

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

2023

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	13
1.1.3. Equipos de comunicaciones	13
1.1.4. Equipamiento auxiliar	13
1.1.5. Unidades de Almacenamiento en Red	14
1.1.6. Instalaciones	14
1.1.7. Personal	14
1.2. DEPENDENCIAS ENTRE LOS ACTIVOS	15
1.2.1. Hardware	15
1.2.2. Software	16
1.3. VALORACION DE LOS ACTIVOS	16
1.3.1. Servidores	16
1.3.2. Software	27
1.3.3. Equipo de comunicaciones	28
1.3.4. Equipamiento auxiliar	28
1.3.5. Unidades de Almacenamiento en Red	28
Capítulo 2 – IDENTIFICACION DE CONTROLES EXISTENTES	29
2.1. Identificación de controles existentes	29
Capítulo 3 – IDENTIFICACION DE VULNERABILIDADES	30
Capítulo 4 – CARACTERIZACIÓN DE LAS AMENAZAS	32
4.1. IDENTIFICACIÓN DE AMENAZAS SOBRE LOS ACTIVOS	32
4.2. VALORACION DE LAS AMENAZAS	34
4.2.1. Riesgos Físicos Internos	34
4.2.2. Riesgos Físicos Externos	38
4.2.3. Riesgos Lógicos Internos	39

4.2.4. Riesgos Lógicos Externos	42
4.3. PRIORIZACION DE LAS AMENAZAS	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	50
5.1.3. Riesgos Lógicos Internos	50
5.1.4. Riesgos Lógicos Externos	52
6. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS	54
7. REFERENCIAS	55

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	COORDINADOR PRO
6224	SERVIDOR HP ML110	S/N BCR018N0SF -INTEL XEON QUA	DATIC	COORDINADOR PRO
6435	SERVIDOR HP ML350	PROCESADOR XEON 4 NUCLEOS 2.4G	DATIC	COORDINADOR PRO
9583	SERVIDOR HP ML350	ML350E GEN 8 V2 E5-2404V2 BASE	DATIC	COORDINADOR PRO
7536	SERVIDOR HP PROLIA	INTEL XEON QUAD COREX3430 2.4	DATIC	COORDINADOR PRO
11205	SERVIDOR DELL	DELL T30	DATIC	COORDINADOR PRO

Estaciones de Trabajo

Ref.	Nombre	Ubicación	Responsable
11789	COMPUTADOR HP ProOne 400G5 AiO	ADMINISTRACION FINANCIERA	PROFESIONAL FINANCIERO - FERNANDO PATIÑO
9765	COMPUTADOR COMPACTO	ALMACEN Y SUMINISTROS	GESTION INTEGRAL
6247	TORRE QBEX TWIN3C00	ALMACEN Y SUMINISTROS	GESTION INTEGRAL
6248	TORRE QBEX TWIN3C00	ALMACEN Y SUMINISTROS	GESTION INTEGRAL
4832	COMPUTADOR	APOYO CONTABILIDAD	GESTION INTEGRAL
11200	COMPUTADOR LENOVO	APOYO CONTABILIDAD	GESTION INTEGRAL
4871	COMPUTADOR	APOYO DPTO ENFERMERIA	GESTION INTEGRAL
11783	COMPUTADOR HP ProOne 400G5 AiO	APOYO GESTION DE CALIDAD	GESTION INTEGRAL
7599	TORRE HP PRO	APOYO GESTION DE CALIDAD	GESTION INTEGRAL

7453	COMPUTADOR HP PRO 3130	APOYO OFICINA JURIDICA	GESTION INTEGRAL
9526	COMPUTADOR LENOVO E73Z AIO	APOYO OFICINA JURIDICA	GESTION INTEGRAL
4829	COMPUTADOR	APOYO SUBDIRECCION CIENTIFICA	GESTION INTEGRAL
10817	COMPUTADOR LENOVO AIO V510Z	APOYO SUBDIRECCION CIENTIFICA	GESTION INTEGRAL
7602	COMPUTADOR HPO PRO 3400	ATENCION AL USUARIO SIAU	GESTION INTEGRAL
6985	TORRE QBEX LITE 7E00	ATENCION AL USUARIO SIAU	GESTION INTEGRAL
6990	TORRE QBEX LITE 7E00	ATENCION AL USUARIO SIAU	GESTION INTEGRAL
2535	COMPUTADOR	AUDITORIA MEDICA	GESTION INTEGRAL
10649	COMPUTADOR AIO LENOVO E73Z	AUDITORIA MEDICA	GESTION INTEGRAL
10651	COMPUTADOR AIO LENOVO E73Z	AUDITORIA MEDICA	GESTION INTEGRAL
10653	COMPUTADOR AIO LENOVO E73Z	AUDITORIA MEDICA	GESTION INTEGRAL
10886	COMPUTADOR LENOVO AIO V510Z	AUDITORIA MEDICA	GESTION INTEGRAL
4803	TORRE COMPUTADOR	AUDITORIA MEDICA	GESTION INTEGRAL
12077	COMPUTADOR HP-200	CARTERA	GESTION INTEGRAL
12078	COMPUTADOR HP-200	CARTERA	GESTION INTEGRAL
12079	COMPUTADOR HP-200	BODEGA ALMACEN	GESTION INTEGRAL
12080	COMPUTADOR HP-200	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
12088	COMPUTADOR HP-200	BODEGA ALMACEN	GESTION INTEGRAL
12089	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
12090	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
12091	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
12708	COMPUTADOR HP-200	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
7598	TORRE COMPUTADOR HPO PRO 3400	CARTERA	GESTION INTEGRAL
6967	TORRE QBEX LITE 7E00	CARTERA	GESTION INTEGRAL
11202	COMPUTADOR LENOVO	CENTRAL DE ESTERILIZACION	DARSALUD
10507	COMPUTADOR	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
9466	COMPUTADOR	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
10813	COMPUTADOR LENOVO AIO V510Z	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
10814	COMPUTADOR LENOVO AIO V510Z	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
10815	COMPUTADOR LENOVO AIO V510Z	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
10816	COMPUTADOR LENOVO AIO V510Z	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA
11186	COMPUTADOR LENOVO V530Z	CIRUGIA	ENFERMERA JEFE CIRUGIA - MARTHA SEPULVEDA

