



**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y  
PRIVACIDAD DE LA INFORMACION**

**2023**

**MAURICIO ANTONIO TORO ZAPATA**

**GERENTE**

## Tabla de contenido

INTRODUCCIÓN .....	2
OBJETIVOS .....	2
OBJETIVO GENERAL.....	2
OBJETIVOS ESPECÍFICOS.....	3
ALCANCE.....	3
MARCO CONCEPTUAL .....	3
DESCRIPCIÓN DEL PLAN .....	5
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN.....	6
Primarios .....	6
De Soporte.....	6
IDENTIFICACIÓN DE RIESGO .....	7
Descripción de Causas.....	8
Consecuencias:.....	9
ELABORACIÓN DEL PLAN E INTERPRETACIÓN.....	9
Flujo del proceso .....	9
Infraestructura Data Center .....	9
INFRAESTRUCTURA TI.....	14
Servidores.....	14
Redes & Telecomunicaciones.....	15
Seguridad Electrónica CCTV .....	16
Potencia y electricidad .....	17
REFERENCIAS.....	18

## **INTRODUCCIÓN**

La Seguridad de la Información, según ISO 27001, describe la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan; hoy en día la gran mayoría de las entidades cuenta con un sistema de información y reconoce la importancia que esta tiene para su funcionamiento y como esta debe estar adecuadamente identificada y protegida.

La E.S.E Hospital la Merced es una entidad proveedora de gran cantidad de información tanto magnética como física, la cual se encuentra en continuo procesamiento para el reporte de diferentes informes tanto internos como externos, hecho que implica un riesgo a la negligente manipulación de la información o a la pérdida de la misma, lo que podría traer problemas económicos, legales y/o administrativos por lo cual este documento busca establecer una línea de trabajo que permita a la entidad sortear los riesgos a la cual está expuesta y lograr que su información este segura.

Por lo anterior es fundamental que la E.S.E Hospital la Merced vincule el plan de tratamiento de riesgos de seguridad y privacidad de la información en cumplimiento al decreto 612 de 2018, como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, íntegra y disponible.

## **OBJETIVOS**

### **OBJETIVO GENERAL**

Elaborar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E Hospital la Merced; el cual sea una herramienta que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información.

## **OBJETIVOS ESPECÍFICOS**

Diagnosticar la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información de la E.S.E Hospital la Merced

Plantear estrategias para el control, minimización y protección contra el riesgo de pérdida y/o privacidad de la información de la E.S.E Hospital la Merced

Mejorar el sistema de Seguridad y Privacidad de la Información con el fin de que las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad; de tal forma que la prestación de servicios integrales de salud sea satisfactoria a los usuarios con calidad técnica, científica humana y oportuna.

Proteger los activos informáticos mediante la implementación de acciones de mitigación frente al riesgo.

## **ALCANCE**

El Plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información física y magnética de la E.S.E Hospital la Merced.

## **MARCO CONCEPTUAL**

**Riesgo:** situación vulnerable a la que no se está exento que puede ocasionar pérdida o daños en diferente magnitud en la información de una entidad.

**Riesgo Inherente:** Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

**Riesgo Residual:** Nivel de riesgo que permanece tras el tratamiento del mismo o nivel resultante del riesgo después de aplicar los controles.

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

**Activo de información:** información que tenga valor para la organización.

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización

**Análisis de Riesgo:** Proceso para formular recomendaciones o respuestas ante un nivel de riesgo.

**Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

**SGSI:** Sistema de Gestión de Seguridad de la Información.

**Plan de tratamiento de riesgos:** Documento que estipula las diferentes acciones para gestionar los riesgos de seguridad de la información inaceptables e instituir los controles necesarios para proteger la misma.

## **MARCO NORMATIVO**

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

**Ley 1266 (31 de diciembre 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.”

**Resolución 3564 de 2015 (31 de diciembre de 2015):** Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.

**Decreto 1078 (26 de mayo de 2015):** “Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.”

**Ley 1712 (06 de marzo de 2014):** Ley de Transparencia y acceso a la información pública nacional.

**Ley 57 (05 de julio de 1985):** “Por la cual se ordena la publicidad de los actos y documentos oficiales.”

**Acuerdo 03 (17 de febrero de 2015) del Archivo General de la Nación;** “por el cual se establecen lineamientos 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 2669 de 2011”

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

**Ley 962 (08 de julio de 2005):** "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos."

**Decreto 1747 (11 de septiembre de 2000):** "Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales".

**Ley 527 (18 de agosto de 1999):** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y Se establecen las entidades de certificación y se dictan otras disposiciones.

