

ESE HOSPITAL REGIONAL MANUELA BELTRAN SOCORRO

**PLAN DE GESTIÓN Y TRATAMIENTO DE
RIESGOS PLATAFORMA INFORMÁTICA**



Documento elaborado por Ing. RONEY ARMANDO SUAREZ – Coordinador DATIC

DATIC
2025

TABLA DE CONTENIDO

	Página
Introducción	1
Glosario	2
Objetivos	3
Alcance	4
Capítulo I – CARACTERIZACIÓN DE LOS ACTIVOS	5
1.1. IDENTIFICACIÓN DE LOS ACTIVOS	5
1.1.1. Hardware	5
1.1.2. Software	15
1.1.3. Equipos de comunicaciones	16
1.1.4. Equipamiento auxiliar	16
1.1.5. Unidades de Almacenamiento en Red	17
1.1.6. Instalaciones	17
1.1.7. Personal	17
1.2. DEPENDENCIAS ENTRE LOS ACTIVOS	18
1.2.1. Hardware	18
1.2.2. Software	18
1.3. VALORACION DE LOS ACTIVOS	19
1.3.1. Servidores	19
1.3.2. Software	22
1.3.3. Equipo de comunicaciones	22

1.3.4. Equipamiento auxiliar	23
1.3.5. Unidades de Almacenamiento en Red	23
Capítulo 2 – IDENTIFICACION DE CONTROLES EXISTENTES	24
2.1. Identificación de controles existentes	24
Capítulo 3 – IDENTIFICACION DE VULNERABILIDADES	25
Capítulo 4 – CARACTERIZACIÓN DE LAS AMENAZAS	29
4.1. IDENTIFICACIÓN DE AMENAZAS SOBRE LOS ACTIVOS	29
4.2. VALORACION DE LAS AMENAZAS	30
4.2.1. Riesgos Físicos Internos	30
4.2.2. Riesgos Físicos Externos	36
4.2.3. Riesgos Lógicos Internos	38
4.2.4. Riesgos Lógicos Externos	42
4.3. PRIORIZACION DE LOS RIESGOS	45
4.3.1. Riesgos Físicos Internos	45
4.3.2. Riesgos Físicos Externos	46
4.3.3. Riesgos Lógicos Internos	46
4.3.4. Riesgos Lógicos Externos	47
Capítulo 5. DEFINICION DE MEDIDAS PARA REDUCCION DE RIESGOS	48
5.1. DEFINICION DE MEDIDAS	48
5.1.1. Riesgos Físicos Internos	48
5.1.2. Riesgos Físicos Externos	51
5.1.3. Riesgos Lógicos Internos	51
5.1.4. Riesgos Lógicos Externos	52
6. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS	55

7. REFERENCIAS	56
----------------	----

INTRODUCCION

La plataforma informática de la ESE Hospital Regional Manuela Beltrán Socorro con su fuerte crecimiento en los últimos años y su alta integración con los diferentes procesos misionales, se ha convertido en el soporte fundamental para el desarrollo de las actividades misionales y administrativas de la empresa; por lo que garantizar la protección de la información manejada por esta y asegurar su continuidad y escalabilidad son un deber fundamental de los directivos y de la oficina DATIC; por lo anterior y en cumplimiento de lineamientos definidos por entes de control y en el marco de la estrategia nacional “Gobierno Digital”, se ha procedido a la elaboración del presente documento, cuyo objetivos principales son los de identificar los riesgos y vulnerabilidades de la plataforma informática, con el propósito de diseñar e implementar los controles y medidas tendientes a disminuir la probabilidad de ocurrencia de ataques y garantizar la continuidad del funcionamiento.

Para la construcción del presente documento se ha seleccionado la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) versión 3.0; debido a ventajas tales como:

- Su amplia documentación en español.
- Su facilidad de desarrollo e implementación para una empresa de las características de la institución.
- Su enfoque para entidades relacionadas con la administración pública.

De igual manera se usó como referencia el Modelo de Seguridad y Privacidad de MINTIC y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

GLOSARIO

Activos: Componente de un sistema de información susceptible de ser atacado con consecuencias para la organización. Incluye: información, datos, servicios, software, hardware, redes de datos, recursos físicos y recursos humanos.

Amenazas: Son cosas que les pueden pasar a los activos causando un perjuicio a la Organización

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

DATIC: Departamento de Tecnologías de la información y comunicación de la ESE.

Riesgo: Probabilidad de ocurrencia de un evento que afecte el funcionamiento de la plataforma informática.

Tratamiento de los riesgos: Proceso destinado a modificar el riesgo.

Vulnerabilidad: Probabilidad de que se desarrolle una amenaza sobre un activo generando su daño.

OBJETIVOS

1. Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación a los cuáles la plataforma informática pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.
2. Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
3. Gestionar riesgos de Seguridad y Privacidad de la información manejada en la plataforma informática de la ESE para garantizar la continuidad de la Operación.

ALCANCE

El presente plan aplica a todos los activos de información a nivel de hardware, software, redes de datos e información electrónica manejada en la plataforma informática de la ESE. Estos activos se encuentran relacionados en el Capítulo 1 de este documento.

El Plan de Gestión y Tratamiento de Riesgos tendrá en cuenta los riesgos que obtengan una calificación mayor a 6 puntos, acorde con los lineamientos definidos en el presente documento, los riesgos con calificación menor o igual a 6 puntos serán aceptados por la Entidad.

CAPITULO 1. CARACTERIZACIÓN DE LOS ACTIVOS

1.1. IDENTIFICACIÓN DE LOS ACTIVOS

1.1.1. Hardware

A continuación, se relacionan los equipos de cómputo y equipos de digitalización que hacen parte de la plataforma institucional y serán incluidos en el presente análisis de riesgos.

Servidores

Refer	Nombre Elemento	Descripción	Ubicación Actual	Responsable
12446	SERVIDOR LENOVO SR500	Intel Xeon silver 4.2 2.1Ghz 64 RAM	DATIC	PROCESO DATIC
6435	SERVIDOR HP ML350	PROCESADOR XEON 4 NUCLEOS 2.4G	DATIC	PROCESO DATIC
9583	SERVIDOR HP ML350	ML350E GEN 8 V2 E5-2404V2 BASE	DATIC	PROCESO DATIC
12744	SERVIDOR LENOVO SR250	SERVIDOR LENOVO SR250	DATIC	PROCESO DATIC
12745	SERVIDOR LENOVO SR550	SERVIDOR LENOVO SR550	DATIC	PROCESO DATIC
12746	SERVIDOR LENOVO SR550	SERVIDOR LENOVO SR550	DATIC	PROCESO DATIC
12747	SERVIDOR LENOVO SR550	SERVIDOR LENOVO SR550	DATIC	PROCESO DATIC
12748	SERVIDOR LENOVO SR550	SERVIDOR LENOVO SR550	DATIC	PROCESO DATIC
12743	SERVIDOR LENOVO SRV2	SERVIDOR LENOVO SRV2	DATIC	PROCESO DATIC

Estaciones de Trabajo

Ref.	Nombre	Ubicación	Responsable
10294	TORRE COMPUTADOR	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10298	COMPUTADOR LENOVO C260	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
10357	COMPUTADOR	VACUNACION COVID 19	ENFERMERA JEFE/ COORD DEL SERVICIO
10405	COMPUTADOR	VACUNACION	ENFERMERA JEFE/ COORD DEL SERVICIO
10406	COMPUTADOR	PUESTO DE SALUD DE PALMAS	ENFERMERA JEFE/ COORD DEL SERVICIO
10407	COMPUTADOR	PUESTO DE SALUD DEL HATO	ENFERMERA JEFE/ COORD DEL SERVICIO
10480	COMPUTADOR PORTATIL	GESTORA HOSPITALARIA	JEFE LORENA SARMIENTO GARCIA
10485	TORRE LENOVO THINKCENTRE	PUESTO DE SALUD DE PALMAS	ENFERMERA JEFE/ COORD DEL SERVICIO
10490	COMPUTADOR PORTATIL HP 450G3	GINECOBSTERICIA	ENFERMERA JEFE/ COORD DEL SERVICIO
10492	COMPUTADOR PORTATIL HP 450G3	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
10494	COMPUTADOR LENOVO AIO E73Z	GINECOBSTERICIA	ENFERMERA JEFE/ COORD DEL SERVICIO
10495	COMPUTADOR LENOVO AIO E73Z	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
10496	COMPUTADOR LENOVO AIO E73Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10497	COMPUTADOR LENOVO AIO E73Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10498	COMPUTADOR LENOVO AIO E73Z	QUIRURGICAS	ENFERMERA JEFE/ COORD DEL SERVICIO
10499	COMPUTADOR LENOVO AIO E73Z	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
10500	COMPUTADOR LENOVO AIO E73Z	QUIRURGICAS	ENFERMERA JEFE/ COORD DEL SERVICIO
10507	COMPUTADOR	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
10511	COMPUTADOR PORTATIL	LABORATORIO CLINICO	COORDINADORA LABORATORIO CLINICO
10514	COMPUTADOR	PUESTO DE SALUD DE PALMAS	ENFERMERA JEFE/ COORD DEL SERVICIO
10647	COMPUTADOR AIO LENOVO E73Z	EDUCACION MEDICA - CUARTO DE INTERNOS	COORDINADOR MEDICO INTERNOS
10648	COMPUTADOR AIO LENOVO E73Z	APOYO GESTION DE CALIDAD	COORDINADOR OFICINA CALIDAD
10649	COMPUTADOR AIO LENOVO E73Z	AUDITORIA MEDICA	COORDINADOR OFICINA CARTERA/AUDITORIA
10650	COMPUTADOR AIO LENOVO E73Z	MEDICOS HOSPITALARIOS	COORDINADOR MEDICO
10651	COMPUTADOR AIO LENOVO E73Z	AUDITORIA MEDICA	COORDINADOR OFICINA CARTERA/AUDITORIA
10652	COMPUTADOR AIO LENOVO E73Z	EDUCACION MEDICA - CUARTO DE INTERNOS	COORDINADOR MEDICO INTERNOS
10653	COMPUTADOR AIO LENOVO E73Z	AUDITORIA MEDICA	COORDINADOR OFICINA CARTERA/AUDITORIA
10654	COMPUTADOR AIO LENOVO E73Z	GESTION DE CALIDAD	COORDINADOR OFICINA CALIDAD
10655	COMPUTADOR AIO LENOVO E73Z	ESTADISTICA E HISTORIAS CLINICAS	COORDINADOR DEL SERVICIO
10656	COMPUTADOR AIO LENOVO E73Z	EDUCACION MEDICA - CUARTO DE INTERNOS	COORDINADOR MEDICO INTERNOS
10657	COMPUTADOR AIO LENOVO E73Z	GESTION DE CALIDAD	COORDINADOR OFICINA CALIDAD