5749	COMPUTADOR PORTATIL TOSHIBA	COBRO PREJURIDICO	GESTION INTEGRAL
9767	COMPUTADOR COMPACTO	CONSULTA EXTERNA	DARSALUD
9770	COMPUTADOR COMPACTO	CONSULTA EXTERNA	DARSALUD
11786	COMPUTADOR HP ProOne 400G5 AiO	CONSULTA EXTERNA	DARSALUD
9519	COMPUTADOR LENOVO E73Z AIO	CONSULTA EXTERNA	DARSALUD
9520	COMPUTADOR LENOVO E73Z AIO	CONSULTA EXTERNA	DARSALUD
9525	COMPUTADOR LENOVO E73Z AIO	CONSULTA EXTERNA	DARSALUD
11023	COMPUTADOR LENOVO V310Z	CONSULTA EXTERNA	DARSALUD
9339	TORRE COMPUTADOR	CONSULTA EXTERNA	DARSALUD
7002	TORRE QBEX LITE 7E00	CONSULTA EXTERNA	DARSALUD
6251	TORRE QBEX TWIN 3C00	CONSULTA EXTERNA	DARSALUD
4869	COMPUTADOR	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10496	COMPUTADOR LENOVO AIO E73Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10497	COMPUTADOR LENOVO AIO E73Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10819	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10820	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10821	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10822	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10823	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10824	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10825	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10826	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10827	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10828	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10829	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10830	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10831	COMPUTADOR LENOVO AIO V510Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
9522	COMPUTADOR LENOVO E73Z AIO	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
9528	COMPUTADOR LENOVO E73Z AIO	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA

11021	COMPUTADOR LENOVO V310Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
11022	COMPUTADOR LENOVO V310Z	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
10294	TORRE COMPUTADOR	CONSULTA EXTERNA ESPECIALIZADA	ENFERMERA JEFE LUZ EMILSE ESPINOSA
11198	COMPUTADOR LENOVO	CONTABILIDAD	PROFESIONAL CONTABILIDAD - BLAS ARAQUE
7557	TORRE HP 3400	CONTRATACION	GESTION INTEGRAL
4822	COMPUTADOR	CONTROL INTERNO	JOSE DANIEL ARGUELLO
11096	COMPUTADOR LENOVO	COORDINACIÓN DE NODOS Y TRANSPORTE	GESTION INTEGRAL
10989	LENOVO V310Z ALL-IN-ONE 19.5"	COORDINADOR MEDICO	SUBDIRECCION CIENTIFICA - ORLANDO LESMEZ
9757	COMPUTADOR COMPACTO	COSTOS	GESTION INTEGRAL
7450	COMPUTADOR HP PRO 3130	COSTOS	GESTION INTEGRAL
11163	COMPUTADOR LENOVO	COSTOS	GESTION INTEGRAL
10646	COMPUTADOR AIO LENOVO E73Z	DATIC	GESTION INTEGRAL
11172	COMPUTADOR JANUS	DATIC	GESTION INTEGRAL
5994	COMPUTADOR QBEX APOLO TORRE	DATIC	GESTION INTEGRAL
11164	CPU LENOVO	DATIC	GESTION INTEGRAL
11166	CPU LENOVO	DATIC	GESTION INTEGRAL
11168	CPU LENOVO	DATIC	GESTION INTEGRAL
11170	CPU LENOVO	DATIC	GESTION INTEGRAL
11293	TORRE COMPUTADOR	DATIC	GESTION INTEGRAL
6250	TORRE QBEX TWIN3C00	DATIC	GESTION INTEGRAL
7604	COMPUTADOR HPO PRO 3400	DEPARTAMENTO DE ENFERMERIA/ PROMOCION Y PREVENICION	
9932	COMPUTADOR LENOVO E73Z	DEPARTAMENTO DE ENFERMERIA/ PROMOCION Y PREVENICION	
11235	CPU LENOVO	DEPARTAMENTO DE ENFERMERIA/ PROMOCION Y PREVENICION	
8010	TORRE COMPUTADOR	EDUCACION CONTINUADA DEPARTAMENTO DE ENFERMERIA	
10647	COMPUTADOR AIO LENOVO E73Z	EDUCACION MEDICA - CUARTO DE INTERNOS	SUBDIRECCION CIENTIFICA - ORLANDO LESMEZ
10648	COMPUTADOR AIO LENOVO E73Z	EDUCACION MEDICA - CUARTO DE INTERNOS	SUBDIRECCION CIENTIFICA - ORLANDO LESMEZ
10652	COMPUTADOR AIO LENOVO E73Z	EDUCACION MEDICA - CUARTO DE INTERNOS	SUBDIRECCION CIENTIFICA - ORLANDO LESMEZ
10656	COMPUTADOR AIO LENOVO E73Z	EDUCACION MEDICA - CUARTO DE INTERNOS	SUBDIRECCION CIENTIFICA - ORLANDO LESMEZ
4802	COMPUTADOR	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL
4839	COMPUTADOR	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL
5752	COMPUTADOR HP DX2400 MT	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL
10655	COMPUTADOR AIO LENOVO E73Z	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL

11788	COMPUTADOR HP ProOne 400G5 AiO	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL
7605	COMPUTADOR HPO PRO 3400	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL
11158	COMPUTADOR LENOVO	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL
6999	TORRE QBEX LITE 7E00	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL
6254	TORRE QBEX TWIN 3C00	ESTADISTICA E HISTORIAS CLINICAS	GESTION INTEGRAL
9755	COMPUTADOR COMPACTO	FARMACIA	DARSALUD
9756	COMPUTADOR COMPACTO	FARMACIA	DARSALUD
9768	COMPUTADOR COMPACTO	FARMACIA	DARSALUD
9769	COMPUTADOR COMPACTO	FARMACIA	DARSALUD
6964	TORRE QBEX LITE 7E00	FARMACIA	DARSALUD
6971	TORRE QBEX LITE 7E00	FARMACIA	DARSALUD
7007	TORRE QBEX LITE 7E00	FARMACIA	DARSALUD
989	COMPUTADOR	FARMACIA HATO	DARSALUD
6956	TORRE QBEX LITE 7E00	FARMACIA PALMAS DEL SOCORRO	DARSALUD
7961	COMPUTADOR PORTATIL	FISIOTERAPIA	DARSALUD
5951	COMPUTADOR QBEX LITE5 - TORRE	FISIOTERAPIA	DARSALUD
5949	COMPUTADOR QBEX LITE5- TORRE CONS 1	FISIOTERAPIA	DARSALUD
6979	TORRE QBEX LITE 7E00	FISIOTERAPIA	DARSALUD
6963	TORRE QBEX LITE 7E00	FISIOTERAPIA	DARSALUD
6977	TORRE QBEX LITE 7E00	FISIOTERAPIA	DARSALUD
6988	TORRE QBEX LITE 7E00	FISIOTERAPIA	DARSALUD
6986	TORRE QBEX LITE 7E00	FISIOTERAPIA	DARSALUD
9855	COMPUTADOR PORTATIL	FONOAUDIOLOGIA	DARSALUD
10812	COMPUTADOR LENOVO AIO V510Z	GERENCIA	GERENCIA-PABLO CACERES
11007	COMPUTADOR LENOVO V310Z	GERENCIA	GERENCIA-PABLO CACERES
11185	COMPUTADOR PORTATIL LENOVO	GERENCIA	GERENCIA-PABLO CACERES
6983	TORRE QBEX LITE 7E00	GESTION AMBIENTAL	GESTION INTEGRAL
10654	COMPUTADOR AIO LENOVO E73Z	GESTION DE CALIDAD	PROFESION CALIDAD - YULI BARRIOS
10657	COMPUTADOR AIO LENOVO E73Z	GESTION DE CALIDAD	PROFESION CALIDAD - YULI BARRIOS
6292	COMPUTADOR PORTATIL HP4520S	GESTION DE CALIDAD	PROFESION CALIDAD - YULI BARRIOS
4836	COMPUTADOR	GESTION DOCUMENTAL	GESTION INTEGRAL
5957	COMPUTADOR QBEX LITE5- TORRE	GESTION DOCUMENTAL	GESTION INTEGRAL
10480	COMPUTADOR PORTATIL	GESTORA HOSPITALARIA	DARSALUD
9759	COMPUTADOR COMPACTO	GINECOBSTETRICIA	DARSALUD
9764	COMPUTADOR COMPACTO	GINECOBSTETRICIA	DARSALUD
10494	COMPUTADOR LENOVO AIO E73Z	GINECOBSTETRICIA	DARSALUD

