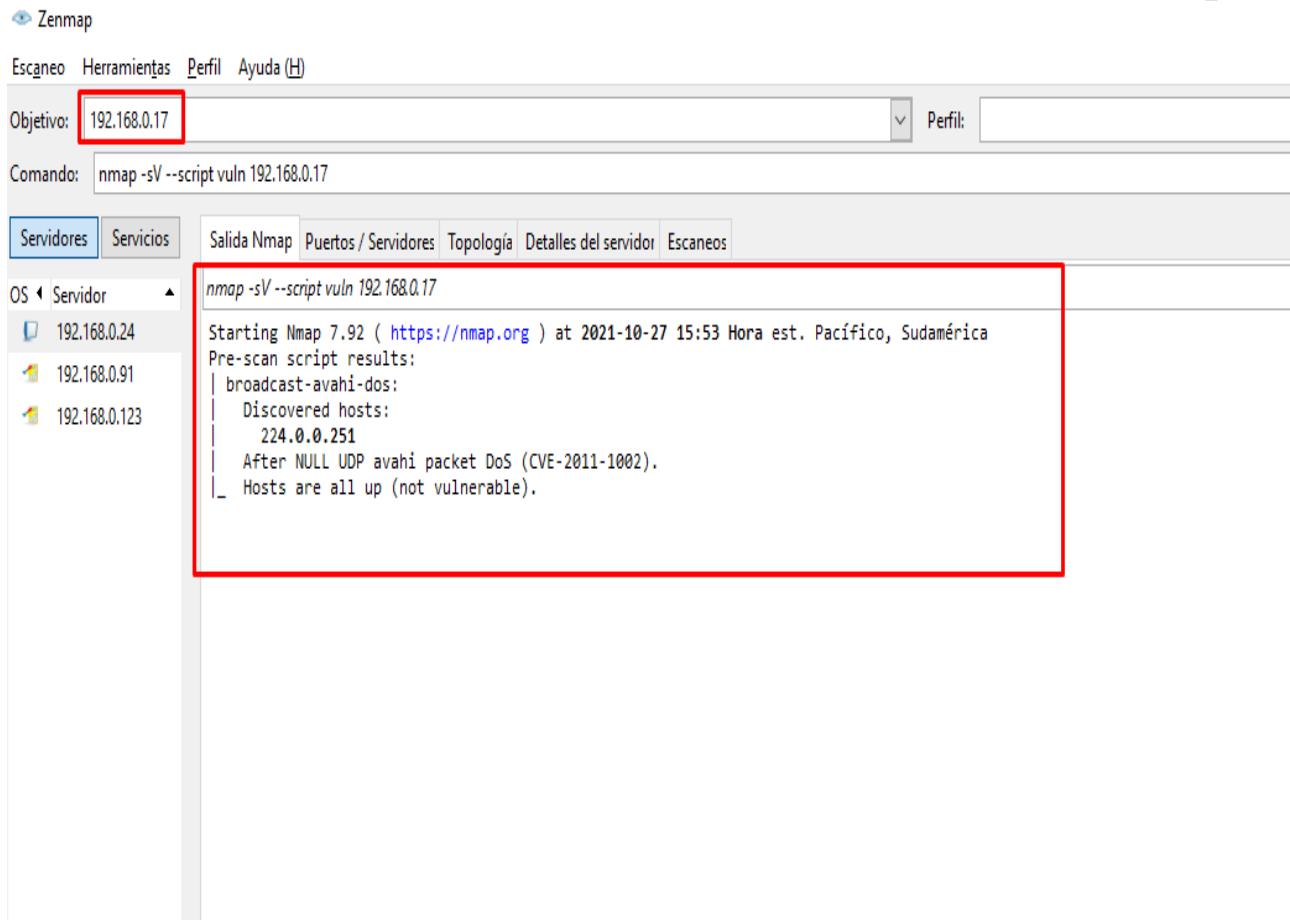
	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 40 de 62