PLAN DE PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS PLATAFORMA INFORMÁTICA 2025

Ref.	Nombre	Ubicación	Responsable
10799	COMPUTADOR LENOVO 310 AIO BLANCO	TRABAJO SOCIAL	TRABAJADOR SOCIAL
10800	COMPUTADOR LENOVO 310 AIO BLANCO	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
10801	SWITCH ARUBA 2920 J9728A	DATIC	PROCESO DATIC
10802	SWITCH ARUBA 2920 J9728A	DATIC	PROCESO DATIC
10803	UPS SU3000XL 3KVA	DATIC	PROCESO DATIC
10812	COMPUTADOR LENOVO AIO V510Z	GERENCIA	Dr. ROBINSON SARMIENTO GARCIA
10813	COMPUTADOR LENOVO AIO V510Z	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
10814	COMPUTADOR LENOVO AIO V510Z	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
10815	COMPUTADOR LENOVO AIO V510Z	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
10816	COMPUTADOR LENOVO AIO V510Z	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
10817	COMPUTADOR LENOVO AIO V510Z	APOYO SUBDIRECCION CIENTIFICA	APOYO PROFESIONAL SUBDIRECCION CIENTIFICA
10818	COMPUTADOR LENOVO AIO V510Z	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
10819	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10820	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10821	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10822	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10823	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10824	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10825	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10826	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10827	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10828	COMPUTADOR LENOVO AIO V510Z	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
10829	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10830	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10831	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
10886	COMPUTADOR LENOVO AIO V510Z	AUDITORIA MEDICA	COORDINADOR OFICINA CARTERA/AUDITORIA
10897	COMPUTADOR LENOVO	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	DRA JAZBLEIDY SARMIENTO
10981	COMPUTADOR LENOVO	SALUD OCUPACIONAL	PROFESIONAL SALUD OCUPACIONAL
10982	COMPUTADOR LENOVO	OFICINA JURIDICA Y CONTRATACION	PROFESIONAL OFICINA JURIDICA
10989	LENOVO V310Z ALL-IN-ONE 19.5"	SALA DE CONFERENCIAS	SERVICIO DE VIGILANCIA.
10990	LENOVO V310Z ALL-IN-ONE 19.5"	MÉDICO DE INFECCIONES	Dra. ANGELINE JAIMES
11002	COMPUTADOR LENOVO V310Z	GINECOBSTETRICIA	ENFERMERA JEFE/ COORD DEL SERVICIO
11003	COMPUTADOR LENOVO V310Z	GINECOBSTETRICIA	ENFERMERA JEFE/ COORD DEL SERVICIO

PLAN DE PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS PLATAFORMA INFORMÁTICA 2025

Ref.	Nombre	Ubicación	Responsable
11004	COMPUTADOR LENOVO V310Z	PEDIATRIA	ENFERMERA JEFE/ COORD DEL SERVICIO
11005	COMPUTADOR LENOVO V310Z	PEDIATRIA	ENFERMERA JEFE/ COORD DEL SERVICIO
11007	COMPUTADOR LENOVO V310Z	COSTOS	COORDINADOR OFICINA COSTOS
11020	CPU JANUS	PUESTO DE SALUD DEL HATO	ENFERMERA JEFE/ COORD DEL SERVICIO
11021	COMPUTADOR LENOVO V310Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
11022	COMPUTADOR LENOVO V310Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
11023	COMPUTADOR LENOVO V310Z	CONSULTA EXTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
11096	COMPUTADOR LENOVO	COORDINACIÓN DE NODOS Y TRANSPORTE	COORDINACIÓN DE NODOS Y TRANSPORTE
11121	UPS 15 KVA TRIFÁSICA	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
11157	COMPUTADOR LENOVO	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
11158	COMPUTADOR LENOVO	ESTADISTICA E HISTORIAS CLINICAS	COORDINADOR DEL SERVICIO
11160	COMPUTADOR LENOVO	REFERENCIA Y CONTRAREFERENCIA	COORDINADOR DEL SERVICIO
11161	COMPUTADOR LENOVO	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
11162	COMPUTADOR LENOVO	REFERENCIA Y CONTRAREFERENCIA	COORDINADOR DEL SERVICIO
11163	COMPUTADOR LENOVO	COSTOS	COORDINADOR OFICINA COSTOS
11164	CPU LENOVO	DATIC	PROCESO DATIC
11166	CPU LENOVO	DATIC	PROCESO DATIC
11168	CPU LENOVO	DATIC	PROCESO DATIC
11170	CPU LENOVO	DATIC	PROCESO DATIC
11172	COMPUTADOR JANUS	DATIC	PROCESO DATIC
11173	UPS FORZA	DATIC	PROCESO DATIC
11185	COMPUTADOR PORTATIL LENOVO	GERENCIA	Dr. ROBINSON SARMIENTO GARCIA
11187	COMPUTADOR LENOVO V530Z	SUBDIRECCION CIENTIFICA	DR. JUAN CARLOS PEÑA
11198	COMPUTADOR LENOVO	CONTABILIDAD	DR BLAS ARAQUE
11199	COMPUTADOR LENOVO	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
11200	COMPUTADOR LENOVO	APOYO CONTABILIDAD	DR BLAS ARAQUE
11201	COMPUTADOR LENOVO	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
11202	COMPUTADOR LENOVO	CENTRAL DE ESTERILIZACION	COORDINADOR DEL SERVICIO
11203	COMPUTADOR LENOVO	UNIDAD DE CUIDADOS INTENSIVOS NEONATALES	ENFERMERA JEFE/ COORD DEL SERVICIO
11204	COMPUTADOR LENOVO	UNIDAD DE CUIDADOS INTENSIVOS NEONATALES	ENFERMERA JEFE/ COORD DEL SERVICIO
11205	SERVIDOR DELL T30	DATIC	PROCESO DATIC
11233	CPU LENOVO	PROMOCION Y PREVENCION	PROMOCION Y PREVENCION
11235	CPU LENOVO	DEPARTAMENTO DE ENFERMERIA/ PROMOCION Y PREVENCION	JEFE DANNY LEON

PLAN DE PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS PLATAFORMA INFORMÁTICA 2025

Ref.	Nombre	Ubicación	Responsable
11293	TORRE COMPUTADOR	DATIC	PROCESO DATIC
11294	LENOVO V330	UCI ADULTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
11295	LENOVO V330	UCI ADULTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
11296	LENOVO V330	UCI ADULTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
11297	LENOVO V330	UCI ADULTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
11320	COMPUTADOR TODO EN UNO LENOVO	APOYO PROFESIONAL SUBDIRECCION	APOYO PROFESIONAL SUBDIRECCION
11542	SWITCH JH295A	DATIC	PROCESO DATIC
11543	SWITCH JG961A	DATIC	PROCESO DATIC
11544	UPS 3KVA	DATIC	PROCESO DATIC
11598	COMPUTADOR LENOVO AIO V530	OFICINA DE MERCADEO	PROFESIONAL MERCADEO
11781	COMPUTADOR HP ProOne 400G5 AiO	SECRETARIA GERENCIA	APOYO PROFESIONAL GERENCIA
11782	COMPUTADOR HP ProOne 400G5 AiO	FONOAUDIOLOGIA	DRA MARTHA NUBIA CASTAÑEDA
11783	COMPUTADOR HP ProOne 400G5 AiO	APOYO GESTION DE CALIDAD	COORDINADOR OFICINA CALIDAD
11784	COMPUTADOR HP ProOne 400G5 AiO	TALENTO HUMANO	JENNY JOHANA CELIS RIVERA
11785	COMPUTADOR HP ProOne 400G5 AiO	TESORERIA	COORDINADOR OFICINA FINANCIERA
11786	COMPUTADOR HP ProOne 400G5 AiO	CONSULTA EXTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
11787	COMPUTADOR HP ProOne 400G5 AiO	MANTENIMIENTO	COORDINADOR RECURSOS FISICOS
11788	COMPUTADOR HP ProOne 400G5 AiO	ESTADISTICA E HISTORIAS CLINICAS	COORDINADOR RECURSOS FISICOS
11789	COMPUTADOR HP ProOne 400G5 AiO	ADMINISTRACION FINANCIERA	COORDINADOR OFICINA FINANCIERA
12075	COMPUTADOR HP-200	LABORATORIO CLINICO	Coordinador Proceso Laboratorio Clínico.
12076	COMPUTADOR HP-200	LABORATORIO CLINICO	Coordinador Proceso Laboratorio Clínico.
12077	COMPUTADOR HP-200	CARTERA	COORDINADOR CARTERA
12078	COMPUTADOR HP-200	CARTERA	COORDINADOR CARTERA
12079	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12080	COMPUTADOR HP-200	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
12081	COMPUTADOR HP-200	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
12082	COMPUTADOR HP-200	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
12088	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12089	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12090	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12091	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO

PLAN DE PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS PLATAFORMA INFORMÁTICA 2025