11002	COMPUTADOR LENOVO V310Z	GINECOBSTETRICIA	DARSALUD
11003	COMPUTADOR LENOVO V310Z	GINECOBSTETRICIA	DARSALUD
10490	COMPUTADOR PORTATIL HP 450G3	GINECOBSTETRICIA	DARSALUD
5953	COMPUTADOR QBEX LITE5-TORRE	INSTRUMENTACION	DARSALUD
6253	TORRE QBEX TWIN C3C00	INSTRUMENTACION	DARSALUD
9931	COMPUTADOR LENOVO E73Z	INVENTARIOS	GESTION INTEGRAL
4833	COMPUTADOR	JEFE DE INFECCIONES	DARSALUD
12075	COMPUTADOR HP-200	LABORATORIO CLINICO	DARSALUD
12076	COMPUTADOR HP-200	LABORATORIO CLINICO	DARSALUD
10511	COMPUTADOR PORTATIL	LABORATORIO CLINICO	DARSALUD
4830	COMPUTADOR	MANTENIMIENTO	GESTION INTEGRAL
4837	COMPUTADOR	MANTENIMIENTO	GESTION INTEGRAL
11787	COMPUTADOR HP ProOne 400G5 AiO	MANTENIMIENTO	GESTION INTEGRAL
4840	COMPUTADOR LENOVO	MANTENIMIENTO	GESTION INTEGRAL
5919	CPU ESTACION	MANTENIMIENTO	GESTION INTEGRAL
9485	COMPUTADOR	MEDICINA INTERNA	DARSALUD
9762	COMPUTADOR COMPACTO	MEDICINA INTERNA	DARSALUD
9763	COMPUTADOR COMPACTO	MEDICINA INTERNA	DARSALUD
12081	COMPUTADOR HP-200	MEDICINA INTERNA	DARSALUD
11199	COMPUTADOR LENOVO	MEDICINA INTERNA	DARSALUD
11201	COMPUTADOR LENOVO	MEDICINA INTERNA	DARSALUD
10495	COMPUTADOR LENOVO AIO E73Z	MEDICINA INTERNA	DARSALUD
6289	COMPUTADOR PORTATIL HP4520S	MEDICINA INTERNA	DARSALUD
7601	TORRE COMPUTADOR HPO PRO 3400	MEDICINA LEGAL / MORGUE	DARSALUD
10990	LENOVO V310Z ALL-IN-ONE 19.5"	MÉDICO DE INFECCIONES	DARSALUD
10650	COMPUTADOR AIO LENOVO E73Z	MEDICOS HOSPITALARIOS	DARSALUD
7452	COMPUTADOR HP PRO 3130	ODONTOLOGIA	DARSALUD
6957	TORRE QBEX LITE 7E00	ODONTOLOGIA	DARSALUD
9523	COMPUTADOR LENOVO E73Z AIO	ODONTOLOGIA ESPECIALIZADA MAXILO/ORTODONCIA	DARSALUD
2078	CPU	ODONTOLOGIA HATO	DARSALUD
4841	COMPUTADOR	ODONTOLOGIA PALMAS DEL SOCORRO	DARSALUD
11784	COMPUTADOR HP ProOne 400G5 AiO	OFICINA ASESORA GERENCIA	PROFESIONAL ASESOR GERENCIA
7008	TORRE QBEX LITE 7E00	OFICINA ASESORA GERENCIA	PROFESIONAL ASESOR GERENCIA
11598	COMPUTADOR LENOVO AIO V530	OFICINA DE MERCADEO	GESTION INTEGRAL
10982	COMPUTADOR LENOVO	OFICINA JURIDICA Y CONTRATACION	PROFESIONAL JURIDICO
11004	COMPUTADOR LENOVO V310Z	PEDIATRIA	DARSALUD
11005	COMPUTADOR LENOVO V310Z	PEDIATRIA	DARSALUD
10991	LENOVO V310Z ALL-IN-ONE 19.5"	PEDIATRIA	DARSALUD