Ilustración 4- Escaneo de vulnerabilidades - HP Prolaint DL 180




Fuente: Análisis aplicativo Nmap

- **Servidor de Imágenes Diagnosticas**

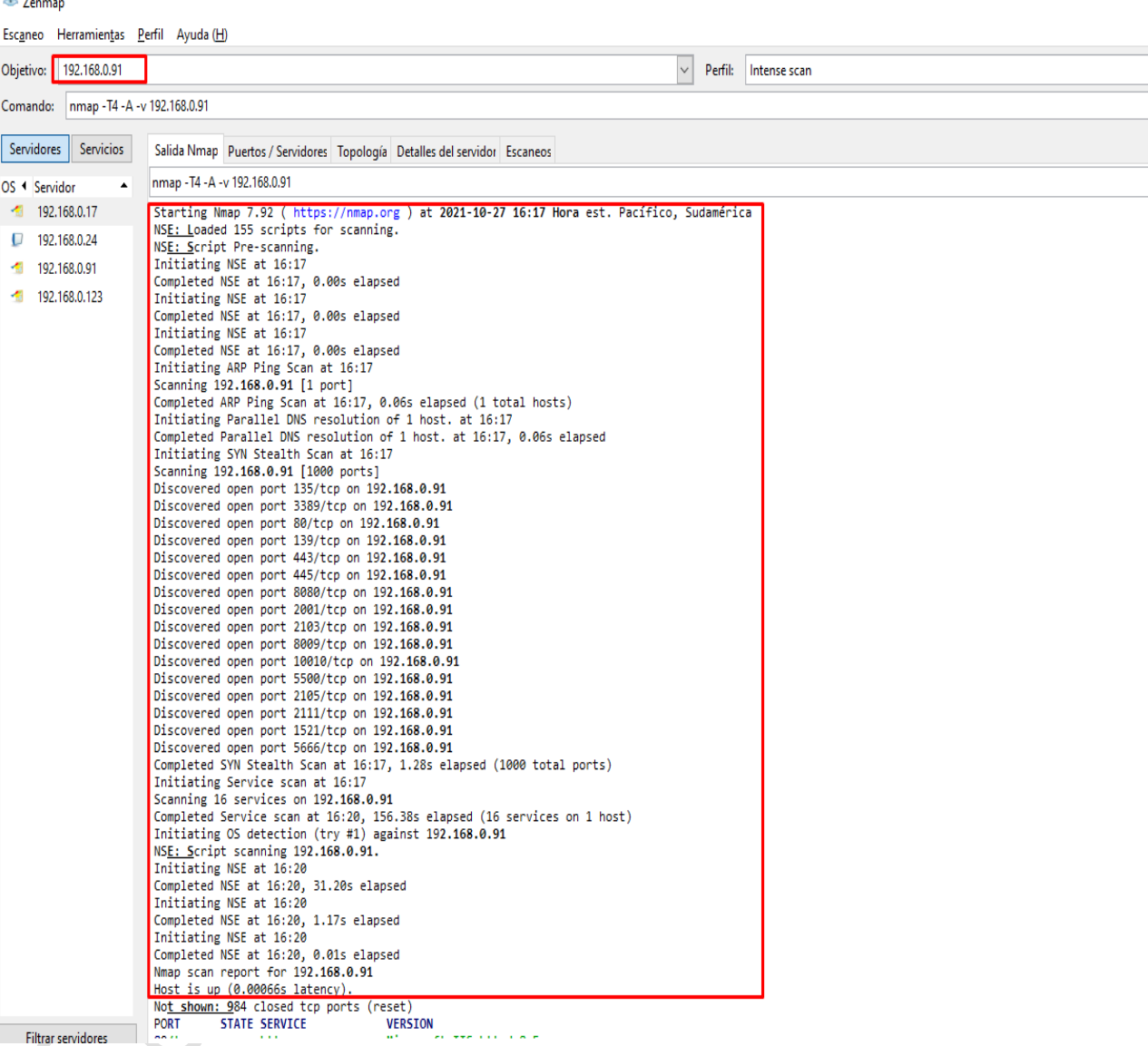
En la ilustración 18, 19 y 20 se realiza el análisis e identificación las Vulnerabilidades del servidor con dirección 192.168.0.91 identificadas con el aplicativo Nmap, para el escaneo de vulnerabilidades.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	Fecha: 26/04/2024
		Código: MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	Versión: 02
		Página No. 41 de 62
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>		

### Ilustración 1– Análisis del servidor - HP Prolaint DL 180 IMÁGENES DIAGNOSTICAS



The screenshot shows the Zenmap interface with the following details:

- Objetivo:** 192.168.0.91
- Perfil:** Intense scan
- Comando:** nmap -T4 -A -v 192.168.0.91
- Salida Nmap:**

```

Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-27 16:17 Hora est. Pacifico, Sudamérica
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:17
Completed NSE at 16:17, 0.00s elapsed
Initiating NSE at 16:17
Completed NSE at 16:17, 0.00s elapsed
Initiating NSE at 16:17
Completed NSE at 16:17, 0.00s elapsed
Initiating ARP Ping Scan at 16:17
Scanning 192.168.0.91 [1 port]
Completed ARP Ping Scan at 16:17, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:17
Completed Parallel DNS resolution of 1 host. at 16:17, 0.06s elapsed
Initiating SYN Stealth Scan at 16:17
Scanning 192.168.0.91 [1000 ports]
Discovered open port 135/tcp on 192.168.0.91
Discovered open port 3389/tcp on 192.168.0.91
Discovered open port 80/tcp on 192.168.0.91
Discovered open port 139/tcp on 192.168.0.91
Discovered open port 443/tcp on 192.168.0.91
Discovered open port 445/tcp on 192.168.0.91
Discovered open port 8080/tcp on 192.168.0.91
Discovered open port 2001/tcp on 192.168.0.91
Discovered open port 2103/tcp on 192.168.0.91
Discovered open port 8009/tcp on 192.168.0.91
Discovered open port 10010/tcp on 192.168.0.91
Discovered open port 5500/tcp on 192.168.0.91
Discovered open port 2105/tcp on 192.168.0.91
Discovered open port 2111/tcp on 192.168.0.91
Discovered open port 1521/tcp on 192.168.0.91
Discovered open port 5666/tcp on 192.168.0.91
Completed SYN Stealth Scan at 16:17, 1.28s elapsed (1000 total ports)
Initiating Service scan at 16:17
Scanning 16 services on 192.168.0.91
Completed Service scan at 16:20, 156.38s elapsed (16 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.91
NSE: Script scanning 192.168.0.91.
Initiating NSE at 16:20
Completed NSE at 16:20, 31.20s elapsed
Initiating NSE at 16:20
Completed NSE at 16:20, 1.17s elapsed
Initiating NSE at 16:20
Completed NSE at 16:20, 0.01s elapsed
Nmap scan report for 192.168.0.91
Host is up (0.00066s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION

```


Fuente: Análisis aplicativo Nmap

En la pestaña puertos/servidores se observa un recopilatorio de todos los puertos abiertos, el número de puerto, protocolo, estado, servicio, dependiendo del tipo de escaneo que realicemos, muestra más o menos puertos.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