Ref.	Nombre	Ubicación	Responsable
12094	UPS 3KVA	DATIC	PROCESO DATIC
12155	TORRE JANUS	VIGILANCIA Y SEGURIDAD	PROCESO VIGILANCIA
12156	TORRE JANUS	VIGILANCIA Y SEGURIDAD	PROCESO VIGILANCIA
12393	COMPUTADOR AIO HP	DEPARTAMENTO DE ENFERMERIA/ PROMOCION Y PREVENCION	JEFE DANNY LEON
12394	COMPUTADOR HP AIO	DEPARTAMENTO DE ENFERMERIA/ PROMOCION Y PREVENCION	JEFE DANNY LEON
12395	COMPUTADOR HP AIO	APOYO GESTION DE CALIDAD	COORDINADOR OFICINA CALIDAD
12396	COMPUTADOR HP AIO	APOYO OFICINA JURIDICA	APOYO OFICINA JURIDICA
12426	COMPUTADOR HP G4 AIO	GESTION DOCUMENTAL	GESTION DOCUMENTAL
12427	COMPUTADOR HP G4 AIO	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12428	COMPUTADOR HP G4 AIO	CONTRATACION	CONTRATACION
12429	COMPUTADOR HP G4 AIO	GESTION AMBIENTAL	COORDINADOR RECURSOS FISICOS
12430	COMPUTADOR HP G4 AIO	TERAPIA OCUPACIONAL	MARIA EUGENIA CASTILLO RUEDA
12431	COMPUTADOR HP G4 AIO	FARMACIA	COORDINADOR DEL SERVICIO
12432	COMPUTADOR HP G4 AIO	CONSULTA EXTERNA ESPECIALIZADA	JEFE LUZ EMILCE ESPINOSA
12433	COMPUTADOR HP G4 AIO	ALMACEN Y SUMINISTROS	PROCESO ALMACEN
12434	COMPUTADOR HP G4 AIO	ALMACEN Y SUMINISTROS	PROCESO ALMACEN
12435	COMPUTADOR HP G4 AIO	ESTADISTICA E HISTORIAS CLINICAS	PROCESO ESTADISTICA
12436	COMPUTADOR HP G4 AIO	ODONTOLOGIA	COORDINADOR ODONTOLOGIA
12438	COMPUTADOR HP G4 AIO	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
12439	COMPUTADOR HP G4 AIO	APOYO SUBDIRECCION CIENTIFICA	APOYO SUBDIRECCION CIENTIFICA
12440	COMPUTADOR HP G4 AIO	CONSULTA EXTERNA	ENFERMERA JEFE
12441	COMPUTADOR HP G4 AIO	MANTENIMIENTO	COORDINADOR RECURSOS FISICOS
12446	SERVIDOR LENOVO SR550	DATIC	PROCESO DATIC
12451	UPS POWEST EA9915 UL 15KVA	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12452	SW Aruba Ion 48G 2XT 2XF SW	BODEGA ALMACEN	GESTION INTEGRAL
12718	TORRE HP	CONTROL INTERNO	PROFESIONAL CONTROL INTERNO
12721	TORRE HP	CARTERA	COORDINADOR CARTERA
12723	TORRE HP	MANTENIMIENTO	COORDINADOR RECURSOS FISICOS
12725	TORRE HP	AUDITORIO ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
12727	TORRE HP	CONSULTA EXTERNA GENERAL	ENFERMERA JEFE/ COORD DEL SERVICIO

PLAN DE PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS PLATAFORMA INFORMÁTICA 2025

Ref.	Nombre	Ubicación	Responsable
12729	TORRE HP	CONSULTA EXTERNA GENERAL	ENFERMERA JEFE/ COORD DEL SERVICIO
12731	TORRE HP	CONSULTA EXTERNA GENERAL	ENFERMERA JEFE/ COORD DEL SERVICIO
12733	TORRE HP	PROGRAMACION CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12735	TORRE HP	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
12737	TORRE HP	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
12739	TORRE HP	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
12741	TORRE HP	LABORATORIO CLINICO	COORDINADORA LABORATORIO CLINICO
12845	COMPUTADOR HP AIO	DEPARTAMENTO FINANCIERO	APOYO PROFESIONAL CONTABILIDAD
12853	COMPUTADOR HP AIO	CONSULTA EXTERNA GENERAL	ENFERMERA JEFE/ COORD DEL SERVICIO
12861	COMPUTADOR HP AIO	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
12846	COMPUTADOR HP AIO	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12854	COMPUTADOR HP AIO	GINECOOBSTETRICIA	ENFERMERA JEFE/ COORD DEL SERVICIO
12847	COMPUTADOR HP AIO	URGENCIAS CONSULTA Y PROC	ENFERMERA JEFE/ COORD DEL SERVICIO
12855	COMPUTADOR HP AIO	URGENCIAS CONSULTA Y PROC	ENFERMERA JEFE/ COORD DEL SERVICIO
12856	COMPUTADOR HP AIO	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
12859	COMPUTADOR HP AIO	OFICINA DE CONTRATOS	OFICINA DE CONTRATOS
12857	COMPUTADOR HP AIO	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
12850	COMPUTADOR HP AIO	ASESOR GERENCIA	Gerencia

PLAN DE PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS PLATAFORMA INFORMÁTICA 2025

Ref.	Nombre	Ubicación	Responsable
12858	COMPUTADOR HP AIO	URGENCIAS CONSULTA Y PROC	ENFERMERA JEFE/ COORD DEL SERVICIO
12851	COMPUTADOR HP AIO	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
2859	COMPUTADOR HP AIO	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
12852	COMPUTADOR HP AIO	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
12860	COMPUTADOR HP AIO	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
2535	COMPUTADOR	AUDITORIA MEDICA	COORDINADORA CARTERA
4825	COMPUTADOR	VACUNACION COVID 19	JEFE DANNY LEON
4834	COMPUTADOR	AUDITORIO ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
4869	COMPUTADOR	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
5749	COMPUTADOR PORTATIL TOSHIBA	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
5750	COMPUTADOR PORTATIL TOSHIBA	VACUNACION COVID 19	ENFERMERA JEFE/ COORD DEL SERVICIO
5751	COMPUTADOR HP DX2400 MT - TORRE	VIGILANCIA Y SEGURIDAD	COOPVISGSAN CTA - LUIS ALFONSO SUAREZ
5752	COMPUTADOR HP DX2400 MT	ESTADISTICA E HISTORIAS CLINICAS	PROCESO ESTADISTICA
5952	COMPUTADOR QBEX LITE5-TORRE	OFICINA ASESOR GERENCIA	EDGAR JADIR SOLANO TOLOZA
5957	COMPUTADOR QBEX LITE5-TORRE	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
5994	COMPUTADOR QBEX APOLO TORRE	DATIC	PROCESO DATIC
6224	SERVIDOR HP ML110	DATIC	PROCESO DATIC
6247	TORRE QBEX TWIN3C00	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
6248	TORRE QBEX TWIN3C00	ALMACEN Y SUMINISTROS	PROCESO ALMACEN
6249	TORRE QBEX TWIN3C00	PUESTO DE SALUD DEL HATO	ENFERMERA JEFE/ COORD DEL SERVICIO
6250	TORRE QBEX TWIN3C00	MANTENIMIENTO	COORDINADOR DEL SERVICIO
6252	TORRE QBEX TWIN 3C00	VIGILANCIA Y SEGURIDAD	COOPVISGSAN CTA - LUIS ALFONSO SUAREZ
6253	TORRE QBEX TWIN C3C00	INSTRUMENTACION	ANGELICA MARIA GUALDRON
6254	TORRE QBEX TWIN 3C00	ESTADISTICA E HISTORIAS CLINICAS	COORDINADOR DEL SERVICIO
6268	SWITCH HP NETWORKING 2952	DATIC	PROCESO DATIC
6269	SWITCH HP NETWORKING 2952	DATIC	PROCESO DATIC
6289	COMPUTADOR PORTATIL HP4520S	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
6291	COMPUTADOR PORTATIL HP4520S	QUIRURGICAS	ENFERMERA JEFE/ COORD DEL SERVICIO
6292	COMPUTADOR PORTATIL HP4520S	GESTION DE CALIDAD	COORDINADOR DEL SERVICIO

PLAN DE PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS PLATAFORMA INFORMÁTICA 2025

Ref.	Nombre	Ubicación	Responsable
6293	COMPUTADOR PORTATIL HP4520S	GINECOBSTERICIA	ENFERMERA JEFE/ COORD DEL SERVICIO
6435	SERVIDOR HP ML350	DATIC	PROCESO DATIC
6911	UPS TRIPPLITE INTERACTIVAS	DATIC	PROCESO DATIC
6956	TORRE QBEX LITE 7E00	FARMACIA PALMAS DEL SOCORRO	COORDINADOR DEL SERVICIO
6957	TORRE QBEX LITE 7E00	ODONTOLOGIA	COORDINADOR ODONTOLOGIA
6961	TORRE QBEX LITE 7E00	PUESTO DE SALUD DEL HATO	ENFERMERA JEFE/ COORD DEL SERVICIO
6963	TORRE QBEX LITE 7E00	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
6964	TORRE QBEX LITE 7E00	FARMACIA	COORDINADOR DEL SERVICIO
6971	TORRE QBEX LITE 7E00	FARMACIA	COORDINADOR DEL SERVICIO
6973	TORRE QBEX LITE 7E00	VIGILANCIA Y SEGURIDAD	PROCESO VIGILANCIA
6979	TORRE QBEX LITE 7E00	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
6983	TORRE QBEX LITE 7E00	MANTENIMIENTO	PROCESO MANTENIMIENTO
6985	TORRE QBEX LITE 7E00	JEFE DE INFECCIONES	ENFERMERA JEFE
6986	TORRE QBEX LITE 7E00	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
6988	TORRE QBEX LITE 7E00	FISIOTERAPIA	COORDINADORA TERAPIA FISICA
6990	TORRE QBEX LITE 7E00	ATENCION AL USUARIO SIAU	COORDINADOR SIAU
6999	TORRE QBEX LITE 7E00	ESTADISTICA E HISTORIAS CLINICAS	COORDINADOR DEL SERVICIO
7001	TORRE QBEX LITE7E00	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
7002	TORRE QBEX LITE 7E00	CONSULTA EXTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
7007	TORRE QBEX LITE 7E00	FARMACIA HATO	REGENTE FARMACIA
7450	COMPUTADOR HP PRO 3130	MANTENIMIENTO	COORDINADOR DEL SERVICIO
7451	COMPUTADOR HP PRO 3130	PUESTO DE SALUD DEL HATO	ENFERMERA JEFE/ COORD DEL SERVICIO
7452	COMPUTADOR HP PRO 3130	ODONTOLOGIA PALMAS DEL SOCORRO	ODONTOLOGA
7453	COMPUTADOR HP PRO 3130	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
7461	COMPUTADOR HEWLET PACKARD	VACUNACION	ENFERMERA JEFE/ COORD DEL SERVICIO
7536	SERVIDOR HP PROLIANT ML 110G6	DATIC	COORDINADOR PROCESO DATIC
7557	TORRE HP 3400	AUDITORIO PRINCIPAL	VIGILANCIA
7559	TORRE HP 3400	PUESTO DE SALUD DE PALMAS	ENFERMERA JEFE/ COORD DEL SERVICIO
7563	TORRE HP PRO 3400	PROGRAMACION DE CIRUGIA	GLADYS CELIS
7587	SWITCH HPN V1910-48 G	DATIC	COORDINADOR DEL SERVICIO
7598	TORRE COMPUTADOR HPO PRO 3400	CARTERA	COORDINADOR DEL SERVICIO
7600	TORRE HPO PRO 3400	REVISORIA FISCAL	REVISOR FISCAL

PLAN DE PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS PLATAFORMA INFORMÁTICA 2025