**Decreto Ley 2150 de (05 de diciembre de 1995):** "Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública."

**Decreto 1078 (26 de mayo de 2015):** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

## **DESCRIPCIÓN DEL PLAN**

Inicialmente se hace una breve descripción de los activos informáticos con que cuenta la E.S.E Hospital la Merced, con el fin de reconocer el tipo de información y su clasificación.

Para cada una de las amenazas se analiza las vulnerabilidades (debilidades) que se podrían presentar en el proceso. Se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de la información.

Finalmente se describen acciones que se deben llevar a cabo para solventar las problemáticas presentadas.

## **IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN**

Los activos de información se clasifican en dos tipos:

### **Primarios:**

**Procesos o subprocesos y actividades de la entidad:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización:

- información del área de facturación.
- Información de historias clínicas
- Información General: información que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados; información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo.
- Información del área de tesorería, presupuesto y contabilidad.
- Información del área de contratación.
- Información de talento humano.
- Inventarios del área de farmacia.
- Inventarios área de almacén.

Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

- Información del área de tesorería.
- Información del área de contratación.
- Información de procesos jurídicos de la entidad.

### **De Soporte**

### **Hardware:**

Consta de todos los elementos físicos que dan soporte a los procesos.

- 140 computadores propios
- 10 computadores Alquilados
- 1 servidor de aplicaciones y DHCP
- 1 servidor de Base de Datos.
- 1 servidor de Call Center
- 1 servidor de Escritorio Remoto
- 1 servidor de Correos y Centro Documental (alquilado)
- 1 servidor de Ayudas Diagnosticas (rayos x)
- 11 impresoras. Propias
- 24 impresoras Alquiladas.
- Historias clínicas de usuarios de la E.S.E Hospital la Merced.
- Contratos y documentos de legalización y pago.

**Software:**

Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos.

- Software Xenco Advanced (SXG5DB)
- SIVIGILA
- Papperless, Office, Plataformas de las Eps y Entes de Control.

**Redes:**

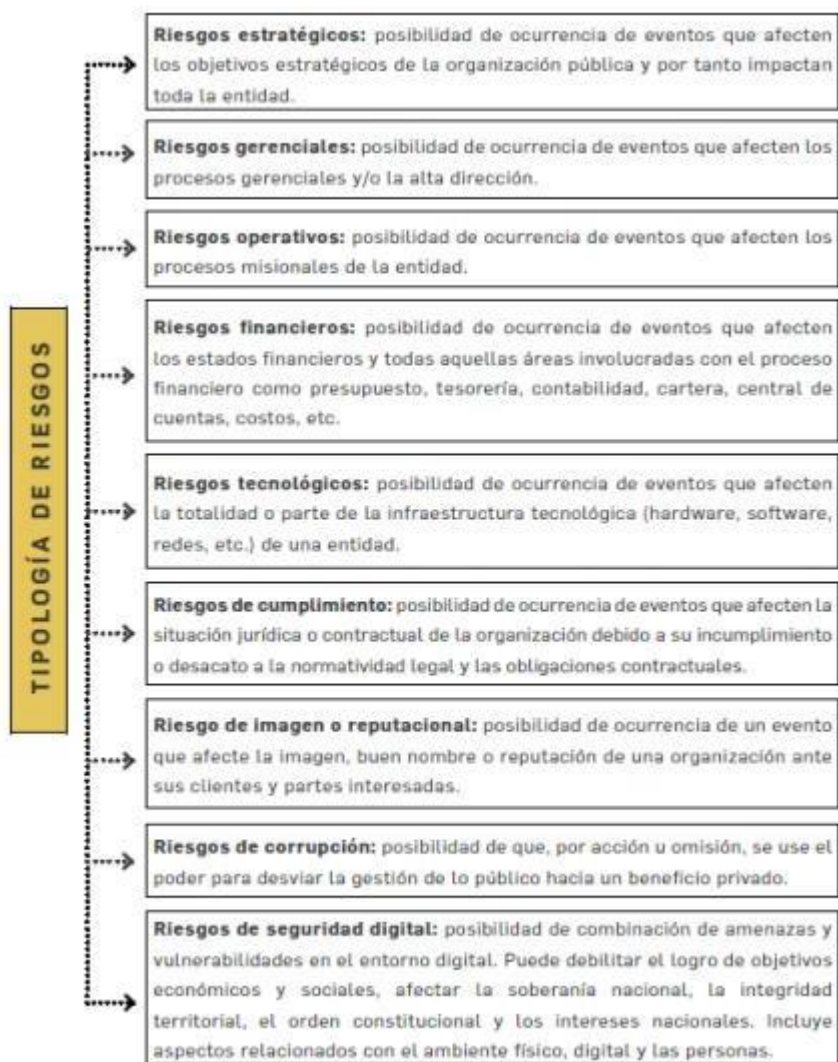
Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