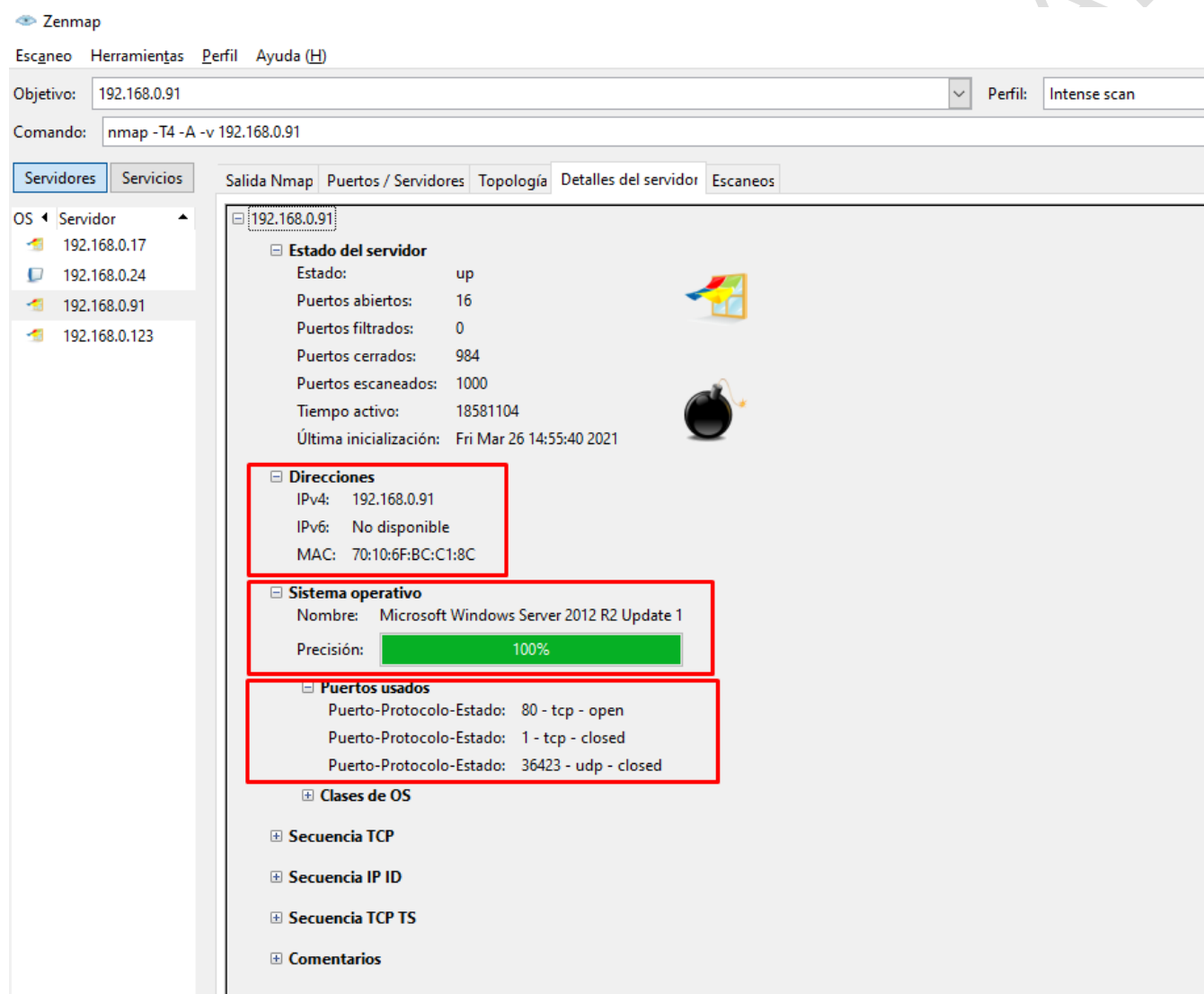
“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”



	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	<b>Código:</b> MAG-GIT-AS-IF-001
	<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 43 de 62

El equipo escaneado se puede ver en la pestaña Detalles del servidor donde se encuentra cada uno de los datos correspondientes al mismo.

Ilustración 3 – Detalles del servidor- HP Prolaint DL 180 IMÁGENES DIAGNOSTICAS



**Estado del servidor**  
Estado: up  
Puertos abiertos: 16  
Puertos filtrados: 0  
Puertos cerrados: 984  
Puertos escaneados: 1000  
Tiempo activo: 18581104  
Última inicialización: Fri Mar 26 14:55:40 2021

**Direcciones**  
IPv4: 192.168.0.91  
IPv6: No disponible  
MAC: 70:10:6F:BC:C1:8C


**Sistema operativo**  
Nombre: Microsoft Windows Server 2012 R2 Update 1  
Precisión: 100%

**Puertos usados**  
Puerto-Protocolo-Estado: 80 - tcp - open  
Puerto-Protocolo-Estado: 1 - tcp - closed  
Puerto-Protocolo-Estado: 36423 - udp - closed