10992	LENOVO V310Z ALL-IN-ONE 19.5"	PEDIATRIA	DARSALUD
7563	TORRE HP PRO 3400	PROGRAMACION DE CIRUGIA	DARSALUD
9524	COMPUTADOR LENOVO E73Z AIO	PROMOCION Y PREVENCION	DARSALUD
11233	CPU LENOVO	PROMOCION Y PREVENCION	DARSALUD
4834	COMPUTADOR	PSICOLOGIA COVID	DARSALUD
10406	COMPUTADOR	PUESTO DE SALUD DE PALMAS	DARSALUD
10514	COMPUTADOR	PUESTO DE SALUD DE PALMAS	DARSALUD
7559	TORRE HP 3400	PUESTO DE SALUD DE PALMAS	DARSALUD
10485	TORRE LENOVO THINKCENTRE	PUESTO DE SALUD DE PALMAS	DARSALUD
10407	COMPUTADOR	PUESTO DE SALUD DEL HATO	DARSALUD
7451	COMPUTADOR HP PRO 3130	PUESTO DE SALUD DEL HATO	DARSALUD
11020	CPU JANUS	PUESTO DE SALUD DEL HATO	DARSALUD
7603	TORRE HPO PRO 3400	PUESTO DE SALUD DEL HATO	DARSALUD
6961	TORRE QBEX LITE 7E00	PUESTO DE SALUD DEL HATO	DARSALUD
6249	TORRE QBEX TWIN3C00	PUESTO DE SALUD DEL HATO	DARSALUD
9754	COMPUTADOR COMPACTO	QUIRURGICAS	DARSALUD
9761	COMPUTADOR COMPACTO	QUIRURGICAS	DARSALUD
10498	COMPUTADOR LENOVO AIO E73Z	QUIRURGICAS	DARSALUD
10500	COMPUTADOR LENOVO AIO E73Z	QUIRURGICAS	DARSALUD
9935	COMPUTADOR LENOVO E73Z	QUIRURGICAS	DARSALUD
6291	COMPUTADOR PORTATIL HP4520S	QUIRURGICAS	DARSALUD
6994	TORRE QBEX LITE 7E00	RAYOS X	GONZALEZ FLOREZ
6974	TORRE QBEX LITE 7E00	RAYOS X	GONZALEZ FLOREZ
6995	TORRE QBEX LITE 7E00	RAYOS X	GONZALEZ FLOREZ
11160	COMPUTADOR LENOVO	REFERENCIA Y CONTRAREFERENCIA	GESTION INTEGRAL
11162	COMPUTADOR LENOVO	REFERENCIA Y CONTRAREFERENCIA	GESTION INTEGRAL
7600	TORRE HPO PRO 3400	REVISORIA FISCAL	REVISOR FISCAL
10981	COMPUTADOR LENOVO	SALUD OCUPACIONAL	DARSALUD
11781	COMPUTADOR HP ProOne 400G5 AiO	SECRETARIA GERENCIA	GESTION INTEGRAL
11320	COMPUTADOR TODO EN UNO LENOVO	SECRETARIO SUBGERENCIA ADMINISTRATIVA	GESTION INTEGRAL
10897	COMPUTADOR LENOVO	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	SUBDIRECTORA ADMNISTRATIVA
11187	COMPUTADOR LENOVO V530Z	SUBDIRECCION CIENTIFICA	SUBDIRECTOR CIENTIFICO
5952	COMPUTADOR QBEX LITE5- TORRE	SUBDIRECCION CIENTIFICA	SUBDIRECTOR CIENTIFICO
619	COMPUTADOR	TALENTO HUMANO	PROFESIONAL TALENTO HUMANO
7951	TORRE COMPUTADOR CPU ARGOM TX -373	TERAPIA OCUPACIONAL	DARSALUD
11785	COMPUTADOR HP ProOne 400G5 AiO	TESORERIA	GESTION INTEGRAL
11294	LENOVO V330	UCI ADULTOS	DARSALUD
11295	LENOVO V330	UCI ADULTOS	DARSALUD

11296	LENOVO V330	UCI ADULTOS	DARSALUD
11297	LENOVO V330	UCI ADULTOS	DARSALUD
9724	COMPUTADOR COMPACTO	UNIDAD DE CUIDADO INTENSIVO- COVID 19	DARSALUD
9516	COMPUTADOR LENOVO E73Z AIO	UNIDAD DE CUIDADO INTENSIVO- COVID 19	DARSALUD
6290	COMPUTADOR PORTATIL HP4520S	UNIDAD DE CUIDADO INTENSIVO- COVID 19	DARSALUD
11203	COMPUTADOR LENOVO	UNIDAD DE CUIDADOS INTENSIVOS NEONATALES	DARSALUD
11204	COMPUTADOR LENOVO	UNIDAD DE CUIDADOS INTENSIVOS NEONATALES	DARSALUD
9760	COMPUTADOR COMPACTO	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
9766	COMPUTADOR COMPACTO	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
12082	COMPUTADOR HP-200	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
11157	COMPUTADOR LENOVO	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
11161	COMPUTADOR LENOVO	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
10499	COMPUTADOR LENOVO AIO E73Z	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
10818	COMPUTADOR LENOVO AIO V510Z	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
9933	COMPUTADOR LENOVO E73Z	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
9934	COMPUTADOR LENOVO E73Z	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
5948	COMPUTADOR QBEX LITE5 - TORRE CONS 4	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
7001	TORRE QBEX LITE7E00	URGENCIAS CONSULTA Y PROCEDIMIENTOS	DARSALUD
10298	COMPUTADOR LENOVO C260	URGENCIAS OBSERVACION	DARSALUD
9725	COMPUTADOR COMPACTO	URGENCIAS OBSERVACION	DARSALUD
9758	COMPUTADOR COMPACTO	URGENCIAS OBSERVACION	DARSALUD
9517	COMPUTADOR LENOVO E73Z AIO	URGENCIAS OBSERVACION	DARSALUD
9518	COMPUTADOR LENOVO E73Z AIO	URGENCIAS OBSERVACION	DARSALUD
9521	COMPUTADOR LENOVO E73Z AIO	URGENCIAS OBSERVACION	DARSALUD
10491	COMPUTADOR PORTATIL HP 450G3	URGENCIAS OBSERVACION	DARSALUD
10492	COMPUTADOR PORTATIL HP 450G3	URGENCIAS OBSERVACION	DARSALUD
10405	COMPUTADOR	VACUNACION	DARSALUD
7461	COMPUTADOR HEWLET PACKARD	VACUNACION	DARSALUD
10357	COMPUTADOR	VACUNACION COVID 19	DARSALUD
6293	COMPUTADOR PORTATIL HP4520S	VACUNACION COVID 19	DARSALUD
5750	COMPUTADOR PORTATIL TOSHIBA	VACUNACION COVID 19	DARSALUD
9527	COMPUTADOR LENOVO E73Z AIO	VENTANILLA UNICA	GESTION INTEGRAL
4825	COMPUTADOR	VIGILANCIA Y SEGURIDAD	DETECCION LIMITADA
5751	HP DX2400 MT - TORRE	VIGILANCIA Y SEGURIDAD	DETECCION LIMITADA
6973	TORRE QBEX LITE 7E00	VIGILANCIA Y SEGURIDAD	DETECCION LIMITADA
6252	TORRE QBEX TWIN 3C00	VIGILANCIA Y SEGURIDAD	DETECCION LIMITADA
6255	TORRE QBEX TWIN 3C00	VIGILANCIA Y SEGURIDAD	DETECCION LIMITADA

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
Histosoft	Historia clínica asistencial, proceso de almacén e inventarios, mantenimiento, cartera, tesorería, gestión documental, talento humano.	Toda la institución
Medisoft	Facturación servicios de salud prestados	Proceso de Facturación
GD	Información contable y tesorería	Contabilidad
Sicosalud	Registro y generación de informes sobre costos de producción	Costos
Coco	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	COORDINADOR PRO
10801	SWITCH	ARUBA	DATIC	COORDINADOR PRO
10802	SWITCH	ARUBA	DATIC	COORDINADOR PRO
11542	SWITCH	JH295A	DATIC	COORDINADOR PRO
	SWITCH	HP V1910	URGENCIAS	COORDINADOR URGENCIAS
6268	SWITCH HP NETWORK	927FCPRB460E4 SWITCH PH NETWORK	DATIC	COORDINADOR PRO
7587	SWITCH HP V1910-4	S/N CN 18BX53VS HP 660008353	DATIC	COORDINADOR PRO
6269	SWITHC HP NETWORK	927FCPRA0491F SWITCH HP NETW	DATIC	COORDINADOR PRO