**Personal:**

Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.) - Personal a cargo de elementos de cómputo de la institución, personal encargado del archivo.

**IDENTIFICACIÓN DE RIESGO**

Se identifica los tipos de riesgo y su magnitud con la que pueden afectar a la seguridad y privacidad de la información. Los tipos de riesgo se nombran a continuación:



Adaptado de guía para administración de riesgo DAFP 2018

### Descripción de Causas:

La causa es el fundamento, motivo, origen y principio de algo; con respecto al riesgo estas pueden ser generadas por personas, procesos, equipos, tiempo, entre otras que provocan un mal uso, una inadecuada acción o mal trabajo como origen de un hecho ya sea positivo o negativo.

**Consecuencias:**

Son los efectos asociados a la materialización del riesgo, estos pueden ser de diferente índole de acuerdo a la acción realizada y al perjuicio que se presente después de lo acontecido.

## ELABORACIÓN DEL PLAN E INTERPRETACIÓN

**Flujo del proceso**

Para MinTIC, los procesos de tecnología de la información están enmarcado en: “buscando organizar, estandarizar y orientar a las entidades públicas sobre la manera de gestionar la Tecnología de Información en todos los sectores y con el fin de maximizar los beneficios hacia el ciudadano y facilitar que las entidades sean más eficientes y transparentes se construyó el marco de referencia de arquitectura empresarial para la gestión de TI a partir del cual se establecen los estándares y lineamientos para la gestión de las tecnologías de la información que orientan el diseño e implementación de las arquitecturas de TI institucionales, sectoriales y territoriales”.

Se describirá los ítems a remediar, su descripción y en su defecto los prerequisites necesarios.

**Infraestructura Data Center**

Es el sitio principal donde se encuentran ubicados los equipos de plataforma de IT que apoya el CORE del negocio, es de vital importancia ejecutar las siguientes mejoras:

1. La data center se encuentra en estado deficiente, es necesario realizar reubicación de Rack, este ítem se refiere a que el rack que contiene los equipos está ubicado de costado y afecta el acceso a los puntos de red de los equipos.

**Impacto de la mejora:**

- Al reorganizar el rack y reubicarlo les permite un mejor acceso a los equipos, minimizando errores al momento de dar soporte.
- Mejora la circulación de aire frío evitando fallos por incremento de temperatura.
- Reorganizar el cableado estructurado del datacenter, los Patch Cord se encuentran completamente desordenados, fuera de las regletas organizadoras y hay cables que no tienen uso y deben retirarse, además decambiar los que sean necesarios.

- Mejora el control sobre el inventario tanto de los equipos como de los puntos de red de datos y voz.
- Minimiza la generación de estática al interior del datacenter.
- Se eliminan cables innecesarios.
- Permite dar un orden a la red de datos de acuerdo al tipo de plataforma.
- Permite agilizar los tiempos de soporte ante fallos de la red, redundando en ahorro del costo operativo.
- Ubicar en forma eficiente la posición de los equipos de comunicaciones, servidores, CCTV, etc. Debido a que los equipos están mal distribuidos en el rack principal, se debe usar el rack secundario para mover algunos puntos a este y tener un balanceo más lógico en las cargas de los racks.
- Mejora el control sobre el inventario tanto de los equipos, como de los puntos de red.
- Es fundamental que el data center TI, debe contar con aire acondicionado independiente y que maneje rangos de temperatura entre 18 a 20 grados como máximo.
- Se logra tener un mejor comportamiento de los equipos de cómputo y de red al tener la temperatura indicada por las normas.
- Permite aislar la calidad del aire que debe circular en el datacenter, minimizando costos en mantenimiento y soporte, ante fallos ocasionados por temperatura, humedad y polvo.
- Permite aislar los equipos del personal no autorizado, minimizando el riesgo por pérdida o daño en la información y daño malintencionado en los equipos de cómputo.
- Apoya los lineamientos de gobierno, respecto a la seguridad y privacidad de la información
- Se requiere seguridad independiente con Biométricos de ingreso y cámaras CCTV que controlen el ingreso de personal al sitio.
- Permite aislar los equipos del personal no autorizado, minimizando el riesgo por pérdida o daño en la información y daño malintencionado en los equipos de cómputo.
- Se tiene registro visual y lógico del personal que accede al datacenter.
- Apoya los lineamientos de gobierno, respecto a la seguridad y privacidad de la información.
- Al tener un riesgo medio de inundación es necesario contar con piso falso, en caso de anegación la altura del piso permita evitar que se afecten los equipos de IT, además de ayudar con el flujo del aire en el data center.