Fuente: Análisis aplicativo Nmap

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

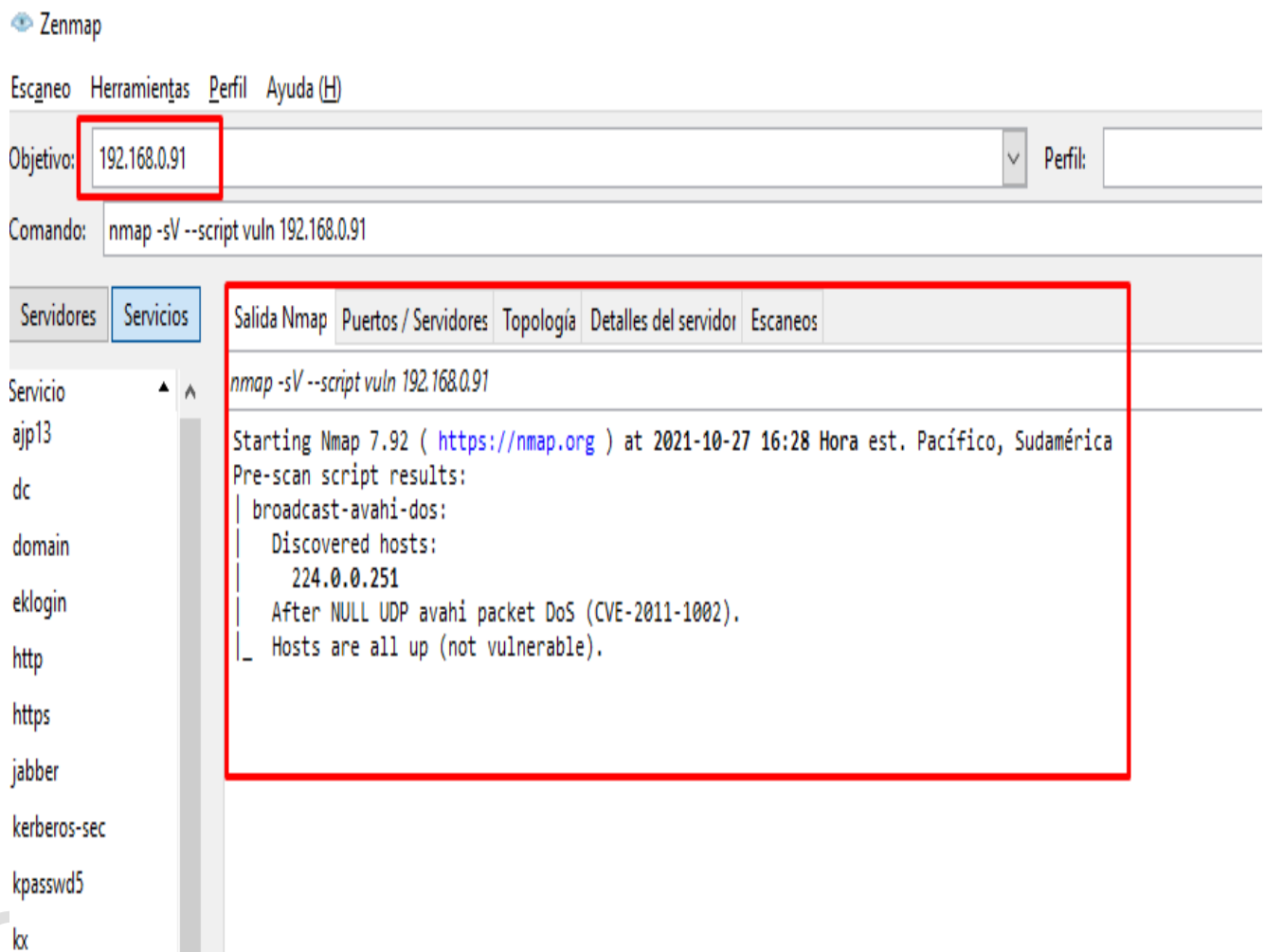
“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 44 de 62

En la ilustración 21 se evidencia vulnerabilidades del servidor del servidor 192.168.0.91 identificadas con el aplicativo Nmap, para el escaneo de vulnerabilidades se utiliza el *scriptVuln*.

Ilustración 4– Escaneo de vulnerabilidades - HP Prolaint DL 180 IMÁGENES DIAGNOSTICAS

No se encontró ninguna vulnerabilidad.



The screenshot shows the Zenmap interface. The 'Objetivo' field contains '192.168.0.91'. The 'Comando' field contains 'nmap -sV --script vuln 192.168.0.91'. The 'Salida Nmap' tab is selected, showing the following output:

```
nmap -sV --script vuln 192.168.0.91
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-27 16:28 Hora est. Pacífico, Sudamérica
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
```

Fuente: Análisis aplicativo Nmap

El siguiente es el diagrama de red generado a través del aplicativo Nmap

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*


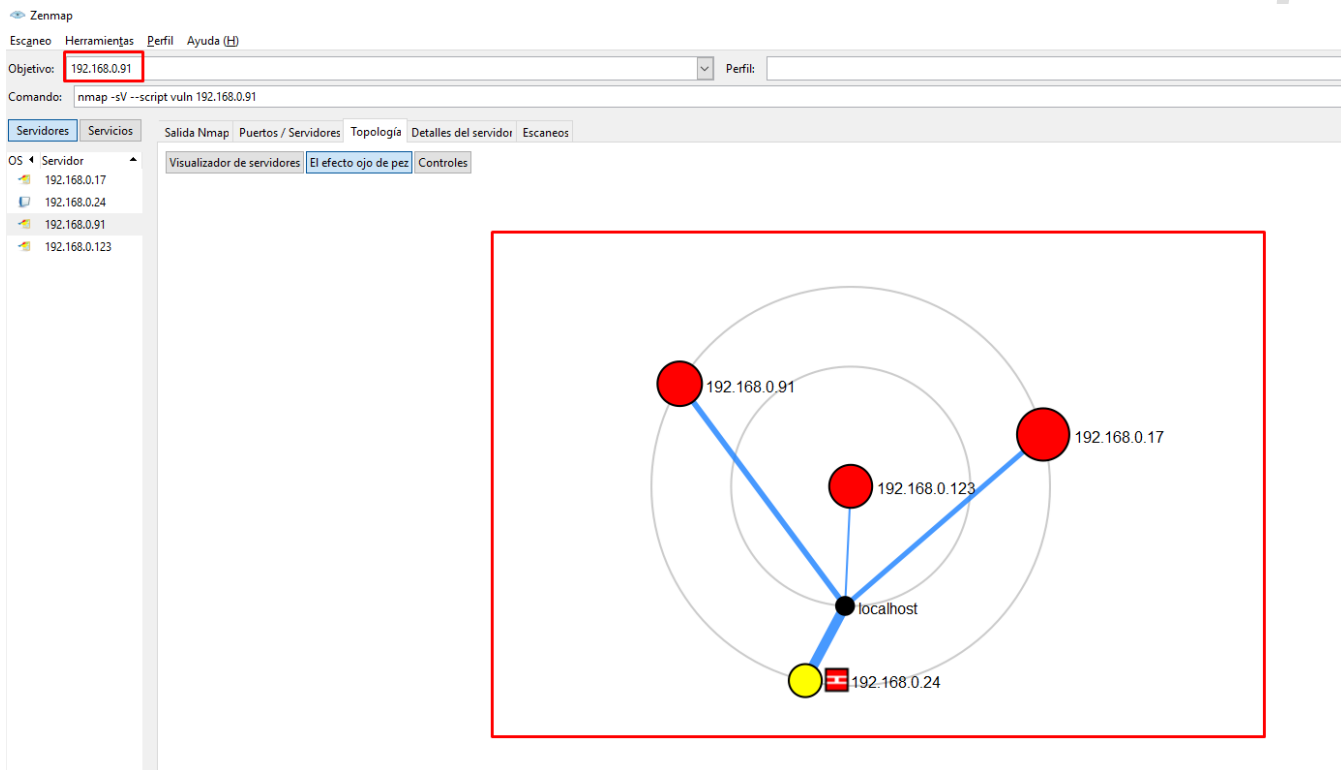
	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 45 de 62
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>		