Ref.	Nombre	Ubicación	Responsable
7602	COMPUTADOR HPO PRO 3400	ATENCION AL USUARIO SIAU	COORDINADOR SIAU
7603	TORRE HPO PRO 3400	PUESTO DE SALUD DEL HATO	ENFERMERA JEFE/ COORD DEL SERVICIO
7604	COMPUTADOR HPO PRO 3400	DEPARTAMENTO DE ENFERMERIA/ PROMOCION Y PREVENCION	ENFERMERA JEFE/ COORD DEL SERVICIO
7605	COMPUTADOR HPO PRO 3400	ESTADISTICA E HISTORIAS CLINICAS	COORDINADOR DEL SERVICIO
7961	COMPUTADOR PORTATIL	FISIOTERAPIA	FISIOTERAPEUTA
8010	TORRE COMPUTADOR	ODONTOLOGIA HATO	COORDINADOR DEL SERVICIO
8379	SERVIDOR HP	DATIC	COORDINADOR DEL SERVICIO
8622	UPS TIPO TRUE ON-LINE	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
9339	TORRE COMPUTADOR	CONSULTA EXTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
9466	COMPUTADOR	CIRUGIA	ENFERMERA JEFE/ COORD DEL SERVICIO
9485	COMPUTADOR	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
9518	COMPUTADOR LENOVO E73Z AIO	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
9519	COMPUTADOR LENOVO E73Z AIO	CONSULTA EXTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
9520	COMPUTADOR LENOVO E73Z AIO	CONSULTA EXTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
9521	COMPUTADOR LENOVO E73Z AIO	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
9522	COMPUTADOR LENOVO E73Z AIO	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE/ COORD DEL SERVICIO
9523	COMPUTADOR LENOVO E73Z AIO	ODONTOLOGIA ESPECIALIZADA MAXILO/ORTODONCIA	COORDINADOR ODONTOLOGIA
9526	COMPUTADOR LENOVO E73Z AIO	APOYO OFICINA JURIDICA	COORDINADOR DEL SERVICIO
9527	COMPUTADOR LENOVO E73Z AIO	VENTANILLA UNICA	COORDINADOR DEL SERVICIO
9528	COMPUTADOR LENOVO E73Z AIO	PUESTO DE SALUD DEL HATO	ENFERMERA JEFE/ COORD DEL SERVICIO
9583	SERVIDOR HP PROLIANT	DATIC	COORDINADOR DEL SERVICIO
9725	COMPUTADOR COMPACTO	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
9754	COMPUTADOR COMPACTO	QUIRURGICAS	ENFERMERA JEFE/ COORD DEL SERVICIO
9755	COMPUTADOR COMPACTO	FARMACIA	COORDINADOR DEL SERVICIO
9756	COMPUTADOR COMPACTO	FARMACIA	COORDINADOR DEL SERVICIO
9757	COMPUTADOR COMPACTO	COSTOS	COORDINADOR DEL SERVICIO
9759	COMPUTADOR COMPACTO	GINECOBSTETRICIA	ENFERMERA JEFE/ COORD DEL SERVICIO
9760	COMPUTADOR COMPACTO	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
9761	COMPUTADOR COMPACTO	QUIRURGICAS	ENFERMERA JEFE/ COORD DEL SERVICIO
9762	COMPUTADOR COMPACTO	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO

Ref.	Nombre	Ubicación	Responsable
9763	COMPUTADOR COMPACTO	MEDICINA INTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
9764	COMPUTADOR COMPACTO	GINECOBSTETRICIA	ENFERMERA JEFE/ COORD DEL SERVICIO
9765	COMPUTADOR COMPACTO	URGENCIAS OBSERVACION	ENFERMERA JEFE/ COORD DEL SERVICIO
9766	COMPUTADOR COMPACTO	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
9767	COMPUTADOR COMPACTO	CONSULTA EXTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
9768	COMPUTADOR COMPACTO	FARMACIA	COORDINADOR DEL SERVICIO
9769	COMPUTADOR COMPACTO	FARMACIA	COORDINADOR DEL SERVICIO
9770	COMPUTADOR COMPACTO	CONSULTA EXTERNA	ENFERMERA JEFE/ COORD DEL SERVICIO
9855	COMPUTADOR PORTATIL	FONOAUDIOLOGIA	DRA MARTHA NUBIA CASTAÑEDA
9931	COMPUTADOR LENOVO E73Z	INVENTARIOS	COORDINADOR DEL SERVICIO
9932	COMPUTADOR LENOVO E73Z	DEPARTAMENTO DE ENFERMERIA/ PROMOCION Y PREVENICION	JEFE DANNY LEON
9933	COMPUTADOR LENOVO E73Z	URGENCIAS CONSULTA Y PROCEDIMIENTOS	ENFERMERA JEFE/ COORD DEL SERVICIO
9934	COMPUTADOR LENOVO E73Z	COBRO PREJURIDICO	COORDINADOR DEL SERVICIO
9935	COMPUTADOR LENOVO E73Z	QUIRURGICAS	ENFERMERA JEFE/ COORD DEL SERVICIO

1.1.2. Software

Los aplicativos relacionados a continuación son aquellos que conforman la plataforma informática de la institución a nivel de software específico, y son aquellos que manejan datos de los usuarios, asistenciales y administrativos pertenecientes a los procesos de la ESE.

Nombre del Aplicativo	Funciones	Ubicación
Dinámica Gerencial	Historia clínica asistencial, proceso de almacén e inventarios, cartera, tesorería, talento humano.	Toda la institución
Histosoft	Historia clínica asistencial, proceso de almacén e inventarios, mantenimiento, cartera, tesorería, gestión documental, talento humano.	Toda la institución
Arthenia	Asignación de citas para consulta externa.	Estadística – Consulta Externa
Enterprise	Automatización de procesos laboratorio clínico.	Área asistencial

1.1.3. Equipos de Comunicaciones

Refer	Nombre Elemento	Descripción	Ubicación Actual	Responsable
12452	SWITCH	ARUBA ION	DATIC	Proceso DATIC
10801	SWITCH	ARUBA	DATIC	Proceso DATIC
10802	SWITCH	ARUBA	DATIC	Proceso DATIC
11542	SWITCH	JH295A	DATIC	Proceso DATIC
	SWITCH	HP V1910	URGENCIAS	COORDINADOR URGENCIAS
6268	SWITCH HP NETWORK	927FCPRB460E4 SWITCH PH NETWORK	DATIC	Proceso DATIC
7587	SWITCH HP V1910-4	S/N CN 18BX53VS HP 660008353	DATIC	Proceso DATIC
6269	SWITHC HP NETWORK	927FCPRA0491F SWITCH HP NETW	DATIC	Proceso DATIC

1.1.4. Equipamiento auxiliar

En esta sección solamente se detallan las UPS que soportan los servicios principales del datacenter y aquellas que soportan múltiples equipos.

Refer	Nombre Elemento	Descripción	Ubicación Actual	Responsable
10803	UPS SU3000XL	Soporte Swtich de Datos	DATIC	Proceso DATIC
6911	UPS TRIPPLITE SMART 3000	Soporte proxis internet, servidor Enterprise, pública	DATIC	Proceso DATIC
8622	UPS ENERGEX 12 KVA	Soporte área de urgencias	URGENCIAS	Jefe Servicio Urgencias
12094	UPS TRIPPLITE SMART 3000	Soporte Servidor principal	DATIC	Proceso DATIC
11121	UPS ENERGEX 15 KVA	Soporte área Consulta especializada	CONSULTA ESPECIALIZADA	Jefe Servicio Consulta Especializada
12451	UPS POWEST 15 KVA	Soporte área Cirugía	CIRUGÍA	Jefe Servicio Cirugía
12864	UPS RACK	Soporte Servidores Dinámica Gerencial	DATIC	Proceso DATIC

1.1.5. Unidades de Almacenamiento en Red

Refer	Nombre	Ubicación	Descripción
12095	NAS Synologic	Datos consulta externa	Almacenamiento de las carpetas privadas y pública

1.1.6. Instalaciones

Nombre	Ubicación	Descripción
Datacenter principal	DATIC	Datacenter principal de la entidad, con los servidores y las UPS para los mismos y los switch de datos.
Datos urgencias	Urgencias	Zona de cableado, switch y UPS, para el área de urgencias.
Datos consulta externa	Consulta Externa especializada	Zona de cableado, switch y UPS, para el área de consulta externa especializada.
Datos Cirugía	Cirugía	Zona de cableado, switch y UPS, para el área de cirugía.

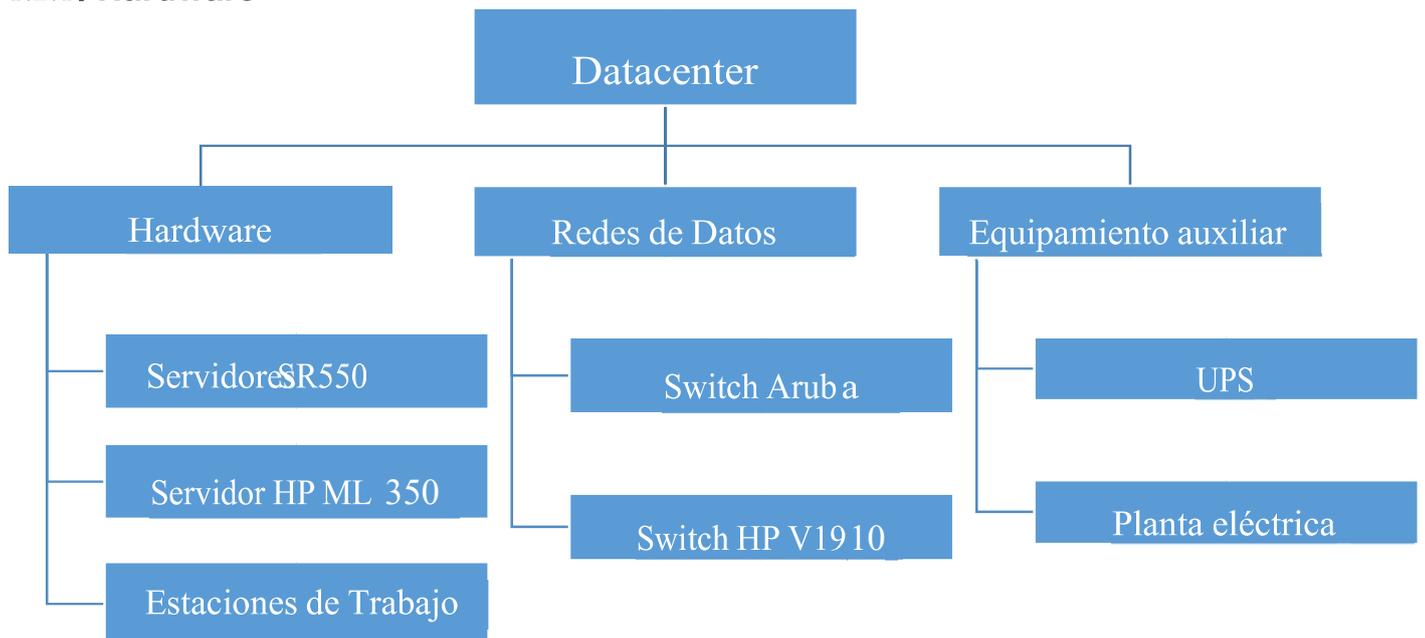
1.1.7. Personal

El soporte y desarrollo de la plataforma está a cargo del personal de DATIC, el cual hace parte de un proceso subcontrato por la institución.