### **Rack Secundario Sede Alternativa**

Se encuentra un rack secundario en la sede alternativa de la entidad, este tiene un alto riesgo de ser afectado o afectar las instalaciones, por el hecho de encontrarse ubicado en las habitaciones de los médicos internos, los cuales pueden manipular con sus equipos y que en caso de corto circuito podrían afectar el total de los equipos. Es fundamental trasladar dicho rack de la zona, por normas técnicas y por control todo equipo de TI debe estar localizado en un sitio que permita tener control de los elementos y permita gestión eficiente de la información de una forma segura.

### **Impacto de la mejora:**

- Permite integrar las diferentes plataformas tecnológicas con las que cuenta el hospital en un solo sitio.
- Elimina el riesgo de conato de incendio por corto de equipos electrónicos
- Permite minimizar los costos por tiempo de soporte, al tener en un solo sitio todos los equipos.
- Minimiza riesgos por vandalismo al tener los equipos en un sitio controlado.
- Minimiza los riesgos de pérdida o daño de equipos ante una inundación, debido a que los equipos se encuentran en el piso.
- Permite mejorar el control de inventario de los puntos de red tanto de datos como de la red de cámaras.

## **INFRAESTRUCTURA TI**

### **Servidores**

La infraestructura actual de servidores en el Hospital consta de:

- 1 servidor de aplicaciones y DHCP
- 1 servidor de Base de Datos.
- 1 servidor de Call Center
- 1 servidor de Escritorio Remoto
- 1 servidor de Correos y Centro Documental (alquilado)
- 1 servidor de Ayudas Diagnosticas (rayos x)
-

<b>INVENTARIO DE SERVIDORES PROPIOS</b>			
<b>¿SERVIDOR UTILIZADO PARA?: ANDROMEDA</b> <b>Servidor HP ML 350 G9, EL CUAL MANEJA CONTROLADOR DE DOMINO, POLITICA DE SEGURIDAD, SERVIDOR DE DHCP, SERVIDOR DNS, SERVIDOR FIREWALL, SERVIDOR DE ESCRITORIO REMOTO TERMINAL SERVER, CONTAMOS CON UNA NAS THECUS, LA CUAL MANEJA LOS BUZONES DE CORREOS ELECTRONICOS, Y CARPETAS COMPARTIDAS.</b>			
Modelo	HP ML 350 G9	Aplicación/Usos Principales	Otro
Cantidad de Procesadores	2	Velocidad Procesadores	2.5 GHz
Memoria RAM	128 GB	Memoria Cache	6 MB ó más
Cantidad de Tarjetas de Red	4	Velocidad Tarjetas de Red	1 Gbps
Capacidad Disco Duro 1	1 TB	Capacidad Disco Duro 3	1 TB
Capacidad Disco Duro 2	1 TB	Capacidad Disco Duro 4	500 GB
Sistema Operativo	Windows Server 2012	Capacidad Almac. Externo	2 TB
<b>SERVIDOR UTILIZADO PARA?: ORION</b> <b>SERVIDOR DELL POWER EDGE 1950 , EL CUAL MANEJA EL ESCRITORIO REMOTO TERMINAL SERVER,</b>			
Modelo	DELL POWER EDGE 1950	Aplicación/Usos Principales	Otro
Cantidad de Procesadores	2	Velocidad Procesadores	2.5 GHz
Memoria RAM	16 GB	Memoria Cache	6 MB ó más
Cantidad de Tarjetas de Red	1	Velocidad Tarjetas de Red	1 Gbps
Capacidad Disco Duro 1	1 TB	Capacidad Disco Duro 3	
Capacidad Disco Duro 2		Capacidad Disco Duro 4	
Sistema Operativo	Windows Server 2012	Capacidad Almac. Externo	
<b>¿SERVIDOR UTILIZADO PARA?: GEDSYS (ALQUILADO)</b> <b>Servidor HP ML 350 G9, SERVIDOR DE ARCHIVO DOCUMENTAL GEDSYS, SERVIDOR DE CORREOS</b>			
Modelo	HP PROLIANT 360 9 G	Aplicación/Usos Principales	Otro
Cantidad de Procesadores	2	Velocidad Procesadores	2.5 GHz
Memoria RAM	128 GB	Memoria Cache	6 MB ó más
Cantidad de Tarjetas de Red	4	Velocidad Tarjetas de Red	1 Gbps
Capacidad Disco Duro 1	1 TB	Capacidad Disco Duro 3	1 TB
Capacidad Disco Duro 2	1 TB	Capacidad Disco Duro 4	500 GB
Sistema Operativo	Windows Server 2016	Capacidad Almac. Externo	2 TB
<b>¿SERVIDOR UTILIZADO PARA?: JUPITER</b> <b>SERVIDOR MODELO DEL SISTEMA POWEREDGE T550, SERVIDOR BASE DE DATOS SQL SERVER, BASE DE DATOS GEDSYS, ARCHIVO ADMINISTRATIVO, CONSOLA DE ANTIVIRUS NOD32,</b>			
Modelo	POWEREDGE T550	Aplicación/Usos Principales	Otro