Ilustración 1 – Diagrama e Red generado por Nmap




Fuente: Análisis aplicativo Nmap

- Vulnerabilidad de Información: con una puntuación de 0 (impacto mínimo).
- Baja: la vulnerabilidad es etiquetada como gravedad "Bajo" si tiene una puntuación base CVSS de 0.0 a 3.9.
- Medio: la vulnerabilidad es etiquetada como gravedad "Medio" si tiene una puntuación base CVSS de 4.0 a 6.9.
- Alta: la vulnerabilidad es etiquetada como gravedad "Alta" si tiene una puntuación base CVSS de 7.0 a 9.9.
- Crítica: la vulnerabilidad es etiquetada como Crítica si tiene una puntuación base CVSS de 10.

*"Hospital Humanizado y Seguro es Nuestro Compromiso"*

"Documento no valido en medio impreso sin la identificación de Marca de Agua "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital"

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 46 de 62

### 6.3 ANÁLISIS DE RIESGOS

#### CARACTERIZACIÓN E IDENTIFICACION DE AMENAZAS

En este apartado se identifican las amenazas a que están expuestos los activos de la empresa, para ello se utiliza la siguiente clasificación:

- |                                |  |
|--------------------------------|--|
| <b>(A) Ataque intencionado</b> | <b>(E) Errores y fallos no intencionados</b> |
| <b>(I) Origen industrial</b>   | <b>(N) Desastre natural</b>                  |

Tabla 1 - Análisis de Riesgos


ACTIVO	AMENAZAS
<b>Internet</b>	(A.10) Acceso no autorizado (E.8) Uso no controlado (E.8) Fallas en los servicios de comunicación
<b>Backup BD DGH</b>	(E.9) Averías de origen físico y/o lógico (E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización (A.7) Suplantación de usuarios
<b>DINÁMICA GERENCIAL DGH</b>	(E.6) Fallas en la configuración y parámetros (E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización (A.7) Suplantación de usuarios

Tabla. 2

ACTIVO	AMENAZA
<b>DGH.NET</b>	<b>(A.4) Accesos no autorizados, (A.3) Modificación de la información, (N.4) Desastres naturales (N.2) Daño por condiciones ambientales inadecuadas</b>

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 47 de 62


<b>SQL SERVER</b>	(E.6) Inadecuada configuración (A.7) Accesos no autorizados (I.4) Averías lógicas y físicas
<b>OUTLOOK</b>	(A.7) Difusión de software dañino (A.6) Filtrado de información
<b>PAQUETE OFFICE</b>	(I.3) Averías de origen lógico (A.6) Vulnerabilidades del programa
<b>SITIO WEB</b>	(A.7) Difusión de software dañino (A.7) Acceso de terceros al sistema

Tabla 3.

<b>ACTIVO</b>	<b>AMENAZA</b>
<b>Informes Medios Magnéticos</b>	(D.4) Daños por condiciones ambientales inadecuadas (A.5) Accesos no autorizados (E.4) Fallas en el almacenamiento (A.3) Alteración de la información
<b>Historia Jurídica de Pacientes Inimputables</b>	(D.4) Daños por condiciones ambientales inadecuadas (A.5) Accesos no autorizados (E.4) Fallas en el almacenamiento (A.3) Alteración de la información
<b>Contratos</b>	(D.4) Daños por condiciones ambientales inadecuadas (A.5) Accesos no autorizados (E.4) Fallas en el almacenamiento (A.3) Alteración de la información
<b>Acciones legales</b>	(D.4) Daños por condiciones ambientales inadecuadas (A.5) Accesos no autorizados (E.4) Fallas en el almacenamiento (A.3) Alteración de la información

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 48 de 62

<b>Equipos de cómputo - Escritorio</b>	(E.6) Caída del sistema por agotamiento del recurso. (E.7) Privilegios de acceso inadecuados o abuso de estos (E.3) Averías de origen físico y lógico (D.4) Daños por agua, fuego (D.4) Desastres naturales
--	---

Tabla 4.

ACTIVO	AMENAZA
<b>HP PROLIANT DL 180 DGH</b>	(D.4) Daño físico por inundaciones (D.4) Daño físico por fuego, (D.4) Desastres naturales (E.3) Condiciones ambientales inadecuadas (E.4) Errores en la administración (A.4) Accesos no autorizados
<b>HP PROLIANT DL 180 DHCP</b>	(D.4) Daño físico por inundaciones (D.4) Daño físico por fuego (D.4) Desastres naturales (E.3) Condiciones ambientales inadecuadas (E.4) Errores en la administración (A.4) Accesos no autorizados (E.4) Manipulación inadecuada del hardware

Fuente: Plataforma Documental HDSAP


## 7. SALVAGUARDAS

### 7.1 CARACTERIZACIÓN DE LAS SALVAGUARDAS

En este ítem se definen las medidas que se implementan para reducir el riesgo. Son aquellas metodologías, políticas, procedimientos y/o elementos que deben adoptarse para que la empresa se encuentre con una protección razonable para sus activos de información.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 49 de 62

A continuación, se hace una descripción de las salvaguardas establecidas por la empresa para la protección de sus activos, identificando y valorando las mismas.