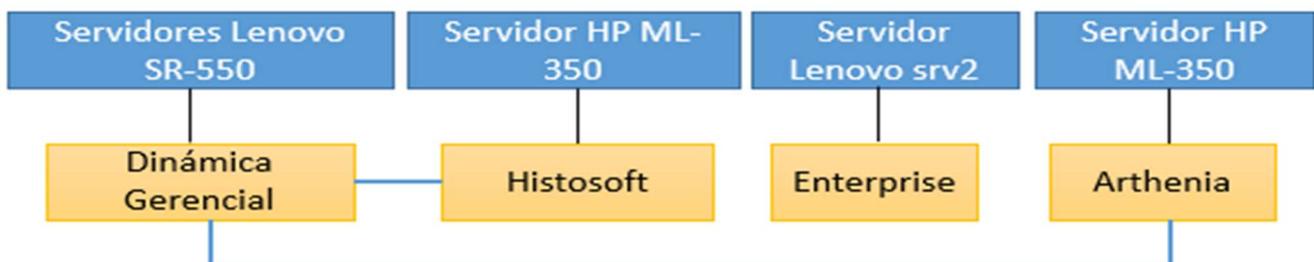
Cargo	Funciones
Coordinador DATIC	Coordinación de actividades, manejo de gerencia de procesos, diseño y desarrollo de software de la plataforma.
Ingeniero de Soporte	Soporte a plataforma Dinámica Gerencial/histosoft, aplicativos web, diseño y desarrollo página web
Tecnólogo de Soporte 1	Soporte a plataforma Dinámica Gerencial, intranet, Enterprise, internet y redes de datos.
Tecnólogo de Soporte 2	Soporte a software básico, Hardware, seguridad informática y cámaras de vigilancia

1.2. DEPENDENCIA ENTRE LOS ACTIVOS

1.2.1. Hardware



1.2.2. Software



1.3. VALORACION DE LOS ACTIVOS

Para la realización de la valoración de activos se utilizará la siguiente escala, la cual se aplica dependiendo de los criterios de confidencialidad, integridad y disponibilidad, de acuerdo a la exposición por parte del activo a las diferentes amenazas.

Puntaje	Valor	Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8.9	Alto	Daño grave
3-5.9	Medio	Daño muy importante
1-2.9	Bajo	Daño menor
0	Despreciable	Irrelevante

A continuación, se realiza la valoración de los activos definidos en el inventario de acuerdo a la tabla anterior.

1.3.1. Hardware

Servidores

Refer	Nombre Elemento	Ubicación Actual	Valor
12744	SERVIDOR LENOVO SR250	DATIC	8.2
12743	SERVIDOR SRV2	DATIC	7.1
12745	SERVIDOR LEN MR550	DATIC	8.2
12746	SERVIDOR LEN MR550	DATIC	8.2
12747	SERVIDOR LEN MR550	DATIC	8.2

12748	SERVIDOR LEN MR550	DATIC	8.2
6435	SERVIDOR HP ML350 G6	DATIC	8.2
9583	SERVIDOR HP ML350 G8	DATIC	5
12446	SERVIDOR LEN MR550	DATIC	5

Estaciones de Trabajo

Refer	Nombre Elemento	Ubicación Actual	Valor
12718	COMPUTADOR	CONTROL INTERNO	3
11164	COMPUTADOR	DATIC	3
11168	COMPUTADOR	DATIC	3
11170	COMPUTADOR	DATIC	3
11781	COMPUTADOR	SECRETARIA GERE	3
11166	COMPUTADOR	DATIC	3
10405	COMPUTADOR	VACUNACION	3
11789	COMPUTADOR HP PRO_ONE	ADMINISTRACION FINANCIERA	3
11163	COMPUTADOR LENOVO	COSTOS	3
10657	COMPUTADOR AIO LEN	GESTION DE CALI	3
10646	COMPUTADOR AIO LEN	SUBDIRECCION CI	3

7604	COMPUTADOR HPO PRO	ALMACEN Y SUMIN	3
12850	COMPUTADOR HPO PRO	CONTABILIDAD	3
10982	COMPUTADOR LENOVO	OFICINA JURIDIC	3
10897	COMPUTADOR LENOVO	SUBDIRECCION AD	3
10812	COMPUTADOR LENOVO	GERENCIA	3
10817	COMPUTADOR LENOVO	SUBDIRECCION CI	3
9932	COMPUTADOR LENOVO	DEPARTAMENTO DE	3
9931	COMPUTADOR LENOVO	INVENTARIOS	3
9526	COMPUTADOR LENOVO	OFICINA JURIDICA	3
7961	COMPUTADOR PORTATI	FISIOTERAPIA	5
9855	COMPUTADOR PORTATI	FONOAUDIOLOGIA	5
5994	COMPUTADOR QBEX AP	DATIC	5
9339	TORRE COMPUTADOR	DEPARTAMENTO DE	3
7598	TORRE COMPUTADOR H	CARTERA	3
11007	TORRE COMPUTADOR Q	COSTOS	3
6981	TORRE QBEX LITE 7E	ARCHIVO	3

Los demás equipos de informática no incluidos en la anterior tabla se consideran riesgo 2.

1.3.2. Software

Nombre del Aplicativo	Funciones	Ubicación	Valor
Dinámica Gerencial	Historia clínica asistencial, proceso de almacén e inventarios, cartera, tesorería, talento humano.	Toda la institución	10
Histosoft	Consulta histórica: proceso de almacén e inventarios, Historia clínica asistencial, cartera, tesorería. Proceso de mantenimiento, gestión documental, cuadro de mando integral, calendario de eventos.	Toda la institución	8
Enterprise	Automatización de procesos laboratorio clínico.	Área asistencial	8
Arthenia	Asignación de citas para consulta externa	Estadística – Consulta externa	5

1.3.3. Equipos de Comunicaciones

Refer	Nombre Elemento	Ubicación Actual	Valor
11543	SWITCH JG961A	DATIC	8
11542	SWITCH JH295A	DATIC	8
10801	SWITCH	DATIC	7
10802	SWITCH	DATIC	7
5753	SWITCH	DATIC	3
4943	SWITCH	DATIC	5
	SWITCH	URGENCIAS	5
6268	SWITCH HP NETWORK	DATIC	5
7587	SWITCH HP V1910-4	DATIC	5
12452	SWITCH ARUBA	DATIC	8

1.3.4. Equipamiento auxiliar

Refer	Nombre Elemento	Ubicación Actual	Valor
10803	UPS SU3000XL	DATIC	6
7467	UPS HP AF450A	DATIC	6
6911	UPS TRIPPLITE SMART 3000	DATIC	3
8622	UPS ENERGEX 12 KVA	URGENCIAS	6
12094	UPS TRIPPLITE SMART 3000	DATIC	6
11121	UPS ENERGEX 15 KVA	CONSULTA ESPECIALIZADA	6
12451	UPS POWEST 15 KVA	CIRUGÍA	6
12864	UPS TRIPPLITE SMART 3000	DATIC	6

1.3.5. Unidades de Almacenamiento en Red

Refer	Nombre Elemento	Ubicación Actual	Valor
12095	NAS Synologic	Datos consulta externa	6

CAPITULO 2. CONTROLES EXISTENTES

2.1. IDENTIFICACION DE CONTROLES EXISTENTES

En esta sección se detallan los controles que actualmente tiene implementados la ESE, en sus activos de información:

Tipo de Riesgo	Controles
Riesgos Físicos Internos	Acceso restringido a la zona de servidores
Riesgos Físicos Externos	Sistema de cámaras de seguridad Plan de Contingencia
Riesgos Lógicos Internos	Utilización de cuentas limitadas Software Antivirus Procedimiento de copias de seguridad Perfiles de acceso a los diferentes aplicativos
Riesgos Lógicos Externos	Software Antivirus Perfiles de acceso a los diferentes aplicativos Procedimiento de copias de seguridad Seguridad perimetral

CAPITULO 3. IDENTIFICACIÓN DE LAS VULNERABILIDADES

Tipo de Activo	Vulnerabilidad	Amenaza
Hardware	Mantenimiento insuficiente	Daño por mal uso, destrucción, falta de mantenimiento
	Hurtos medios o equipos	Robo
	Susceptibilidad a las variaciones de temperatura	Falla de equipos de climatización
	Fenómenos meteorológicos	Inundación
	Susceptibilidad a las variaciones de voltaje Pérdida del suministro de energía	Falla suministro eléctrico
	Error en el uso	Daño por mal uso
	Destrucción de equipos o medios.	Daño por mal uso, destrucción, falta de mantenimiento
	Ausencia de sensores en el datacenter	Incendio
	Fenómenos ambientales y sociales	Daño por evento catastrófico.
Software	Insuficiencia de pruebas de software	-Acceso a información no autorizada. -Borrado de información. -Fuga de información
	Incompletos registros de auditoria	-Acceso a información no autorizada. -Borrado de información. -Fuga de información

	Ausencia de mecanismos de identificación y autenticación	-Acceso a información no autorizada. -Fuga de información
	Gestión deficiente de las contraseñas	-Acceso a información no autorizada. -Fuga de información
	Descarga y uso no controlado de software	Instalación y/o ataque de malware
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	-Acceso a información no autorizada. -Fuga de información
	Servidores de datos con baja capacidad de almacenamiento	Agotamiento de recursos
Equipos de Comunicaciones	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	-Acceso a información no autorizada. -Fuga de información -Agotamiento de recursos
	Tráfico sensible sin protección	-Acceso a información no autorizada. -Fuga de información
	Líneas de comunicación sin protección	-Acceso a información no autorizada. -Fuga de información
	Ausencia de identificación y autenticación de emisor y receptor	-Acceso a información no autorizada. -Fuga de información
Equipamiento auxiliar	Hurtos medios o equipos	Robo
	Destrucción de equipos o medios.	Daño por mal uso, destrucción, falta de mantenimiento