Cantidad de Procesadores	12	Velocidad Procesadores	2.10 GHz
Memoria RAM	144 GB	Memoria Cache	6 MB ó más
Cantidad de Tarjetas de Red	4	Velocidad Tarjetas de Red	1 Gbps
Capacidad Disco Duro 1	1 TB	Capacidad Disco Duro 3	500 GB
Capacidad Disco Duro 2	1 TB	Capacidad Disco Duro 4	
Sistema Operativo	Windows Server 2016	Capacidad Almac. Externo	2 TB
<b>¿SERVIDOR UTILIZADO PARA?: ZEUS</b>			
<b>SERVIDOR DELL PROLIANT DL160 GEN9, EL CUAL MANEJA EL ESCRITORIO REMOTO TERMINAL SERVER,</b>			
Modelo	PROLIANT DL160 GEN9	Aplicación/Usó Principal	Otro
Cantidad de Procesadores	2	Velocidad Procesadores	2.5 GHz
Memoria RAM	64 GB	Memoria Cache	6 MB ó más
Cantidad de Tarjetas de Red	1	Velocidad Tarjetas de Red	1 Gbps
Capacidad Disco Duro 1	500 GB	Capacidad Disco Duro 3	
Capacidad Disco Duro 2	1 TB	Capacidad Disco Duro 4	
Sistema Operativo	Windows Server 2012	Capacidad Almac. Externo	

Equipos de cómputo con las siguientes especificaciones:

Servicio	Ambiente o área	Nombre de la dotación	Especificaciones mínimas obligatorias (EMO)
CONSULTA EXTERNA FARMACIA URGENCIAS LABORATORIO RAYOS X HOSPITALIZACION CIRUGIA PROMOCION Y PREVENCION SALUD PUBLICA ODONTOLOGIA ORTOPEDIA AREA ADMINISTRATIVA FISIOTERAPIA FACTURACION	CONSULTORIO	Equipo de cómputo	1. Tipo de chasis: All In One / todo en uno 2. Línea: Corporativa 3. Procesamiento 3.1 Procesador: Procesador Intel® Core™ i7 décima generacion de 65 W o superior; compatible Windows 10 4. Chipset: Q470 5. Memoria 5.1 RAM instalada: 16 GB RAM instalada en un solo módulo ó superior con posibilidad de incluir un segundo módulo y crecimiento máximo a 64 GB. 5.2 Tipo: DDR4 2933 Mhz 6. Almacenamiento 6.1 Disco duro: 1TB SDD 6.2 Tipo de tecnología del disco: SATA 6 Gb/s + PCIe 32 Gb/s 7. Monitor y Accesorios 7.1 Monitor integrado al equipo 7.2 WLED 7.3 Altura ajustable 7.4 Antireflejos 7.4 FHD, IPS no táctil 7.8 Tamaño: 23.8" o superior 7.9 Resolución: 1920 x 1080 a 60 Hz o superior 7.10 Tarjeta gráfica: Gráficos integrados Intel®