### Protección general de los activos

Propias de todos los activos, se identifican las salvaguardas que son transversales y que aplican independientemente del activo que se trate.

### Autorización de Acceso


Hace referencia a la restricción que se implementa para el acceso tanto en datos, servicios, aplicaciones, equipos, redes y soporte de información. Se controla el personal que tiene acceso a estos medios y, el alcance que se le permite en cada uno de ellos. Con esto se protege la integridad y confidencialidad.

Este se enfoca en la protección de las amenazas:

- Acceso no autorizado
- Suplantación de usuarios
- Cambios en la parametrización y en la información
- Modificación de la información
- Filtrado de información
- Acceso de terceros al sistema
- Errores en la administración
- Alteración de la información
- Privilegios de acceso inadecuados o abuso de los mismos

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 50 de 62

### Filtración contra códigos maliciosos

Hace referencia a que se pongan en marcha de manera controlada las herramientas que posee la empresa para detectar los códigos maliciosos que quieran ser incluidos en los sistemas. Mantener en constante actualización, para contar con lo último en códigos de protección. Esto solo aplica sobre el software, por lo que debe mantenerse actualizado, tanto la herramienta antivirus como el sistema de defensa y arranque del sistema. Asegura la confidencialidad y disponibilidad de la información.

Esta salvaguarda protege contra las amenazas de:

- Vulnerabilidad en el programa
- Errores en la actualización
- Accesos no autorizados
- Difusión de software dañino
- Filtrado de información
- Vulnerabilidades del programa
- Acceso de terceros al sistema
- Fallas en las actualizaciones de seguridad

### Protección de instalación de software y aplicaciones


La ESE Hospital Departamental San Antonio de Padua, con su política de seguridad Digital, establece mejores controles para restringir el uso de software no autorizado por la empresa y la descarga de aplicaciones que pueden llegar a ser potencialmente peligrosas para los sistemas de información. Se asegura así la confidencialidad e integridad.

Esto exige que se lleve estricto control de las actualizaciones del sistema, la persona responsable de esto y los tiempos en que se realiza.

Esta salvaguarda apunta a las siguientes amenazas:

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 51 de 62

- Acceso no autorizado
- Uso no controlado
- Errores en la actualización
- Difusión de software dañino
- Filtrado de información
- Acceso de terceros al sistema
- Fallas en las actualizaciones
- Daños lógicos y/o físicos
- Fallas en las actualizaciones de seguridad

### Protección de equipos

Se debe implementar y aplicar los perfiles para el ingreso a los equipos, protección física de los mismos y uso de medios extraíbles. Una herramienta que permite configurar esto es el directorio activo, que puede ser una opción para el control con políticas aplicables a todos los equipos que deben incluirse en la red. Con esto se protege la integridad, confidencialidad y autenticidad en los activos de información.

Esta salvaguarda cubre las amenazas de:


- Acceso no autorizado
- Errores en la administración

### Protección de comunicaciones

La ESE Hospital Departamental San Antonio de Padua, debe robustecer el control sobre la red que administra sus sistemas de información, implementando perfiles, haciendo seguimiento al uso de la red, controlando IP de conexión para cada usuario o grupo de usuarios. Para el

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 52 de 62

acceso a internet se debe garantizar un control de filtrado, configurar navegadores, restringir descargas, monitorear tráfico, instalar anti-spyware y controlar dispositivos que permitan navegación.

Con esto se controla la autenticidad, confidencialidad e integridad y se hace frente a la amenaza de:

- Accesos no autorizados
- Uso no controlado
- Difusión de software dañino

### Protección física


Todos los equipos y herramientas (incluidos servidores, switch y demás) deben tener una protección no solo contra el acceso de terceros, sino contra las condiciones del medio en el que se encuentran o instalan. Por eso se recomienda validar las condiciones locativas, la seguridad física de las instalaciones y establecer la metodología para el ingreso y salida del personal, en función de validar que la información permanezca en la empresa.

Con esto se guarda la confidencialidad de la información y se cubren las amenazas de:

- Averías de origen físico y/o lógico
- Accesos no autorizados
- Daño por condiciones ambientales inadecuadas
- Averías lógicas y físicas
- Acceso de terceros al sistema
- Daño físico por inundaciones
- Daño físico por fuego
- Daño por agua

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 53 de 62

- Daño por fuego

### Protección de instalaciones

Disponer de norma de seguridad para las instalaciones, áreas específicas para la custodia de equipos y archivos digitales y físicos, protección perimetral.

Este ítem, hace frente a las amenazas de:

- Acceso no autorizado
- Acceso de terceros al sistema

### Mantenimientos

No solo se debe velar por el mantenimiento físico de las instalaciones, se debe implementar plan y cronograma para el mantenimiento lógico de los sistemas de información, es decir mantener las aplicaciones actualizadas, los equipos y servidores en las capacidades que deben estar acordes a las actividades que se realizan.

Con esto la empresa cubre las amenazas de:

- Fallas en la configuración y parámetros
- Desastres naturales
- Averías lógicas y físicas
- Caída del sistema por agotamiento del recurso.

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*


	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 54 de 62

Tabla 1 - Salvaguardas

ACTIVO	AMENAZAS	SALVAGUARDAS
<b>Internet</b>	(A.10) Acceso no autorizado (E.8) Uso no controlado (E.8) Fallas en los navegadores	Control de acceso lógico y físico  Dispositivos de seguridad perimetral.