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

4904	UPS ENERGEX	Soporte de reserva	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

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

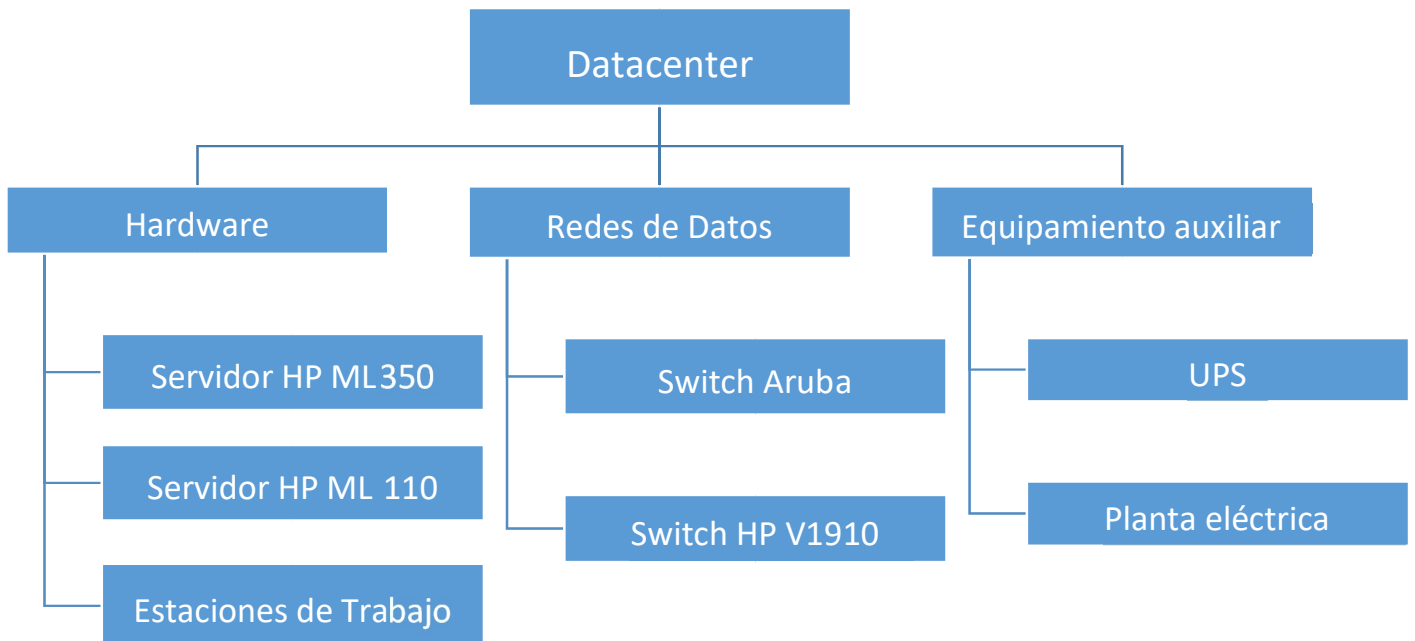
El soporte y desarrollo de la plataforma está a cargo del personal de DATIC, el cual hace parte de un proceso subcontrato por la institución.

Cargo	Funciones
Coordinador DATIC	Coordinación de actividades, manejo de gerencia de procesos, diseño y desarrollo de software de la plataforma.

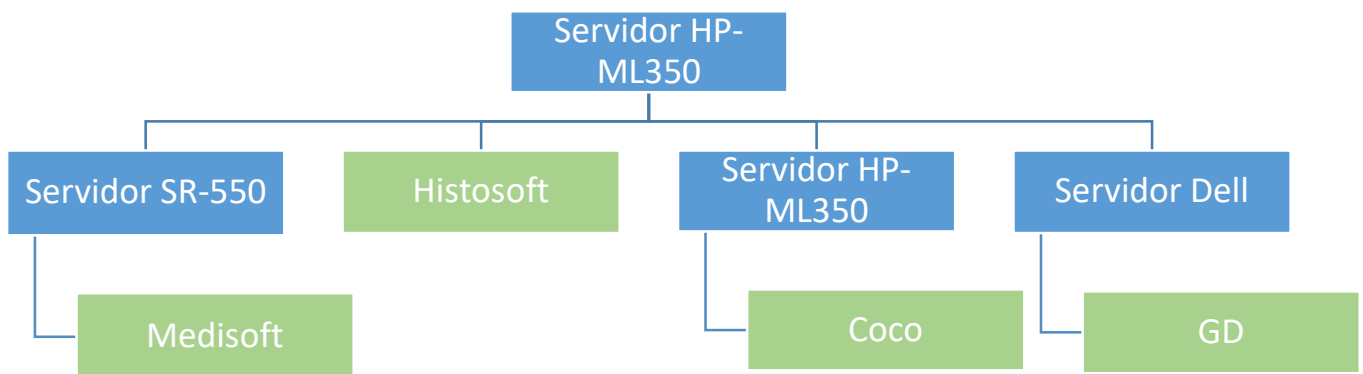
Ingeniero de Soporte	Soporte a plataforma histosoft, aplicativos web, diseño y desarrollo página web
Tecnólogo de Soporte 1	Soporte a software básico, intranet, Enterprise, internet y redes de datos.
Tecnólogo de Soporte 2	Soporte a Medisoft seguridad informática.
Tecnólogo de Soporte 3	Soporte a hardware 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	Alto	Daño grave
3-5	Medio	Daño muy importante
1-2	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
6435	SERVIDOR HP ML350 G6	DATIC	8.2
9583	SERVIDOR HP ML350 G8	DATIC	5
12446	SERVIDOR LEN MR550	DATIC	7.1
11205	SERVIDOR DELL	DATIC	5
7536	SERVIDOR HP ML110	DATIC	5

Estaciones de Trabajo

Refer	Nombre Elemento	Ubicación Actual	Valor
4834	COMPUTADOR	ADMINISTRACION FINAN	2
4835	COMPUTADOR	ATENCION AL USU	2
4829	COMPUTADOR	ATENCION AL USU	2
2535	COMPUTADOR	AUDITORIA MEDIC	2
4869	COMPUTADOR	CARDIOLOGIA	2
10507	COMPUTADOR	CIRUGIA	2
9466	COMPUTADOR	CIRUGIA	2
4832	COMPUTADOR	CONTABILIDAD	2
4837	COMPUTADOR	CONTABILIDAD	2
4822	COMPUTADOR	CONTROL INTERNO	2
4807	COMPUTADOR	DATIC	3
4871	COMPUTADOR	DEPARTAMENTO DE	2

619	COMPUTADOR	ESTADISTICA E H	2
4827	COMPUTADOR	ESTADISTICA E H	2
4825	COMPUTADOR	ESTADISTICA E H	2
989	COMPUTADOR	FARMACIA HATO	2
4830	COMPUTADOR	MANTENIMIENTO	2
4802	COMPUTADOR	ODONTOLOGIA	2
4841	COMPUTADOR	ODONTOLOGIA PAL	2
4836	COMPUTADOR	OFICINA DE MERC	3
10406	COMPUTADOR	PUESTO DE SALUD	2
10514	COMPUTADOR	PUESTO DE SALUD	2
10513	COMPUTADOR	PUESTO DE SALUD	2
10407	COMPUTADOR	PUESTO DE SALUD	2
4826	COMPUTADOR	SECRETARIA GERE	3
4474	COMPUTADOR	VIGILANCIA Y SE	2
4833	COMPUTADOR	COMITE DE INFEC	2
10357	COMPUTADOR	CONSULTA EXTERN	2
4477	COMPUTADOR	DATIC	3
9485	COMPUTADOR	URGENCIAS CONSU	2
10405	COMPUTADOR	VACUNACION	3
5752	COMPUTADOR HP DX2	ESTADISTICA E H	3
7452	COMPUTADOR HP PRO	ODONTOLOGIA	2
4828	COMPUTADOR LENOVO	COSTOS	3

10298	COMPUTADOR LENOVO	URGENCIAS OBSER	2
10653	COMPUTADOR AIO LEN	AUDITORIA MEDIC	2
10649	COMPUTADOR AIO LEN	AUDITORIA MEDIC	2
10651	COMPUTADOR AIO LEN	AUDITORIA MEDIC	2
10655	COMPUTADOR AIO LEN	CONSULTA EXTERN	2
10656	COMPUTADOR AIO LEN	EDUCACION MEDIC	2
10652	COMPUTADOR AIO LEN	EDUCACION MEDIC	2
10648	COMPUTADOR AIO LEN	EDUCACION MEDIC	2
10647	COMPUTADOR AIO LEN	EDUCACION MEDIC	2
10657	COMPUTADOR AIO LEN	GESTION DE CALI	3
10654	COMPUTADOR AIO LEN	GESTION DE CALI	2
10650	COMPUTADOR AIO LEN	MEDICOS HOSPITA	2
10646	COMPUTADOR AIO LEN	SUBDIRECCION CI	3
9765	COMPUTADOR COMPACT	CARTERA	2
9757	COMPUTADOR COMPACT	CONSULTA EXTERN	2
9767	COMPUTADOR COMPACT	CONSULTA EXTERN	2
9770	COMPUTADOR COMPACT	CONSULTA EXTERN	2
9766	COMPUTADOR COMPACT	CONSULTA EXTERN	2
9769	COMPUTADOR COMPACT	FARMACIA	2
9768	COMPUTADOR COMPACT	FARMACIA	2
9756	COMPUTADOR COMPACT	FARMACIA	2
9755	COMPUTADOR COMPACT	FARMACIA	2

9764	COMPUTADOR COMPACT	GINECOBSTETRICI	2
9759	COMPUTADOR COMPACT	GINECOBSTETRICI	2
9762	COMPUTADOR COMPACT	MEDICINA INTERN	2
9763	COMPUTADOR COMPACT	MEDICINA INTERN	2
9754	COMPUTADOR COMPACT	QUIRURGICAS	2
9761	COMPUTADOR COMPACT	QUIRURGICAS	2
9760	COMPUTADOR COMPACT	URGENCIAS CONSU	2
9724	COMPUTADOR COMPACT	URGENCIAS OBSER	2
9758	COMPUTADOR COMPACT	URGENCIAS OBSER	2
9725	COMPUTADOR COMPACT	URGENCIAS OBSER	2
7461	COMPUTADOR HEWLET	VACUNACION	2
5751	COMPUTADOR HP DX24	VIGILANCIA Y SE	2
7450	COMPUTADOR HP PRO	ADMINISTRACION	2
7453	COMPUTADOR HP PRO	OFICINA JURIDIC	3
7451	COMPUTADOR HP PRO	PUESTO DE SALUD	2
7604	COMPUTADOR HPO PRO	ALMACEN Y SUMIN	3
7600	COMPUTADOR HPO PRO	CONTABILIDAD	3
7602	COMPUTADOR HPO PRO	COORDINACION DE	2
7605	COMPUTADOR HPO PRO	ESTADISTICA E H	2
7599	COMPUTADOR HPO PRO	GESTION DE CALI	2
7603	COMPUTADOR HPO PRO	PUESTO DE SALUD	2
4823	COMPUTADOR LENOVO	INSTRUMENTACION	2

10982	COMPUTADOR LENOVO	OFICINA JURIDIC	3
10897	COMPUTADOR LENOVO	SUBDIRECCION AD	3
10981	COMPUTADOR LENOVO	COORDINADOR MED	3
4840	COMPUTADOR LENOVO	MANTENIMIENTO	2
10498	COMPUTADOR LENOVO	CONSULTA EXTERN	2
10497	COMPUTADOR LENOVO	CONSULTA EXTERN	2
10496	COMPUTADOR LENOVO	CONSULTA EXTERN	2
10494	COMPUTADOR LENOVO	GINECOBSTETRICI	2
10495	COMPUTADOR LENOVO	MEDICINA INTERN	2
10500	COMPUTADOR LENOVO	QUIRURGICAS	2
10499	COMPUTADOR LENOVO	URGENCIAS CONSU	2
10886	COMPUTADOR LENOVO	AUDITORIA MEDIC	2
10825	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10821	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10828	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10824	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10831	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10827	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10823	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10830	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10826	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10822	COMPUTADOR LENOVO	BODEGA ALMACEN	2

10829	COMPUTADOR LENOVO	BODEGA ALMACEN	2
10814	COMPUTADOR LENOVO	CIRUGIA	2
10813	COMPUTADOR LENOVO	CIRUGIA	2
10816	COMPUTADOR LENOVO	CIRUGIA	2
10815	COMPUTADOR LENOVO	CIRUGIA	2
10818	COMPUTADOR LENOVO	CONSULTA EXTERN	2
10820	COMPUTADOR LENOVO	CONSULTA EXTERN	2

10819	COMPUTADOR LENOVO	CONSULTA EXTERN	2
10812	COMPUTADOR LENOVO	GERENCIA	3
10817	COMPUTADOR LENOVO	SUBDIRECCION CI	3
9935	COMPUTADOR LENOVO	CONSULTA EXTERN	2
9932	COMPUTADOR LENOVO	DEPARTAMENTO DE	3
9931	COMPUTADOR LENOVO	INVENTARIOS	3
9933	COMPUTADOR LENOVO	URGENCIAS CONSU	2
9934	COMPUTADOR LENOVO	URGENCIAS OBSER	2
9528	COMPUTADOR LENOVO	CARDIOLOGIA	2
9525	COMPUTADOR LENOVO	CONSULTA EXTERN	2
9519	COMPUTADOR LENOVO	CONSULTA EXTERN	2
9526	COMPUTADOR LENOVO	OFICINA JURIDIC	3
9524	COMPUTADOR LENOVO	PROMOCION Y PRE	2
9522	COMPUTADOR LENOVO	RAYOS X	2

9523	COMPUTADOR LENOVO	TALENTO HUMANO	2
9518	COMPUTADOR LENOVO	URGENCIAS OBSER	2
9521	COMPUTADOR LENOVO	URGENCIAS OBSER	2
9517	COMPUTADOR LENOVO	URGENCIAS OBSER	2
9520	COMPUTADOR LENOVO	URGENCIAS OBSER	2
9516	COMPUTADOR LENOVO	URGENCIAS OBSER	2
9527	COMPUTADOR LENOVO	VENTANILLA UNIC	3
9772	COMPUTADOR PORTATI	ASESOR GERENCIA	2
10480	COMPUTADOR PORTATI	CLINICA DE HERI	2
10511	COMPUTADOR PORTATI	CONSULTA EXTERN	2
7961	COMPUTADOR PORTATI	FISIOTERAPIA	5
9855	COMPUTADOR PORTATI	FONOAUDIOLOGIA	5
6270	COMPUTADOR PORTATI	GERENCIA	3
10490	COMPUTADOR PORTATI	GINECOBSTETRICI	2
10491	COMPUTADOR PORTATI	URGENCIAS OBSER	2
10492	COMPUTADOR PORTATI	URGENCIAS OBSER	2
6292	COMPUTADOR PORTATI	DEPARTAMENTO DE	2
6293	COMPUTADOR PORTATI	GINECOBSTETRICI	2
6289	COMPUTADOR PORTATI	MEDICINA INTERN	2
6290	COMPUTADOR PORTATI	PEDIATRIA	2
6291	COMPUTADOR PORTATI	QUIRURGICAS	2
5750	COMPUTADOR PORTATI	GESTION DE CALI	2

5749	COMPUTADOR PORTATI	COBRO COACTIVO	2
5994	COMPUTADOR QBEX AP	DATIC	5
5959	COMPUTADOR QBEX LI	ESTADISTICA E H	2
5951	COMPUTADOR QBEX LI	FISIOTERAPIA	2
5948	COMPUTADOR QBEX LI	URGENCIAS CONSU	2
5947	COMPUTADOR QBEX LI	NUTRICION	2
5957	COMPUTADOR QBEX LI	DEPARTAMENTO DE	2
5953	COMPUTADOR QBEX LI	INSTRUMENTACION	2
5952	COMPUTADOR QBEX LI	MANTENIMIENTO	2
5949	COMPUTADOR QBEX LI	FISIOTERAPIA	2
5960	COMPUTADOR QBEX LI	MEDICINA INTERN	2
5955	COMPUTADOR QBEX LI	FONOAUDIOLOGIA	2
5961	COMPUTADOR QBEX LI	MEDICINA INTERN	2
5950	COMPUTADOR QBEX LI	DEVOLUTIVOS EN	2
2078	CPU COMPAQ	ODONTOLOGIA HAT	2
5919	CPU ESTACION	COORDINACION DE	2
8617	CPU LENOVO	LABORATORIO CLI	2
8619	CPU LENOVO	LABORATORIO CLI	2
8615	CPU LENOVO	LABORATORIO CLI	2
10990	LENOVO V310Z ALL-I	COMITE DE INFEC	2
10989	LENOVO V310Z ALL-I	MEDICOS HOSPITA	2

10992	LENOVO V310Z ALL-I	PEDIATRIA	2
10991	LENOVO V310Z ALL-I	PEDIATRIA	2
9537	LICENCIA ORACLE EN	RAYOS X	2
9529	SCANNER HP SJ FLOW	OFICINA JURIDIC	3
9530	SCANNER HP SJ FLOW	OFICINA JURIDIC	3
9930	SCANNER HP	DEPARTAMENTO DE	2
9929	SCANNER HP	VENTANILLA UNIC	5
9928	SCANNER HP	COSTOS	5
7561	SCANNER HP 7000	SUBDIRECCION AD	3
9531	SCANNER HP 7500	ARCHIVO	3
10294	TORRE COMPUTADOR	CONSULTA EXTERN	2
9339	TORRE COMPUTADOR	DEPARTAMENTO DE	3
8010	TORRE COMPUTADOR	EDUCACION CONTI	2
4803	TORRE COMPUTADOR	AUDITORIA MEDIC	2
7951	TORRE COMPUTADOR C	URGENCIAS CONSU	2
7598	TORRE COMPUTADOR H	CARTERA	3
7601	TORRE COMPUTADOR H	URGENCIAS CONSU	2
5956	TORRE COMPUTADOR Q	COSTOS	3
7557	TORRE HP 3400	ASESOR GERENCIA	2
7559	TORRE HP 3400	PUESTO DE SALUD	2
7563	TORRE HP PRO 3400	PROGRAMACION DE	2
10485	TORRE LENOVO THINK	PUESTO DE SALUD	2

2539	TORRE QBEX	FARMACIA PALMAS	2
6968	TORRE QBEX LITE 7E	CARTERA	2
6967	TORRE QBEX LITE 7E	CARTERA	2
6979	TORRE QBEX LITE 7E	FISIOTERAPIA	2
6994	TORRE QBEX LITE 7E	RAYOS X	2
6973	TORRE QBEX LITE 7E	VIGILANCIA Y SE	2
6981	TORRE QBEX LITE 7E	ARCHIVO	3
6963	TORRE QBEX LITE 7E	CONSULTA EXTERN	2
7002	TORRE QBEX LITE 7E	CONSULTA EXTERN	2
6964	TORRE QBEX LITE 7E	COORDINADOR HSE	2
6999	TORRE QBEX LITE 7E	ESTADISTICA E H	2
6971	TORRE QBEX LITE 7E	FARMACIA	2
6983	TORRE QBEX LITE 7E	GESTION AMBIENT	2
6988	TORRE QBEX LITE 7E	LABORATORIO CLI	2
6985	TORRE QBEX LITE 7E	LABORATORIO CLI	2
7008	TORRE QBEX LITE 7E	PEDIATRIA	2
6995	TORRE QBEX LITE 7E	RAYOS X	1
6974	TORRE QBEX LITE 7E	RAYOS X	1
6956	TORRE QBEX LITE 7E	SECRETARIA SUBG	1
7007	TORRE QBEX LITE 7E	TERAPIA OCUPACI	2
6990	TORRE QBEX LITE 7E	URGENCIAS OBSER	2
6961	TORRE QBEX LITE 7E	URGENCIAS OBSER	2

6977	TORRE QBEX LITE 7E	VIGILANCIA Y SE	2
6986	TORRE QBEX LITE 7E	FISIOTERAPIA	2
6957	TORRE QBEX LITE 7E	ODONTOLOGIA	2
7001	TORRE QBEX LITE7E0	URGENCIAS OBSER	2
6251	TORRE QBEX TWIN 3C	CONSULTA EXTERN	2
6254	TORRE QBEX TWIN 3C	GINECOBSTETRICI	2
6252	TORRE QBEX TWIN 3C	PEDIATRIA	2
6255	TORRE QBEX TWIN 3C	VIGILANCIA Y SE	2
6253	TORRE QBEX TWIN C3	GINECOBSTETRICI	2
6248	TORRE QBEX TWIN3C0	ALMACEN Y SUMIN	3
6247	TORRE QBEX TWIN3C0	ALMACEN Y SUMIN	2
6250	TORRE QBEX TWIN3C0	MEDICINA INTERN	2
6249	TORRE QBEX TWIN3C0	MEDICINA INTERN	2

1.3.2. Software

Nombre del Aplicativo	Funciones	Ubicación	Valor
Histosoft	Historia clínica asistencial, proceso de almacén e inventarios, mantenimiento, cartera, tesorería, gestión documental, talento humano.	Toda la institución	10
Medisoft	Facturación servicios de salud prestados	Proceso de Facturación	10
GD	Información contable y tesorería	Contabilidad	5
Sicosalud	Registro y generación de informes sobre costos de producción	Costos	3
Enterprise	Automatización de procesos laboratorio clínico.	Área asistencial	8
Coco	Asignación de citas para consulta externa	Estadística – Consulta externa	5

1.3.3. Equipos de Comunicaciones

Refer	Nombre Elemento	Ubicación Actual	Valor
10801	SWITCH	DATIC	8
10802	SWITCH	DATIC	8
5753	SWITCH	DATIC	3
4943	SWITCH	DATIC	5
	SWITCH	URGENCIAS	8
6268	SWITCH HP NETWORK	DATIC	5
7587	SWITCH HP V1910-4	DATIC	5
6269	SWITHC HP NETWORK	DATIC	3

1.3.4. Equipamiento auxiliar

Refer	Nombre Elemento	Ubicación Actual	Valor
10803	UPS SU3000XL	DATIC	6
4904	UPS ENERGEX	DATIC	3
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

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 medianamente 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 Software tipo “congelador” Encriptado de datos en algunas tablas Procedimiento de copias de seguridad Perfiles de acceso a los diferentes aplicativos
Riesgos Lógicos Externos	Software Antivirus Perfiles de acceso a los diferentes aplicativos Encriptado de datos en algunas tablas Procedimiento de copias de seguridad Seguridad perimetral básica

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	
	Procedimientos inadecuados de contratación	-Fuga de información
		-Daño por mal uso, destrucción, falta de mantenimiento
	Entrenamiento insuficiente en seguridad	-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	11205-SERVIDOR DELL T30	Robo	5	2	4.1
		Daño por mal uso	5	3	4.4
		Incendio	5	2	4.1
		Inundación	5	1	3.5
		Falla suministro eléctrico	5	5	5
		Falla de equipos de climatización	5	4	4.7
	12446 – Servidor SR550	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
	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
	7536- SERVIDOR HP PROLIANT	Robo	7	2	5.5
		Daño por mal uso	7	3	5.8
		Incendio	7	2	5.5
		Inundación	7	1	5.2
		Falla suministro eléctrico	7	5	6.4
		Falla de equipos de climatización	7	4	6.1

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 – Área asistencial	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
		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	11205 – SERVIDOR DELL T30	Robo	5	2	4.1
		Daño por evento catastrófico	5	1	3.8
	6435-SERVIDOR HP ML350 G6	Robo	10	2	7.6
		Daño por evento catastrófico	10	1	7.3
	9583 - SERVIDOR HP ML350 G8	Robo	10	2	7.6
		Daño por evento catastrófico	10	1	7.3
	7536- SERVIDOR HP PROLIANT	Robo	7	2	5.5
		Daño por evento catastrófico	7	1	5.2
	12446 – SERVIDOR MR550	Robo	8	2	6.2
		Daño por evento catastrófico	8	1	5.9

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
Equipos de Comunicaciones	Switch de valor nivel 5	Robo	8	2	6.2
		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 tipo congelador en gran parte de las estaciones, el cual permite preservar la estabilidad de su sistema operativo y configuración básica, solamente algunos equipos tienen habilitado la opción de almacenamiento local de información.
- 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	11205 – SERVIDOR DELL T30	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	10	5	8.5
	7536- SERVIDOR HP ML110	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	3	4.4
		Agotamiento de recursos	5	4	4.7
	12446 - Servidor SR-550	Instalación y ataque de malware	8	3	6.5
		Borrado de información	8	2	6.2
		Acceso a información no autorizada	8	4	6.8
		Fuga de información	8	4	6.8
		Agotamiento de recursos	8	5	7.1

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 valor nivel 5	Instalación y ataque de malware	5	2	4.1

Estaciones de Trabajo – Área asistencial		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	11205 – SERVIDOR DELL T30	Instalación y ataque de malware	5	5	5
		Borrado de información	5	5	5
		Acceso a información no autorizada	5	4	4.7
		Acceso a servicios bancarios	1	1	1
	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	10	5	8.5
	Borrado de información	10	5	8.5
	Acceso a información no autorizada	10	4	8.2
	Acceso a servicios bancarios	1	1	1
7536- SERVIDOR HP ML110	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
12446 – Servidor SR550	Instalación y ataque de malware	8	5	7.1
	Borrado de información	8	5	7.1
	Acceso a información no autorizada	6	4	5.4
	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

Tipo	Nombre Elemento	Amenaza	Valor	Probabilidad	Riesgo
		Acceso a servicios bancarios	1	1	1
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"> • Instalación de la división de seguridad para la zona de servidores. • Implementación del acceso biométrico al datacenter. • Vigilancia remota por la cámara en el datacenter.
	Daño por mal uso	<ul style="list-style-type: none"> • Instalación de la división de seguridad para la zona de servidores. • 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"> • Instalación de la división de seguridad para la zona de servidores. • 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	<p>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.</p>
	Falla suministro eléctrico	<ul style="list-style-type: none"> • Aumento de la capacidad actual de soporte de las UPS. • 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.
		<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"> • Instalación de la división de seguridad para la zona de servidores. • Implementación del acceso biométrico al datacenter. • Vigilancia remota por la cámara en el datacenter.
	Daño por mal uso	<ul style="list-style-type: none"> • Instalación de la división de seguridad para la zona de servidores. • Implementación del acceso biométrico al datacenter.
	Incendio	<ul style="list-style-type: none"> • Instalación de la división de seguridad para la zona de servidores. • 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	<p>Vigilancia remota por la 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.</p>
	Falla suministro eléctrico	<ul style="list-style-type: none"> • Garantizar el correcto soporte de las UPS.

		<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.

	<ul style="list-style-type: none"> • 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. • 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 2023, 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