	Susceptibilidad a las variaciones de voltaje Pérdida del suministro de energía	Falla suministro eléctrico
	Fenómenos ambientales y sociales	Daño por evento catastrófico.
Infraestructura	Control de acceso físico a las edificaciones y los recintos no adecuado.	-Acceso a información no autorizada. -Fuga de información -Daño por mal uso, destrucción, falta de mantenimiento
	Ubicación en área susceptible de inundación	-Daño por mal uso, destrucción, falta de mantenimiento
	Área física inadecuada para el volumen de datos y procedimientos soportados en la plataforma.	-Agotamiento de recursos. -Incendio
	Red energética inestable	-Falla suministro eléctrico
Personal	Ausencia del personal	-Falta soporte técnico
	Procedimientos inadecuados de contratación	-Fuga de información
	Entrenamiento insuficiente en seguridad	-Daño por mal uso, destrucción, falta de mantenimiento -Fuga de información -Borrado de información Instalación y/o ataque de malware
	Falta de conciencia acerca de la seguridad	-Fuga de información -Borrado de información Instalación y/o ataque de malware

Ausencia de mecanismos de monitoreo	-Acceso a información no autorizada. -Fuga de información Instalación y/o ataque de malware
Trabajo no supervisado del personal externo o de limpieza	-Acceso a información no autorizada. -Fuga de información -Daño por mal uso, destrucción, falta de mantenimiento

CAPITULO 4. EVALUACION DE RIESGO

4.1. IDENTIFICACIÓN DE RIESGOS SOBRE LOS ACTIVOS

Para la identificación de las posibles amenazas que pueden afectar los activos, se ha establecido la siguiente clasificación de las mismas de acuerdo a su tipo y origen:

Tipo	Origen	Descripción de la amenaza
Riesgos Físicos	Internos	Robo
		Daño por mal uso, destrucción, falta de mantenimiento
		Incendio
		Inundación
		No funcionamiento
		Falla suministro eléctrico
		Falla de equipos de climatización
Riesgos Físicos	Externos	Robo
		Daño por evento catastrófico
Riesgos Lógicos	Internos	Instalación y/o ataque de malware
		Borrado de información
		Acceso a información no autorizada
		Fuga de información
		Agotamiento de recursos
Riesgos Lógicos	Externos	Instalación y/o ataque de malware
		Borrado de Información
		Acceso a información no autorizada

	Acceso a servicios bancarios
	Denegación de Servicios

4.2. EVALUACION DEL RIESGO

La calificación será realizada mediante la evaluación de dos factores: Probabilidad de ocurrencia y Valor del nivel de afectación o impacto (valor asignado en la sección 1.3), con peso porcentual del 30% y 70% respectivamente sobre la calificación definitiva del riesgo, manejando valores desde el 1 al 10, en donde este último es la mayor probabilidad de ocurrencia o mayor nivel de afectación.

A continuación, se define la tabla de colores y nivel de riesgo de acuerdo al puntaje obtenido por cada amenaza:

Puntos	Nivel de Riesgo	Color
8-10	Alto	Rojo
5-7.9	Medio	Amarillo
1-4.9	Bajo	Blanco

4.2.1. Riesgos Físicos Internos

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Servidores	12744 - SERVIDOR LENOVO SR250	Robo	10	3	9.1
		Daño por mal uso	10	5	8.5
		Incendio	10	2	7.6
		Inundación	10	1	7.3
		Falla suministro eléctrico	10	3	9.1
		Falla de equipos de climatización	10	4	8.2

12745 - SERVIDOR LENOVO SR550	Robo	7	3	5.8
	Daño por mal uso	7	5	6.4
	Incendio	7	2	5.5
	Inundación	7	1	5.2
	Falla suministro eléctrico	7	3	5.8
	Falla de equipos de climatización	7	4	6.1
12746 - SERVIDOR LENOVO SR550	Robo	7	3	5.8
	Daño por mal uso	7	5	6.4
	Incendio	7	2	5.5
	Inundación	7	1	5.2
	Falla suministro eléctrico	7	3	5.8
	Falla de equipos de climatización	7	4	6.1
12747 - SERVIDOR LENOVO SR550	Robo	7	3	5.8
	Daño por mal uso	7	5	6.4
	Incendio	7	2	5.5
	Inundación	7	1	5.2
	Falla suministro eléctrico	7	3	5.8
	Falla de equipos de climatización	7	4	6.1
12446 – Servidor SR550	Robo	5	2	4.1
	Daño por mal uso	5	3	4.4

		Incendio	5	2	4.1
		Inundación	5	1	3.8
		Falla suministro eléctrico	5	3	4.4
		Falla de equipos de climatización	5	4	4.7
6435-SERVIDOR HP ML350 G6		Robo	5	2	4.1
		Daño por mal uso	5	3	4.4
		Incendio	5	2	4.1
		Inundación	5	1	3.8
		Falla suministro eléctrico	5	5	5.0
		Falla de equipos de climatización	5	4	4.7
9583 - SERVIDOR HP ML350 G8		Robo	10	2	7.6
		Daño por mal uso	10	3	7.9
		Incendio	10	2	7.6
		Inundación	10	1	7.3
		Falla suministro eléctrico	10	5	8.5
		Falla de equipos de climatización	10	4	8.2

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Estaciones de Trabajo – Área administrativa	Estaciones de valor nivel 5	Robo	5	3	4.4
		Daño por mal uso	5	4	4.7
		Incendio	5	2	4.1

		Inundación	5	1	3.8
		Falla suministro eléctrico	5	5	5.0
		Falla de equipos de climatización	5	4	4.7
Estaciones de valor nivel 3		Robo	3	3	4.4
		Daño por mal uso	3	4	4.7
		Incendio	3	2	4.1
		Inundación	3	1	3.8
		Falla suministro eléctrico	3	5	5.0
		Falla de equipos de climatización	3	4	4.7
Estaciones de valor nivel 2		Robo	2	3	4.4
		Daño por mal uso	2	4	4.7
		Incendio	2	2	4.1
		Inundación	2	1	3.8
		Falla suministro eléctrico	2	5	5.0
		Falla de equipos de climatización	2	4	4.7

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Estaciones de Trabajo –	Estaciones de valor nivel 5	Robo	5	4	4.7
		Daño por mal uso	5	5	5
		Incendio	5	2	4.1
		Inundación	5	2	4.1
		Falla suministro eléctrico	5	5	5

Área asistencial		Falla de equipos de climatización	5	4	4.7
	Estaciones de valor nivel 3	Robo	3	4	3.3
		Daño por mal uso	3	5	3.6
		Incendio	3	2	2.7
		Inundación	3	2	2.7
		Falla suministro eléctrico	3	5	3.6
		Falla de equipos de climatización	3	4	3.3
	Estaciones de valor nivel 2	Robo	2	4	2.6
		Daño por mal uso	2	5	2.9
		Incendio	2	2	2
		Inundación	2	2	2
		Falla suministro eléctrico	2	5	2.9
		Falla de equipos de climatización	2	4	2.6

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Equipos de Comunicaciones	Switch de valor nivel 8	Robo	8	2	6.2
		Daño por mal uso	8	3	6.5
		Incendio	8	2	6.2
		Inundación	8	1	5.9
		Falla suministro eléctrico	8	5	7.1
		Falla de equipos de climatización	8	4	6.8
	Switch de valor nivel 5	Robo	5	2	4.1

		Daño por mal uso	5	3	4.4
		Incendio	5	2	4.1
		Inundación	5	1	3.8
		Falla suministro eléctrico	5	5	5
		Falla de equipos de climatización	5	4	4.7
	Switch de valor nivel 3	Robo	3	2	2.7
		Daño por mal uso	3	3	3
		Incendio	3	2	2.7
		Inundación	3	1	2.4
		Falla suministro eléctrico	3	5	3.6
		Falla de equipos de climatización	3	4	3.3

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Equipo Auxiliar	UPS de valor nivel 6	Robo	6	2	4.8
		Daño por mal uso	6	3	5.1
		Incendio	6	2	4.8
		Inundación	6	1	4.5
		Falla suministro eléctrico	6	5	5.7
		Falla de equipos de climatización	6	4	5.4
	UPS de valor nivel 3	Robo	3	2	2.7
		Daño por mal uso	3	3	3

		Incendio	3	2	2.7
		Inundación	3	1	2.4
		Falla suministro eléctrico	3	5	3.6
		Falla de equipos de climatización	3	4	3.3

4.2.2. Riesgos Físicos Externos

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Servidores	12744 - SERVIDOR LENOVO SR250	Robo	10	2	7.6
		Daño por evento catastrófico	10	1	7.3
	12745 - SERVIDOR LENOVO SR550	Robo	7	2	7.6
		Daño por evento catastrófico	7	1	7.3
	12746 - SERVIDOR LENOVO SR550	Robo	7	2	7.6
		Daño por evento catastrófico	7	1	7.3
	12747 - SERVIDOR LENOVO SR550	Robo	7	2	7.6
		Daño por evento catastrófico	7	1	7.3
	11205 – SERVIDOR DELL T30	Robo	5	2	4.1
		Daño por evento catastrófico	5	1	3.8
	6435-SERVIDOR HP ML350 G6	Robo	5	2	4.1
		Daño por evento catastrófico	5	1	3.8
	9583 - SERVIDOR HP ML350 G8	Robo	10	2	7.6
		Daño por evento catastrófico	10	1	7.3

SERVIDOR LENOVO ENTERPRISE	Robo	7	2	5.5
	Daño por evento catastrófico	7	1	5.2
12446 – SERVIDOR MR550	Robo	5	2	4.1
	Daño por evento catastrófico	5	1	3.8

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Estaciones de Trabajo – Área administrativa	Estaciones de valor nivel 5	Robo	5	4	4.7
		Daño por evento catastrófico	5	1	3.8
	Estaciones de valor nivel 3	Robo	3	4	3.3
		Daño por evento catastrófico	3	1	2.4
	Estaciones de valor nivel 2	Robo	2	4	2.6
		Daño por evento catastrófico	2	1	1.7
Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Estaciones de Trabajo – Área asistencial	Estaciones de valor nivel 5	Robo	5	5	4.7
		Daño por evento catastrófico	5	1	3.8
	Estaciones de valor nivel 3	Robo	3	5	3.6
		Daño por evento catastrófico	3	1	2.4
	Estaciones de valor nivel 2	Robo	2	5	2.9
		Daño por evento catastrófico	2	1	1.7
Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
	Switch de valor nivel 5	Robo	8	2	6.2

Equipos de Comunicaciones		Daño por evento catastrófico	8	1	5.9
	Switch de valor nivel 5	Robo	5	2	4.1
		Daño por evento catastrófico	5	1	3.8
	Switch de valor nivel 3	Robo	3	2	2.7
Daño por evento catastrófico		3	1	2.4	
Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Equipo Auxiliar	UPS de valor nivel 6	Robo	6	2	4.8
		Daño por evento catastrófico	6	1	4.5
	UPS de valor nivel 3	Robo	3	2	2.7
		Daño por evento catastrófico	3	1	2.4

4.2.3. Riesgos Lógicos Internos

Actualmente las estaciones de trabajo de la institución cuentan con las siguientes medidas para prevenir eventos que afecten la seguridad de la plataforma:

- Software antivirus y antimalware.
- Suspensión de los puertos USB para extraer información de las estaciones de trabajo.
- Filtrado por tipo de usuario de páginas web y contenidos.
- En esta sección se hace referencia a la posibilidad de extraer información institucional de los equipos de cómputo sin la debida autorización para uso externo. Actualmente los funcionarios de acuerdo a sus cargos tienen unos perfiles establecidos en la plataforma informática, lo cual les permite acceder a información relevante a sus actividades, esta información puede ser sacada de la institución de las siguientes formas: Impresión física, correo electrónico o imagen obtenida por fotografía de la pantalla de la estación de trabajo. Para las dos primeras opciones se tiene la trazabilidad sobre el proceso de impresión de documentos y para la última opción, es muy difícil controlar esta acción debido a que la mayoría de los funcionarios cuenta con Smartphone.
- Las bases de datos de los aplicativos se encuentran ubicadas en los servidores de datos sin posibilidad de acceso directo a los funcionarios diferentes a DATIC.

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Servidores	12744 - SERVIDOR LENOVO SR250	Instalación y ataque de malware	10	3	7.9
		Borrado de información	10	2	7.6
		Acceso a información no autorizada	10	4	8.2
		Fuga de información	10	4	8.2
		Agotamiento de recursos	10	5	8.5
	12745 - SERVIDOR LENOVO SR550	Instalación y ataque de malware	7	3	5.8
		Borrado de información	7	2	5.5
		Acceso a información no autorizada	7	4	6.1
		Fuga de información	7	4	6.1
		Agotamiento de recursos	7	5	6.4
	12746 - SERVIDOR LENOVO SR550	Instalación y ataque de malware	7	3	5.8
		Borrado de información	7	2	5.5
		Acceso a información no autorizada	7	4	6.1
		Fuga de información	7	4	6.1
		Agotamiento de recursos	7	5	6.4
	12747 - SERVIDOR LENOVO SR550	Instalación y ataque de malware	7	3	5.8
		Borrado de información	7	2	5.5
		Acceso a información no autorizada	7	4	6.1
		Fuga de información	7	4	6.1
		Agotamiento de recursos	7	5	6.4

SERVIDOR LENOVO ENTERPRISE	Instalación y ataque de malware	5	3	4.4
	Borrado de información	5	2	4.1
	Acceso a información no autorizada	5	3	4.4
	Fuga de información	5	2	4.1
	Agotamiento de recursos	5	4	4.7
6435-SERVIDOR HP ML350 G6	Instalación y ataque de malware	5	3	4.4
	Borrado de información	5	2	4.1
	Acceso a información no autorizada	5	4	4.7
	Fuga de información	5	4	4.7
	Agotamiento de recursos	5	4	4.7
9583 - SERVIDOR HP ML350 G8	Instalación y ataque de malware	10	3	7.9
	Borrado de información	10	2	7.6
	Acceso a información no autorizada	10	4	8.2
	Fuga de información	10	4	8.2
	Agotamiento de recursos	8	5	7.1
12446 - Servidor SR-550	Instalación y ataque de malware	5	3	4.4
	Borrado de información	5	2	4.1
	Acceso a información no autorizada	5	4	4.7
	Fuga de información	5	4	4.7
	Agotamiento de recursos	5	5	5

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Estaciones de Trabajo – Área administrativa	Estaciones de valor nivel 5	Instalación y ataque de malware	5	5	5
		Borrado de información	5	4	4.7
		Acceso a información no autorizada	5	5	5
		Fuga de información	5	5	5
		Agotamiento de recursos	5	3	4.4
	Estaciones de valor nivel 3	Instalación y ataque de malware	3	4	3.3
		Borrado de información	3	2	2.7
		Acceso a información no autorizada	3	4	3.3
		Fuga de información	3	4	3.3
		Agotamiento de recursos	3	3	3
	Estaciones de valor nivel 2	Instalación y ataque de malware	2	2	2
		Borrado de información	2	1	1.7
		Acceso a información no autorizada	2	4	2.6
		Fuga de información	2	4	2.6
		Agotamiento de recursos	2	1	1.7
Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Estaciones de Trabajo – Área asistencial	Estaciones de valor nivel 5	Instalación y ataque de malware	5	2	4.1
		Borrado de información	5	5	5
		Acceso a información no autorizada	5	4	4.7
		Fuga de información	5	4	4.7
		Agotamiento de recursos	5	4	4.7

	Estaciones de valor nivel 3	Instalación y ataque de malware	3	2	2.7
		Borrado de información	3	3	3
		Acceso a información no autorizada	3	4	3.3
		Fuga de información	3	4	3.3
		Agotamiento de recursos	3	2	2.7
	Estaciones de valor nivel 2	Instalación y ataque de malware	2	2	2
		Borrado de información	2	1	1.7
		Acceso a información no autorizada	2	4	2.6
		Fuga de información	2	4	2.6
		Agotamiento de recursos	2	2	2

4.2.4. Riesgos Lógicos Externos

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo	
Servidores	12744 - SERVIDOR LENOVO SR250	Instalación y ataque de malware	10	5	8.5	
		Borrado de información	10	5	8.5	
		Acceso a información no autorizada	10	4	8.2	
		Acceso a servicios bancarios	10	1	7.3	
	12745 - SERVIDOR LENOVO SR550	Instalación y ataque de malware	7	5	6.4	
		Borrado de información	7	5	6.4	
		Acceso a información no autorizada	7	4	6.1	
		Acceso a servicios bancarios	7	1	5.2	
			Instalación y ataque de malware	7	5	6.4

12746 - SERVIDOR LENOVO SR550	Borrado de información	7	5	6.4
	Acceso a información no autorizada	7	4	6.1
	Acceso a servicios bancarios	7	1	5.2
12747 - SERVIDOR LENOVO SR550	Instalación y ataque de malware	7	5	6.4
	Borrado de información	7	5	6.4
	Acceso a información no autorizada	7	4	6.1
	Acceso a servicios bancarios	7	1	5.2
6435-SERVIDOR HP ML350 G6	Instalación y ataque de malware	5	5	5
	Borrado de información	5	5	5
	Acceso a información no autorizada	3	4	3.3
	Acceso a servicios bancarios	1	1	1
9583 - SERVIDOR HP ML350 G8	Instalación y ataque de malware	7	5	6.4
	Borrado de información	7	5	6.4
	Acceso a información no autorizada	7	4	6.1
	Acceso a servicios bancarios	1	1	1
SERVIDOR LENOVO ENTERPRISE	Instalación y ataque de malware	7	5	6.4
	Borrado de información	7	5	6.4
	Acceso a información no autorizada	7	4	6.1
	Acceso a servicios bancarios	1	1	1
	Instalación y ataque de malware	5	5	5.0

12446 – Servidor SR550	Borrado de información	5	4	4.7
	Acceso a información no autorizada	5	4	4.7
	Acceso a servicios bancarios	1	1	1

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Estaciones de Trabajo – Área administrativa	Estaciones de valor nivel 5	Instalación y ataque de malware	5	6	5.3
		Borrado de información	5	5	5
		Acceso a información no autorizada	5	6	5.3
		Acceso a servicios bancarios	7	4	6.1
	Estaciones de valor nivel 3	Instalación y ataque de malware	3	5	3.6
		Borrado de información	3	4	3.3
		Acceso a información no autorizada	3	5	3.6
		Acceso a servicios bancarios	1	1	1
	Estaciones de valor nivel 2	Instalación y ataque de malware	2	5	2.9
		Borrado de información	2	4	2.6
		Acceso a información no autorizada	2	4	2.6
		Acceso a servicios bancarios	1	1	1

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
Estaciones de Trabajo – Área asistencial	Estaciones de valor nivel 5	Instalación y ataque de malware	5	3	4.7
		Borrado de información	5	3	4.7
		Acceso a información no autorizada	5	3	4.7
		Acceso a servicios bancarios	1	1	1

Estaciones de valor nivel 3	Instalación y ataque de malware	3	5	3.6
	Borrado de información	3	3	3
	Acceso a información no autorizada	3	5	3.6
	Acceso a servicios bancarios	1	1	1
Estaciones de valor nivel 2	Instalación y ataque de malware	2	3	2.3
	Borrado de información	2	2	2
	Acceso a información no autorizada	2	5	3.9
	Acceso a servicios bancarios	1	1	1

4.3. PRIORIZACION DE LOS RIESGOS

Para cada uno de los eventos definidos en la anterior sección se determina priorizar aquellos que obtuvieron un puntaje superior a 6.0, considerándolos como riesgo medio-alto, los cuáles se detallan a continuación:

4.3.1. Riesgos Físicos Internos

Activo	Amenaza	Descripción
Servidores	Robo	Acceso de personal no autorizado al datacenter para sustracción de los equipos.
	Daño por mal uso	Daño físico del hardware por fallidos intentos de reparación en caliente, golpes causados por materiales del mismo datacenter y ataques por funcionarios internos.
	Incendio	Incendio del datacenter debido a un corto circuito interno o propagación del fuego desde zonas externas.

	Inundación	Inundación del datacenter por falla en la red hidráulica de los baños ubicados en los costados del mismo.
	Falla suministro eléctrico	Falta de suministro eléctrico al datacenter, debido a problemas técnicos de la subestación del hospital, del proveedor externo y al no funcionamiento de la planta eléctrica institucional.
	Falla de equipos de climatización	Falla del actual equipo de aire acondicionado del datacenter, lo que ocasionaría una elevación de la temperatura del mismo, activando los mecanismos de protección de los servidores iniciando su autoapagado.

4.3.2. Riesgos Físicos Externos

Activo	Amenaza	Descripción
Servidores	Robo	Acceso de personal no autorizado al datacenter para sustracción de los equipos.
	Daño por evento catastrófico	Daño físico del hardware por fallidos intentos de reparación en caliente, golpes causados por materiales del mismo datacenter y ataques por funcionarios internos.

4.3.3. Riesgos Lógicos Internos

Activo	Amenaza	Descripción
Servidores	Acceso a información no autorizada	Acceso a información no autorizada de acuerdo al perfil manejado por el funcionario, o acceso a la plataforma por una persona externa desde una estación de trabajado ubicada dentro de la institución.
	Fuga de información	Extracción de información de la plataforma para su uso externo no autorizado.
	Agotamiento de recursos	Reducción en la disponibilidad de recursos a nivel de procesamiento, memoria y en especial almacenamiento, por el actual tamaño de los discos duros y los grandes volúmenes de datos manejados.

	Instalación y ataque de malware	Instalación y ataque por parte de software malicioso a partir de una estación de trabajo que tenga acceso a los servicios del servidor.
	Borrado de información	Borrado o inutilización de información, como consecuencia de un ataque o error involuntario, generado a partir de una estación de trabajo que tenga acceso a los servicios del servidor.

4.3.4. Riesgos Lógicos Externos

Activo	Amenaza	Descripción
Servidores	Instalación y ataque de malware	Instalación de un malware y generación de ataque por parte del mismo, impidiendo el funcionamiento del servidor y suspendiendo los servicios ofrecidos por el mismo.
	Borrado de información	Borrado o inutilización de información almacenada en las bases de datos por parte de un intruso.
	Acceso a información no autorizada	Acceso a información no autorizada por parte de un intruso.
Estaciones de trabajo administrativas	Acceso no autorizado a servicios bancarios.	Acceso a las plataformas bancarias utilizadas por la institución desde las estaciones de trabajo de gerencia o el área financiera.

CAPITULO 5. DEFINICION DE MEDIDAS PARA REDUCCION DE RIESGOS

5.1. DEFINICION DE MEDIDAS

5.1.1. Riesgos Físicos Internos

Activo	Amenaza	Medidas para reducción del riesgo
Servidores	Robo	<ul style="list-style-type: none"> Definición del área actual como de uso exclusivo para el datacenter. Implementación del acceso biométrico al datacenter. Vigilancia remota por la cámara en el datacenter.
	Daño por mal uso	<ul style="list-style-type: none"> Definición del área actual como de uso exclusivo para el datacenter. Implementación del acceso biométrico al datacenter. Realización de jornadas técnicas sobre manejo de los servidores para el personal DATIC.
	Incendio	<ul style="list-style-type: none"> Definición del área actual como de uso exclusivo para el datacenter. Instalación de sensores de humo en el datacenter. Evaluación de la efectividad del plan de contingencia del datacenter. Vigilancia remota por la cámara en el datacenter.
	Inundación	Instalación de una cámara en el datacenter. Proteger el sistema de cableado eléctrico que circula por el nivel del piso. Instalación de los equipos a un nivel superior a 30 cm del piso.

Falla suministro eléctrico	<ul style="list-style-type: none"> • Aumento de la capacidad actual de soporte de las UPS. • Adecuación de una red de suministro eléctrico de contingencia. • Implementación de un polo a tierra adecuado para el datacenter.
Falla de equipos de climatización	<ul style="list-style-type: none"> • Garantizar el correcto funcionamiento de las dos unidades de climatización, para contar con respaldo en caso de fallo de la que se encuentre en funcionamiento; para esto se requiere la reparación y actualización tecnológica de estos equipos. • Definición del área actual como de uso exclusivo para el datacenter, para realizar una mejor distribución de espacios y optimizar el flujo de temperaturas.
	<ul style="list-style-type: none"> • Disposición de dos unidades de refrigeración tipo ventilador de torre para el caso de la falla de los equipos de refrigeración. • Mantenimiento preventivo de los equipos de climatización.

Activo	Amenaza	Medidas para reducción del riesgo
Equipos de Comunicaciones	Robo	<ul style="list-style-type: none"> • Definición del área actual como de uso exclusivo para el datacenter. • Implementación del acceso biométrico al datacenter. • Vigilancia remota por la cámara en el datacenter.
	Daño por mal uso	<ul style="list-style-type: none"> • Definición del área actual como de uso exclusivo para el datacenter. • Implementación del acceso biométrico al datacenter.

Incendio	<ul style="list-style-type: none"> • Definición del área actual como de uso exclusivo para el datacenter. • Mantenimiento y prueba del sensor de humo en el datacenter. • Evaluación de la efectividad del plan de contingencia del datacenter. • Vigilancia remota por la cámara en el datacenter.
Inundación	<ul style="list-style-type: none"> • Vigilancia remota por la cámara en el datacenter. <ul style="list-style-type: none"> • Proteger el sistema de cableado eléctrico que circula por el nivel del piso. • Instalación de los equipos a un nivel superior a 30 cm del piso.
Falla suministro eléctrico	<ul style="list-style-type: none"> • Garantizar el correcto soporte de las UPS.
	<p>Adecuación de una red de suministro eléctrico de contingencia.</p> <ul style="list-style-type: none"> • Implementación de un polo a tierra adecuado para el datacenter.
Falla de equipos de climatización	<ul style="list-style-type: none"> • Garantizar el correcto funcionamiento de las dos unidades de climatización, para contar con respaldo en caso de fallo de la que se encuentre en funcionamiento; para esto se requiere la reparación y actualización tecnológica de estos equipos. • Instalación de la división de seguridad en la zona de servidores, para realizar una mejor distribución de espacios y optimizar el flujo de temperaturas. • Disposición de dos unidades de refrigeración tipo ventilador de torre para el caso de la falla de los equipos de refrigeración.

5.1.2. Riesgos Físicos Externos

Activo	Amenaza	Medidas para reducción del riesgo
Servidores	Robo	<ul style="list-style-type: none"> • Instalación de la división de seguridad para la zona de servidores. • Implementación del acceso biométrico al datacenter. • Vigilancia remota por la cámara del datacenter.
	Daño por evento catastrófico	<ul style="list-style-type: none"> • Evaluación de la efectividad del plan de contingencia del datacenter. • Disponer de un Servidor de contingencia en un sitio diferente al datacenter.

5.1.3. Riesgos Lógicos Internos

Activo	Amenaza	Medidas para reducción del riesgo
Servidores	Acceso a información no autorizada	<ul style="list-style-type: none"> • Establecer políticas de seguridad para el acceso a unidades de almacenamiento del servidor vía red de datos. • Proceso de encriptado de datos en todas las aplicaciones. • Instalación de la división de seguridad para la zona de servidores. • Implementación del acceso biométrico al datacenter. • Implementación del acceso biométrico a las estaciones de trabajo institucionales. • Cierre de sesión automático de acuerdo a políticas.
	Fuga de información	<ul style="list-style-type: none"> • Ejecutar la política de seguridad para el acceso a unidades de almacenamiento del servidor vía red de datos. • Proceso de encriptado de datos en todas las aplicaciones.

		<ul style="list-style-type: none"> • Instalación de la división de seguridad para la zona de servidores. • Implementación del acceso biométrico al datacenter.
	Agotamiento de recursos	<ul style="list-style-type: none"> • Ampliación de las capacidades del servidor principal de datos. • Mantenimiento preventivo de los servidores.
	Instalación y ataque de malware	<ul style="list-style-type: none"> • Antivirus en los servidores. • Actualización periódica del antivirus. • Evaluación de la efectividad del plan de contingencia del datacenter. • Instalación de medidas de seguridad en las estaciones con acceso al servidor tales como bloqueo de puertos USB, software antivirus y software tipo congelador. • Programa de capacitación sobre seguridad informática a los funcionarios.
	Borrado de información	<ul style="list-style-type: none"> • Ejecutar la política de seguridad para el acceso a unidades de almacenamiento del servidor vía red de datos. • Procedimiento de copias de seguridad. • Antivirus en los servidores. • Actualización periódica del antivirus.

5.1.4. Riesgos Lógicos Externos

Activo	Amenaza	Medidas para reducción del riesgo
Servidores	Instalación y ataque de malware	<ul style="list-style-type: none"> • Antivirus en los servidores. • Actualización periódica del antivirus. • Evaluación de la efectividad del plan de contingencia del datacenter. • Mejoramiento de la seguridad perimetral.

	Borrado de información	<ul style="list-style-type: none"> • Antivirus en los servidores. • Actualización periódica del antivirus. • Evaluación de la efectividad del plan de contingencia del datacenter. • Mejoramiento de la seguridad perimetral.
	Acceso a información no autorizada	<ul style="list-style-type: none"> • Antivirus en los servidores. • Evaluación de la efectividad del plan de contingencia del datacenter. • Proceso de encriptado de datos en todas las aplicaciones. • Mejoramiento de la seguridad perimetral.
Estaciones administrativas	Acceso no autorizado a servicios bancarios	<ul style="list-style-type: none"> • Antivirus en las estaciones de trabajo. • Actualización periódica del antivirus. • Programa de capacitación sobre seguridad informática a los funcionarios.

6. POLÍTICA DE ADMINISTRACION DE RIESGOS

La ESE Hospital Regional Manuela Beltrán por medio de su Modelo Integrado de Seguridad y Privacidad de la Información, se compromete a desarrollar una cultura de la gestión del riesgo con la responsabilidad de diseñar, implementar y promover las políticas y controles requeridos en su plataforma informática, enfocados a la prevención y detección de eventos que puedan afectar la misma, garantizando la privacidad de la Información y Seguridad Digital de manera Integral.

7. RECURSOS

La ESE HRMB, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos:

RECURSOS	DETALLE
Humanos	La Subdirección Administrativa y Financiera como líder del proceso de Gestión de la Información, es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la entidad en lo concerniente a la seguridad y privacidad de la información, todo lo anterior con el apoyo de la oficina DATIC, quién cuenta con un funcionario dedicado medio tiempo exclusivamente a estas actividades.
Técnicos	Guías del Ministerio de las TICS y DAFP
Financieros	Asignación presupuestal para el proceso DATIC, aseguramiento de los recursos definidos el PETIC 2024, para el desarrollo de las actividades planteadas en este documento.

8. REFERENCIAS

- MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (2016). GUIA NRO 7.
- <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>
- <http://www.normas-iso.com/iso-27001/>
- https://www.mintic.gov.co/portal/715/articles-135830_plan_tratamiento_seguridad_2020_u20200902.pdf