Tabla 2


ACTIVO	AMENAZA	SALVAGUARDAS
<b>Backup BD DGH</b>	(E.9) Averías de origen físico y/o lógico (E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización	Proceso de gestión de cambios documentado Plan de contingencia documentado y actualizado
<b>APLICATIVO DG</b>	(A.7) Suplantación de usuarios	Control de acceso lógico y físico
<b>Dinámica Gerencial DGH</b>	(E.9) Averías de origen físico y/o lógico (E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización	Proceso de gestión de cambios documentado Plan de contingencia documentado y actualizado

Tabla 3

ACTIVO	AMENAZA	SALVAGUARDA
<b>Switches</b>	(I.4) Fallas en conexión (E.4) Fallas en configuración (A.5) Acceso no autorizado (I.4) Daño lógicos y/o físicos	Consola de administración configurada.  Manual de configuraciones.  Control de acceso lógico y físico  Plan de contingencia de TI.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

 <p>E.S.E. Hospital Departamental San Antonio de Padua LA PLATA</p>	<b>EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 26/04/2024
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 02
		<b>Página No.</b> 55 de 62


	(D.3) Daño por agua	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.3) Daño por fuego	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
<b>Firewall Físico (Sonicwall)</b>	(E.4) Fallas en las actualizaciones de seguridad (E.4) Condiciones ambientales inadecuadas	Backup periódico de configuración.  Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
<b>Servidor de almacenamiento y DHCP</b>	(D.4) Daño físico por inundaciones  (D.4) Daño físico por fuego  (D.4) Desastres naturales (E.3) Condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia. Sensores ambientales (humo, humedad y temperatura), Plan de contingencia. Sensores ambientales (humo, humedad y temperatura), Plan de contingencia. Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	<b>(A.4) Accesos no autorizados</b>	Control de acceso lógico y físico
	<b>(E.4) Manipulación inadecuada del hardware</b>	Plan de contingencia documentado y actualizado.

## 8. POLÍTICAS Y ESTRATEGIAS

De acuerdo con la situación actual del Hospital Departamental San Antonio de Padua, y en consecuencia del análisis de riesgos y las salvaguardas propuestas se implementan una serie de políticas Institucionales y estrategias con el fin de mitigar el riesgo informático, optimizar los recursos informáticos y reducir el impacto de la materialización de las amenazas identificadas

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>INFORME DE EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 07/09/2021
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 01
		<b>Página No.</b> 56 de 62

del Hospital Departamental San Antonio de Padua. Estas estrategias hacen parte integral del presente proyecto y se presentan como anexos:

## 8.1 INVENTARIO DE ACTIVOS

Este inventario contiene la información de los activos informáticos de la Institución asignándole un identificador, responsable y criticidad del activo, este nos permite catalogar de manera ordenada y completa la información.

## 8.2 PETI, PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN


Este instrumento se utiliza para expresar la Estrategia de TI. Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico. El PETI hace parte integral de la estrategia de la institución. Cada vez que una entidad hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI. ((Ministerio de Tecnologías de la Información y las Comunicaciones)

## 8.3 POLÍTICA DE SEGURIDAD DIGITAL DEL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA

Bajo la cual el Hospital Departamental San Antonio de Padua, reconoce la importancia estratégica de la información y los sistemas de información y por lo cual es importante generar estrategias que permitan garantizar la confidencialidad, disponibilidad e integridad de la información, como herramienta que aporte a la prestación de servicios de manera segura y confiable.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>INFORME DE EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 07/09/2021
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 01
		<b>Página No.</b> 57 de 62

#### **8.4 MANUAL DE USO DE LOS RECURSOS INFORMÁTICOS**

Este manual brinda a los clientes internos una guía para el manejo de los recursos informáticos en su labor diaria, propone el autocontrol como base fundamental para la optimización de recursos y mitigación de los riesgos asociados al factor humano, incluye la normatividad que rige a los empleados públicos y las directrices aprobadas por la dirección en cuanto a sanciones por falta de cumplimiento del manual.

#### **8.5 MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS**

Se establece el proceso y los procedimientos con los que se debe llevar a cabo el mantenimiento preventivo y correctivo de equipos de cómputo tales como: computadores (CPU, monitor, teclado y mouse), Impresoras, Scanner, Servidores, Swicht y UPS.


#### **8.6 PLAN DE CONTINGENCIA DE FALLOS DEL SISTEMA O PERDIDA DE DATOS.**

Se establece las medidas a tomar referente a las decisiones correspondientes de los problemas o fallos que se lleguen a presentar en la ESE Hospital Departamental San Antonio de Padua.

Ver anexo No. 6 PLAN DE CONTINGENCIA DE FALLOS DEL SISTEMA O PERDIDA DE DATOS

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>INFORME DE EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 08/08/2021
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 01
		<b>Página No.</b> 58 de 62

## 10. CONCLUSIONES

Uno de los principales retos a los que se enfrentan las entidades del gobierno en la actualidad es controlar la creciente oleada de ataques informáticos, más cuando los datos del negocio están orientados al sector salud, donde el activo de información más sensible es la historia clínica del paciente, por ende, la identificación de amenazas, vulnerabilidades y riesgos que puedan atentar contra la confidencialidad, integridad y disponibilidad de todos los activos de información, se convierte en una estrategia inicial para el establecimiento de controles que hagan frente a los *ciber* ataques.

Realizar un levantamiento exhaustivo de información de cada uno de los activos, permite documentar un inventario completo de activos de información del Hospital San Antonio de Padua, así como también identificar características importantes que fueron evaluadas en el proceso de gestión del riesgo, bajo la metodología.

Durante la ejecución de los diferentes escaneos y procedimientos de análisis de riesgos no se logró identificar vulnerabilidades críticas distribuidas en tres activos de información más sensibles de la entidad como son servidores de aplicaciones y de servicios de red, cuya importancia en la operación de la infraestructura del Hospital Departamental San Antonio de Padua, se debe seguir realizando una intervención oportuna a los procesos tecnológicos.

La gestión del riesgo bajo la metodología utilizada en el desarrollo de este trabajo permite analizar los riesgos que soportan los sistemas de información y realizar las recomendaciones de las medidas que se deben adoptar para conocer, prevenir, impedir, reducir o controlar los riesgos encontrados, realizar un análisis sobre sus principales elementos los cuales define como activo, amenaza, vulnerabilidades, impacto, riesgo y salvaguarda.