		<p>7.11 Cámara: Si – integrada 1080p o superior.</p> <p>7.12 Micrófono: Si – integrado al monitor</p> <p>7.13 Parlantes: Si – integrados al monitor</p> <p>7.14 Unidad de DVD: DVD RW integrada</p> <p>8. Periféricos</p> <p>8.1 Teclado: Estándar, español. De la misma marca del equipo, alámbrico USB</p> <p>8.2 Mouse Óptico: Conexión USB 2 botones y botón scroll. De la misma marca del equipo</p> <p>9. Conectividad</p> <p>9.1 Red Ethernet: integrada, 10/100/1000 RJ45, wake OnLan</p> <p>9.2 Red Inalámbrica: Interna, 802.11 AX 2x2</p> <p>10 Puertos y Slot</p> <p>10.1 Puertos USB : mínimo 4 usb 3.2 tipo A + 1 USB tipo c 3.2</p> <p>10.2 Puertos: Video adicional a través display port ó HDMI</p> <p>11 Software</p> <p>11.1 Sistema Operativo: Windows 10 Pro, 64 bits, español.</p> <p>11.2 Software de administración del equipo: Software de restauración a parámetros de fábrica</p>
--	--	--

		<p>11.3 BIOS: Propietaria y desarrollada por el fabricante</p> <p>12. Energía</p> <p>12.1 Fuente de poder: desde 120 W con eficiencia mínima del 85%</p> <p>12.2 EnergyStar 8,0 ó superior: SI</p> <p>13. Opciones de seguridad:</p> <p>13.1 TPM 2.0 Discreto.</p> <p>13.2 El equipo debe soportar restauracion de la BIOS.</p> <p>13.3 EPEAT GOLD: SI</p> <p>13.4 RoHS: SI</p> <p>14. Garantía</p> <p>14.1 Cobertura: En partes, mano de obra y sitio al equipo completo, accesorios y periféricos relacionados en estas especificaciones. El tiempo de reemplazo de las partes o del equipo se hará en un tiempo máximo de 72 horas luego de haber reportado el caso. Los repuestos son originales, nuevos y embalados en su respectivo empaque.</p> <p>14.2 Tiempo: Mínimo 5 años de Garantía certificados por el fabricante del equipo</p> <p>Servicio de generación, carga de imagen y alistamiento de las máquinas: migración de datos</p> <p>OFFICE: Office 2019 estándar on-premise</p>
--	--	---

Se cuenta con una NAS de almacenamiento y copias de seguridad siguientes características:

1. NAS THECUS de 21 Teras



2. Nombre del modelo N5810,
3. Versión 3.02.06.13

## **CPU**

- CPU1: Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
- CPU2: Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
- CPU3: Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
- CPU4: Intel(R) Celeron(R) CPU J1900 @ 1.99GHz

## **Memoria**

- Memory Size: 3844MB

## **Tarjeta de interfaz de red**

- WAN/LAN1: Intel Corporation Device 1533 (rev 03)
- LAN2: Intel Corporation Device 1533 (rev 03)

## **Bus serie universal**

- USB2.0-1: Intel Corporation Device 0f35 (rev 0e)
- USB3.0-1: Intel Corporation Device 0f35 (rev 0e)
- USB2.0-2: Device 1b21:1142
- USB3.0-2: Device 1b21:1142

## **Controladora de disco**

- SATA1: Intel Corporation Device 0f23 (rev 0e)
- SATA2: Device 1b4b:9215 (rev 11)

## **Impacto de la mejora:**

- Al ser equipos nuevos se cuenta con garantía de fabricante a 2 años, minimizando los costos de reparación y soporte.
- Mejoran los tiempos de procesamiento de aplicaciones en el hospital, redundando en una mejor calidad de servicio a los usuarios finales.
- Minimiza los tiempos de soporte, ya que se reducen los fallos por obsolescencia.
- El hospital puede crecer en nuevas aplicaciones o procesos, al contar con una buena infraestructura de servidores.
- Al contar con una solución de recuperación de desastres, se minimiza el tiempo de no-disponibilidad de los servicios informáticos del hospital, redundando en una buena imagen para el hospital.
- Al contar con una NAS en la red del hospital, tendrán accesos rápidos a datos respaldados, confiabilidad en la información debido a que el software de respaldo es de muy buena calidad en el proceso de copiado.
- Al contar con un firewall en la red, se tendrá protección perimetral desde y hacia internet de todos y cada uno de los usuarios del hospital que estén permitidos a usar los recursos de red, esto le permitirá al hospital minimizar los riesgos de pérdida de información.

## **Redes & Telecomunicaciones**

La infraestructura actual de redes y telecomunicaciones en el Hospital consta de:

Dichos equipos tienen varios riesgos tecnológicos y que deben ser mitigados:

- Obsolescencia Tecnológica
- Falta de garantía ante el fabricante
- Puertos Dañados
- Falta de capacidad para gestión remota
- Hubs instalados en los puestos de trabajo

Para mitigar dichos riesgos se propone una actualización adquiriendo nuevos equipos y determinando que los equipos anteriores serán usados para la implementación de un plan DRP (Plan de recuperación a desastres) como plataforma de respaldo ante alguna falla física, electrónica o desastre.

Se proponen equipos de red con las siguientes características:

1. 3 switches L2 (capa 2) administrables de 48 puertos y 4 puertos SFP
2. Servicios de VLAN
3. Servicios de bloqueo de puertos
4. Servicios de Fail-Over

#### **Impacto de la mejora:**

- Al ser equipos nuevos se cuenta con garantía de fabricante a 2 años, minimizando los costos de reparación y soporte.
- Mejoran los tiempos de respuesta de las aplicaciones en el hospital, redundando en una mejor calidad de servicio a los usuarios finales.
- Minimiza los tiempos de soporte, ya que se reducen los fallos por obsolescencia.
- El hospital puede crecer en nuevas aplicaciones o procesos, al contar con una buena infraestructura de Redes.
- Permite centralizar todos los equipos de red en un solo sitio, minimizando los tiempos de soporte por fallos en la red.
- Se incrementan los niveles de seguridad lógica, tanto de los equipos como los datos de usuarios y aplicaciones.
- Se eliminan los puntos de fallo por equipos instalados en cascada, al no generarse colisiones de datos en la red, obteniendo un mejor desempeño en la red.

## **Seguridad Electrónica CCTV**

El hospital cuenta actualmente con seguridad electrónica y se propone hacer ajustes en algunos puntos muertos adquiriendo cámaras para mejor protección, además de reubicar unas cuentas que no están cumpliendo con buenas normas.

### **Impacto de la mejora:**

- Mejora toda la disposición de la red de cámaras.
- Minimiza los tiempos soporte ante fallos de la red.
- Al cubrir puntos muertos mejora el cubrimiento de seguridad en el hospital.
- Permite identificar a todo el personal interno y ajeno del hospital por contar con cámaras de mejor calidad de imagen.

## **Potencia y electricidad**

El hospital cuenta actualmente con una infraestructura eléctrica completamente deficiente, no se tienen planos estructurales, ni la distribución eléctrica, por lo tanto para realizar las adecuaciones y mejora de las instalaciones eléctricas es necesario:

- Levantar planos estructurales del Hospital completamente.
- Realizar diseño del nuevo sistema eléctrico.
- Construir planos de distribución eléctrica basada en el nuevo diseño.
- Implementación de la nueva solución eléctrica.

### **Impacto de la mejora:**

- Permite identificar el estado actual de la infraestructura física del hospital.
- El hospital contará con los archivos reales con la posición, capacidad y distribución de los equipos eléctricos y de potencia.
- Se contará con una instalación eléctrica unificada de acuerdo a las normas y estándares de ingeniería eléctrica.
- Se minimizan las pérdidas de equipos por descargas eléctricas, sobrevoltajes y pérdidas de voltaje que puedan afectar el normal funcionamiento del hospital.
- Minimizan los riesgos de conato de incendio por corto circuito.
- En caso de ampliación, mejoras de zonas o nuevas construcciones, el hospital contará con la información suficiente para la toma de decisión eficiente.

- Estas mejoras deben redundar en ajuste de costos por uso indebido del sistema eléctrico.

## REFERENCIAS

1. <https://www.mintic.gov.co/portal/604/w3-propertyvalue-558.html>
2. <https://www.mintic.gov.co/portal/604/w3-propertyvalue-558.html>
3. <https://www.mintic.gov.co/portal/604/w3-propertyvalue-558.html>