***“Hospital Humanizado y Seguro es Nuestro Compromiso”***

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*



**INFORME DE EVALUACION DE VULNERABILIDADES,  
AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL  
DEPARTAMENTAL SAN ANTONIO DE PADUA**

**EMPRESA SOCIAL DEL ESTADO  
HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA  
LA PLATA HUILA  
PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA**

Fecha: 08/08/2023

Código: MAG-GIT-AS-IF-001

Versión: 01

Página No. 59 de 62

## 11. RECOMENDACIONES

Una vez la Institución tome conciencia desde sus directivos hasta sus clientes internos, de la importancia de la información, no solo como parte activo informático, si no como parte fundamental para el crecimiento y efectividad de los procesos, es mucho más fácil la procura de la integridad, confidencialidad y disponibilidad de la información, más cuando gran parte del procesamiento de datos está dado por sistemas informáticos, como lo son computadores, redes, servidores y otros dispositivos que no manejados adecuadamente pueden poner en riesgo la institución.

Para la continuidad del sistema de gestión de seguridad informática dentro de la institución se brindan las siguientes recomendaciones:

- Actualización tecnológica

Establecer un plan de actualización tecnológico para los activos de información más sensibles como son servidores de aplicaciones y de servicios de red, equipos de cómputo, el cual aborde principalmente las vulnerabilidades más críticas evidenciadas en el presente trabajo.

- Capacitación


Brindar capacitación al área de Sistemas de información, manteniendo actualizados sobre últimas tecnologías, ataques y mecanismos de prevención, igualmente normatividad vigente.

- Auditoria internas

Realizar auditorías internas semestrales, con el fin de evaluar el cumplimiento de las políticas, procesos y procedimientos implementados del sistema de gestión de seguridad Informática.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”

	<b>INFORME DE EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 08/08/2021
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	<b>Versión:</b> 01
		<b>Página No.</b> 60 de 62
<b>PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>		

- Certificación de la norma ISO 27001

El proceso de Certificación con la norma ISO 27001:2013, brindará al Hospital Departamental San Antonio de Padua protección de los datos a clientes internos y externos, de igual manera genera una buena imagen corporativa frente a sus partes interesadas que en este caso son pacientes, empresas administradoras de planes de beneficios, entes gubernamentales y funcionarios, donde se logra demostrar el compromiso con la seguridad de la información, reduciendo el riesgo informático, optimizando los recursos y logrando mejorar el rendimiento de los procesos.

## BIBLIOGRAFÍA

GOBIERNO DE COLOMBIA. FUNCIÓN PÚBLICA Sistemas de Información: Modelo Integrado de Planeación y Gestión MIPG. Santa Fe de Bogotá. 2017

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN.  
Documentación. Bogotá: ICONTEC, 1995. (NTC 1487)

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. 17 de febrero de 2016.  
Bogotá: ICONTEC. NTC 6166

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT:  
Versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. Madrid, octubre de 2012

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT: versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. Madrid, octubre de 2012.

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*



**INFORME DE EVALUACION DE VULNERABILIDADES,  
AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL  
DEPARTAMENTAL SAN ANTONIO DE PADUA**

**EMPRESA SOCIAL DEL ESTADO  
HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA  
LA PLATA HUILA  
PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA**

Fecha: 08/08/2023

Código: MAG-GIT-AS-IF-001

Versión: 01

Página No. 61 de 62

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT: versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas. Ministerio de Hacienda y Administraciones

Públicas Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. Madrid, octubre de 2012

National Institute of Standards and Technology, U.S. Department of commerce, [sitio web]. USA; [Consultado: 30 de abril de 2020]. Disponible en: <https://nvd.nist.gov/vuln>.


The MITRE Corporation. Agosto 19 2020. CVE, Common Vulnerabilities and Exposures. U.S. Department of Homeland Security. [sitio web]. USA; [Consultado: 22 de mayo de 2020]. Disponible desde Internet en: <https://cve.mitre.org/>

## 12. ANEXOS

- A. Inventario de Activos
- B. PETI, Plan estratégico de tecnologías de la Información
- C. Política de Seguridad Digital del Hospital Departamental San Antonio de Padua.
- D. Plan de Seguridad de la Información y Uso de los Recursos Informáticos
- E. Mantenimiento preventivo y correctivo de equipos de cómputo
- F. Plan de contingencia de fallos o perdida de datos

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

*“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”*

	<b>INFORME DE EVALUACION DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Fecha:</b> 08/08/2021
		<b>Código:</b> MAG-GIT-AS-IF-001
	<b>EMPRESA SOCIAL DEL ESTADO HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍA</b>	<b>Versión:</b> 01
		<b>Página No.</b> 62 de 62

### CONTROL DE REVISIONES

VERSIÓN	FECHA	COMENTARIO
01	07/09/2021	Elaboración Primera Versión
02	26/04/2024	Elaboración Segunda Versión

Elaborado por: <b>Nombre: EDWIN FABIAN CASTRO QUINTERO</b> <b>Cargo:</b> Ingeniero de Sistemas  <b>Firma:</b>	<b>Fecha:</b> 7/09/2021
Actualizado por: <b>Nombre: EDWIN FABIAN CASTRO QUINTERO</b> <b>Cargo:</b> Ingeniero de Sistemas  <b>Firma:</b>	<b>Fecha:</b> 30/11/2023
Revisado por: <b>Nombre: JOHN DAVID VILLA</b> <b>Cargo:</b> Apoyo Técnico DGH  <b>Firma:</b>	<b>Fecha:</b> 15/12/2023
Aprobado por: <b>Nombre: GLADYS DURAN BORRERO</b> <b>Cargo:</b> Gerente  <b>Firma:</b>	<b>Fecha:</b> 22/12/2023

*“Hospital Humanizado y Seguro es Nuestro Compromiso”*

“Documento no valido en medio impreso sin la identificación de Marca de Agua “Documento Controlado” Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital”