Sistema de Gestión de Seguridad de la Información (SGSI) para la Fundación Clínica Shaio, basado en los lineamientos de la norma ISO/IEC 27001:2022.

Escuela Superior de Guerra “Rafael Reyes Prieto”

Maestría en Ciberseguridad y Ciberdefensa

Gestión de Riesgos Cibernéticos

Bogotá, Colombia

2025

Sistema de Gestión de Seguridad de la Información (SGSI) para la Fundación Clínica Shaio, basado en los lineamientos de la norma ISO/IEC 27001:2022.

Seguridad de la información Fundación Clínica Shaio

Grupo de trabajo:

Miguel Anderson Amaya Piracoca
Erika Tatiana Sánchez Gomez
Cristian Mauricio Toro Mora
Andres Felipe Parrado Camona

Docente encargado:

Ing. Jaider Ospina Navas

Escuela Superior de Guerra “Rafael Reyes Prieto”

Maestría en Ciberseguridad y Ciberdefensa
Gestión de Riesgos Cibernéticos
Bogotá, Colombia
2025

Tabla de Contenido

Lista de figuras

1. Presentación

La Fundación Clínica Shaio es una institución de cuarto nivel, especializada en la alta complejidad, cuenta con infraestructura y personal capacitado para brindar atenciones oportunas a los pacientes. Fundada por el Dr. Fernando Valencia Céspedes y el Dr. Alberto Vejarano Laverde, inició labores en 1957, en su sitio web señalan que desde entonces han marcado la historia de la cardiología en el país. Desde sus inicios fue fundada con un enfoque académico, convirtiéndose en una escuela de cardiología para varios profesionales especializados en el exterior, que encontraron en esta institución un nuevo escenario para aplicar, compartir y crear conocimiento.

En la Fundación Clínica Shaio el estar a la vanguardia de la tecnología y contar con personal altamente calificado son eje fundamental desde sus inicios. Como señalan en la institución, hechos importantes de la medicina colombiana ocurrieron por primera vez en "la Shaio", como caso puntual se tiene el implante del primer marcapasos extracorpóreo, diseñado por el Dr. Jorge Reynolds.

Con más de 60 años, busca ofrecer una atención integral y humanizada siempre en busca de brindar a cada paciente una respuesta oportuna ante las enfermedades cardiovasculares y de alta complejidad, ofreciendo nuevos y mejores tratamientos con un enfoque lo más mínimamente invasivo.

1.1. Servicios ofrecidos por la Fundación

La fundación Clínica Shaio cuenta con seis grandes grupos de servicios enfocados en la Atención en salud, a continuación, se relacionan.

1.1.1. Atención quirúrgica

- Anestesia y Clínica del dolor.
- Cirugía cardiovascular.
- Esterilización e instrumentación quirúrgica.
- Salas de cirugía.

1.1.2. Apoyo Diagnóstico y Terapéutico

- Cardiología no invasiva.
- Farmacia.
- Laboratorio Clínico, Biología Molecular y Proteómica.
- Medicina Nuclear.
- Patología.

- Prevención Cardiovascular.
- Terapias
- Trasplantes.

1.1.3. Atención en Hospitalización

- Enfermería.
- Hospitalización adultos.
- Hospitalización pediátrica.
- Unidad de Cuidado Intensivo Cardiovascular.
- Unidad de Cuidados Intensivos.
- Unidad de Cuidados Intensivos Pediátricos.
- Unidad de Soporte Vital Extracorpóreo (USVEC).

1.1.4. Atención Ambulatoria

- Consulta Externa.
- Hospital día.

1.1.5. Atención en Urgencias

- Referencia y Contrareferencia.
- Urgencias.

1.1.6. Telesalud

- Telemonitoreo.
- Telemedicina

1.2. Estructura organizacional

La Fundación Clínica Shaio tiene sus procesos divididos en cuatro grandes grupos de los cuales se derivan subprocesos, mismos que definen la estructura organizacional.

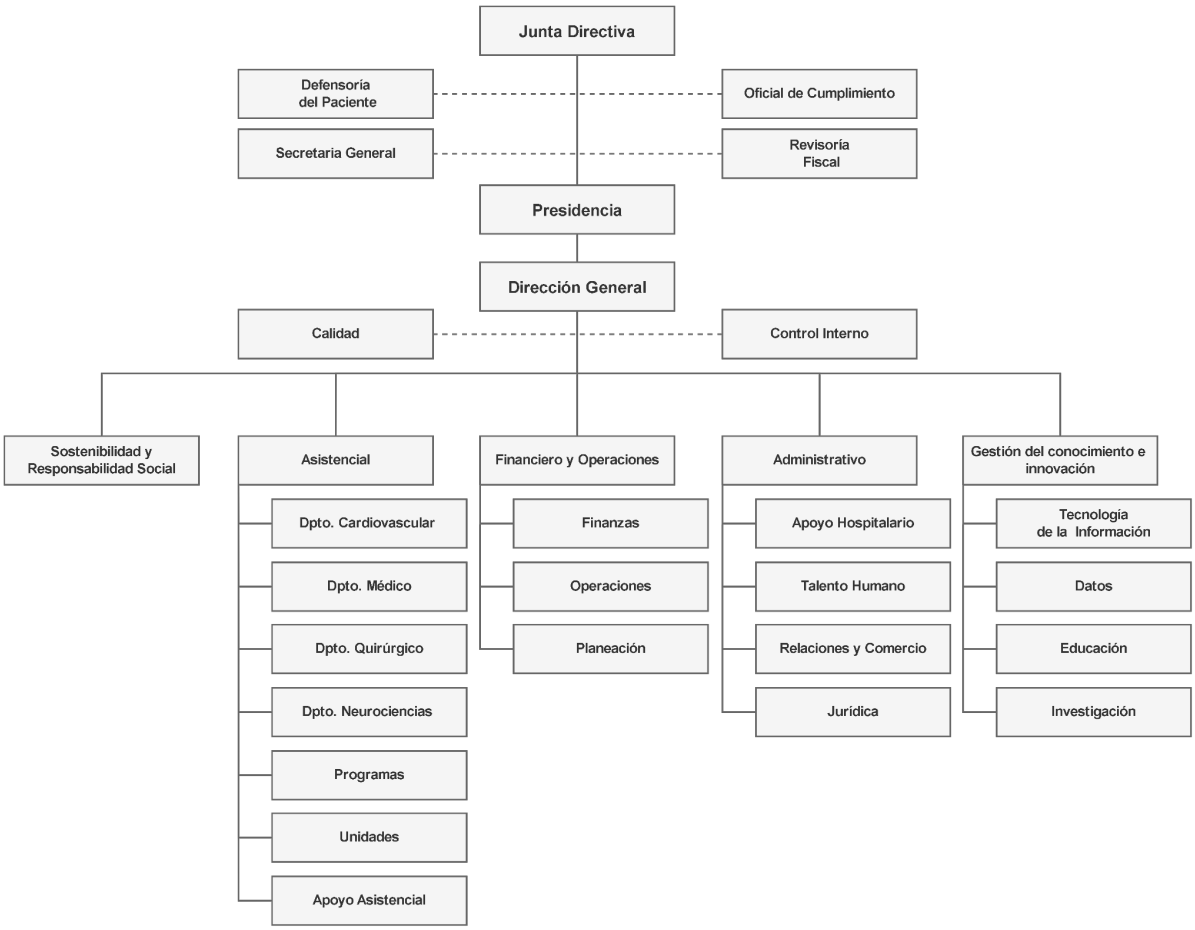
Ilustración 1. Mapa de Procesos

Estratégicos		
Dirección general	Gestión de Recurso Humano	
Misionales		
Sostenibilidad y Responsabilidad Social	Atención en Salud	Gestión del conocimiento
Apoyo		
Gestión de Apoyo Hospitalario	Gestión Financiera	Gestión Jurídica
Gestión Comercial	Gestión de Informática y Comunicación	
Gestión y Evaluación		
Gestión Clínica	Evaluación y Control	Gestión de Calidad y Mejoramiento Continuo (SOGC)

Fuente: Elaboración propia.

El organigrama de la Fundación Clínica Shaio desde el año 2011 a la fecha ha tenido ocho cambios los cuales en gran parte se han derivado de la planeación estratégica, a continuación, se muestra el organigrama actual.

Ilustración 2. Organigrama



Fuente: Elaboración propia.

2. Aspectos Técnicos

La Fundación Clínica Shaio cuenta con una única sede en la Ciudad de Bogotá, localidad de Suba en la dirección Diagonal 115a #70c - 75, dicha sede se encuentra compuesta arquitectónicamente por siete grandes zonas, las cuales se distribuyen así:

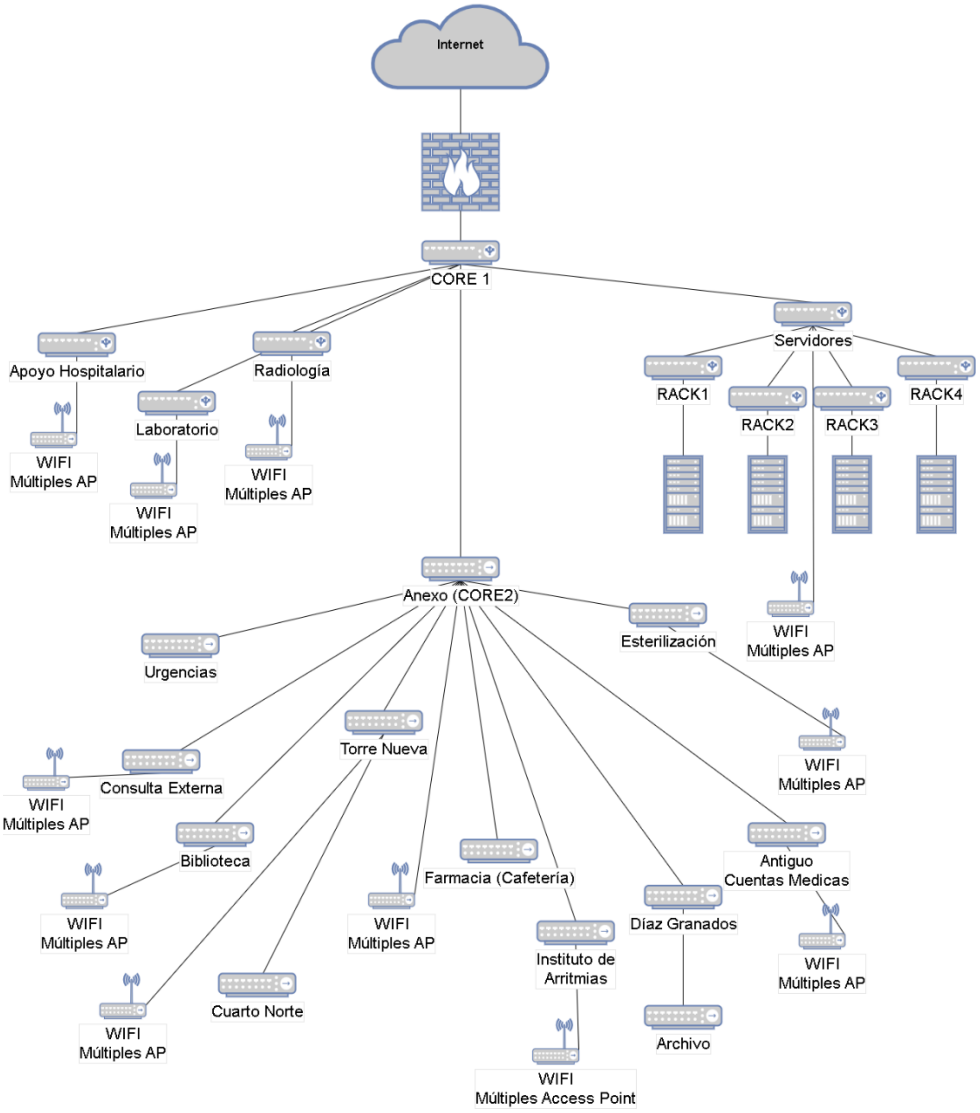
- **Torre Norte**: Una de las construcciones más recientes, está compuesta por seis niveles, en donde cuatro son destinados para hospitalización y los demás tanto para la parte de apoyo diagnóstico como administrativa.
- **Urgencias**: Se denomina Urgencias por el tipo de atención que se brinda, sin embargo, también tiene uso administrativo y de apoyo diagnóstico.
- **Hospitalización**: De uso mayormente para hospitalización de pacientes, también tiene uso administrativo y de apoyo diagnóstico. En esta se encuentran dos niveles divididos en cuatro alas para la hospitalización de pacientes.
- **Torre Quirúrgica**: Se encuentra ubicada a la mitad de la infraestructura, está provista por un helipuerto el cual está cerrado debido a la construcción de la torre norte. En sus diversos niveles se encuentran las Unidades (Cuidado intensivo, coronarios y otras).
- **Casa Consultorios**: La institución a lo largo de los últimos años adquirió las casas que se encontraban al respaldo de la construcción original, dichas casa fueron remodeladas y habilitadas como consultorios para el staff y para parte administrativa.
- **Biblioteca:** Denominada así por su uso inicial alberga en la actualidad parte únicamente administrativa, es la construcción más alejada al centro de datos.
- **Consulta Externa y Hospital Día**: Destinada para la atención del paciente ambulatorio, es la única que está perimetralmente hablando a una calle de distancia.

Ilustración 3. Zona de Distribución

Fuente: Elaboración propia.

Debido al área física que ocupa la infraestructura de la institución, además del centro de datos cuenta con trece centros de cableado. A continuación, se muestra el diagrama de topología de red.

Ilustración 4. Topología de red



Fuente: Elaboración Propia

3. Documentación De La Política De Seguridad

La política de seguridad de la Fundación Clínica Shaio está basada en la norma ISO 27001: 2013, la cual está enfocada en resguardar la integridad, confidencialidad y disponibilidad de sus activos e información. Estas políticas se encuentran definidas en el Anexo: Políticas de Seguridad.

4. Alcance del SGSI

El presente se realiza en las instalaciones de la Fundación Clínica Shaio (única sede) en la Ciudad de Bogotá, localidad de Suba en la dirección Diagonal 115a #70c - 75. abarcando activos y personal vinculado. Es de aclarar que los equipos biomédicos no se tomarán como parte de los activos debido a la complejidad de acceso a los mismos y el impacto que podría llegar a tener las acciones a realizar la declaración del alcance del SGSI:

- Sistemas de información que soportan los procesos Estratégicos, Misionales, Apoyo y Gestión y Evaluación.
- Las pautas descritas en el actual documento serán (aplicadas | efectivas) para los empleados de la Fundación Clínica Shaio en todos los departamentos y niveles.

5. Objetivos

A continuación, se define el objetivo general y objetivos específicos del proyecto.

5.1. Objetivo General

Plantear el diseño de un Sistema de Gestión de Seguridad de la Información, apoyados en los lineamientos de la norma NTC-ISO/IEC 27001:2013 para la Fundación Clínica Shaio, con el fin de lograr procesos internos eficientes y seguros a través de la identificación, gestión y tratamiento de los riesgos.

5.2. Objetivos Específicos

- Elaborar un inventario de activos informáticos y de información de la Fundación Clínica Shaio.
- Realizar un análisis de riesgos y vulnerabilidades basado en la norma ISO 31000:2018.
- Diseñar un plan de tratamiento de riesgos, basado en la norma.

- Diseñar las políticas del sistema de gestión de seguridad de la información en la Fundación Clínica Shaio, basado en la norma NTC-ISO/IEC 27001:2013 al igual que las políticas de seguridad de la información.

6. Requisitos Legales

- CONPES 3701 de 2011, Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016, Política Nacional de Seguridad Digital.
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015, por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 2952 de 2010. Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.
- Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, Delitos Informáticos" protección de la información y los datos.
- Ley 1341 de 2009. Tecnologías de la Información y aplicación de seguridad.
- Ley 1437 de 2011, Código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1581 de 2012, Protección de Datos personales.
- Ley 23 de 1982, Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000, Ley General de Archivos – Criterios de Seguridad.

7. Compromiso de la Dirección

La dirección y coordinación de TI dieron parte positivo y compromiso con el diseño planteado con la política de seguridad y las actividades realizadas frente a los escaneos, diagramas, evaluación de formatos y sugerencias realizadas en el marco de la norma ISO 27001 y metodologías trabajadas para la mejora continua de sus procesos internos.

Adicionalmente muestra gran intención de encaminar la divulgación y distribución interna a gran parte de las áreas y partes interesadas de la Fundación Clínica Shaio para adoptar e implementar los controles y políticas generadas bajo la norma ISO 27001.

8. Marco Organizativo de la seguridad de la información

A continuación, se relacionan los roles identificados en el sistema de información de la Fundación Clínica Shaio.

Tabla 1: Roles del sistema de información de la Fundación Clínica Shaio

Rol	Descripción
Dirección de TI	Está encargada de proponer, organizar y gestionar las directrices de seguridad. Adicionalmente en apoyar las metas establecidas por la institución, garantizando la confidencialidad, integridad y disponibilidad de los recursos de información.
Coordinación de TI	Está encargada de evaluar y validar que se dé cumplimiento de las políticas de seguridad de la información.
Empleados y Asociados	Está encargada de adoptar y cumplir con los parámetros establecidos en cuanto a las políticas de seguridad de la información.

Fuente: Elaboración propia.

8.1. Dirección TI

A continuación, se presentan las responsabilidades de la dirección de TI:

- Facilitar los recursos necesarios para el funcionamiento y mejora del SGSI.
- Asignar las responsabilidades en materia de seguridad de la información.
- Velar por la efectiva implantación de las medidas de seguridad seleccionadas.

8.2. Coordinación TI

A continuación, se presentan las responsabilidades de la coordinación de TI:

- Definir estrategias de seguimiento de riesgos.
- Coordinar el equipo de auditoría interna.
- Revisar el diseño y configuración de aplicaciones corporativas para definir los
- mecanismos requeridos para su protección.

8.3. Empleados y Asociados

A continuación, se presentan las responsabilidades de los empleados y asociados de la Fundación Clínica Shaio:

- Conocer, adoptar y cumplir los parámetros establecidos en las políticas de seguridad de la información

9. Evaluación de riesgos de seguridad

La Fundación Clínica Shaio debe disponer de un recurso encargado de realizar la evaluación de riesgos de seguridad, esto como objetivo de crear planes y estrategias para mitigar posibles ataques que puedan afectar la integridad, disponibilidad y confidencialidad de los sistemas de información.

Dicha evaluación debe contar con la supervisión de la Coordinación de TI y los resultados generados deben ser evaluados por la dirección de TI quienes son también los encargados de evaluar y aprobar cualquier plan estratégico resultante.

9.1. Proceso de análisis y gestión de riesgos

Mediante el uso de la metodología PTES, se realizaron múltiples procesos de identificación de vulnerabilidades, como punto de partida de los hallazgos encontrados, se procede a identificar, valorar y categorizar los posibles riesgos a los que la Fundación Clínica Shaio pueda estar expuesta.

9.2. Criterios de aceptación del riesgo

A continuación, en la tabla ## se relaciona la aceptación del riesgo, en donde se parametriza el rango y la tolerancia que maneja la Fundación Clínica Shaio en la aceptación del riesgo.

Tabla 2: Aceptación del riesgo

Rango	Descripción
Riesgo <= 5	La Fundación Clínica Shaio tolera el riesgo.
Riesgo > 5	La Fundación Clínica Shaio no tolera el riesgo y procede a un tratamiento del riesgo.

Fuente: Elaboración propia.

9.3. Propietarios del riesgo

Los riesgos identificados en este trabajo de análisis deben ser validados, controlados, supervisados y gestionados por la coordinación de TI de la Fundación Clínica Shaio o por un encargado designado por la institución.

Son estos los principales actores que definirán la magnitud del riesgo, adicionalmente de su manejo y si este debe ser transferido como estrategia a un tercero, en cuyo caso será evaluado en conjunto con la dirección de TI.

10. Inventario de activos

Para tener una mayor visibilidad de elementos que pueden llegar a generar o presentar un riesgo para la seguridad de la información en la Fundación Clínica Shaio, se realiza un inventario de activos categorizados. Para ver más a detalle el inventario, consultar el Anexo: Inventario de activos.

10.1. Categorización de los Activos

A continuación, se describe la categorización de activos de la Fundación Clínica Shaio.

Se identificaron tres grandes ítems para la clasificación de activos los cuales se muestran a continuación.

Tabla 3: Categorías para la clasificación de activos

Tipo de activo	Descripción
Información (IF)	A. Base de datos.
Físico (FS)	A. Access Point. B. Cableado C. Canales de comunicación D. Equipo MAC. E. Equipo Portátil. F. Equipo de Escritorio. G. Firewall. H. Rack - Armarios I. Servidor. J. Tablet.
Software y Licencias (SW)	A. Antivirus B. Aplicaciones Médicas C. Aplicaciones propias de la institución. D. Aplicaciones tercerizadas SaaS. E. Bases de datos. F. Correo Electrónico. G. Ofimática. H. Sistemas Operativos.
Personas (PR)	A. Funcionarios tanto del área de TI como los usuarios del sistema.

Fuente: Elaboración propia.

10.1.1. Información

La Fundación Clínica Abood Shaio, cuenta con diversas bases de datos donde se almacena información centralizada tanto de activos fijos, inventarios, empleados, información contable, pacientes, imágenes diagnósticas, entre otras

Tabla 4: Bases de datos

Tipo	Componente	Cantidad	
IF	Base de datos de Activos Fijos.	1	Corresponde a bienes y derechos, denominados activos fijos o activos no corrientes.
IF	Base de datos de Inventarios.	1	Información detallada, ordenada y valorada medicamentos, insumos y consumibles de la institución.
IF	Base de datos de empleados.	1	Es donde se almacena la información digital de los empleados como nómina, pagos, retenciones, etc.
IF	Base de datos de imágenes diagnósticas.	2	Las bases de datos diagnósticas hacen referencia a los estudios por ejemplo de radiología, medicina nuclear, métodos no invasivos, etc.
IF	Base de datos de información Contable.	2	Información NIIF
IF	Base de datos de laboratorios y estudios paraclínicos.	2	Las bases de datos diagnósticas hacen referencia a los estudios de laboratorio y paraclínicos.
IF	Base de datos de pacientes.	1	información de la Historia Clínica de los Pacientes durante las diversas atenciones en la institución.

Fuente: Elaboración propia.

Se identifican diez fuentes de información las cuales se encuentran en múltiples motores de bases de datos como Oracle, MS SQL y DB2.

10.1.2. Software

En este apartado se enlistan todas las aplicaciones usadas por parte de la organización Fundación Clínica Abood Shaio, teniendo en cuenta aquellas herramientas de software que son de carácter utilitario, desarrollo y ofimático.

Tabla 5: Software y Licencias

Tipo	Componente	Cantidad	
SW	Historia Clínica	1	Desarrollo propio para la gestión de información clínica.
SW	Historia Clínica (Web)	1	Desarrollo propio para la gestión de información clínica (Migración del modelo desktop al web).
SW	IBM DB2	4	Motor de Base de Datos
SW	IBM AS 400	4	Sistema Operativo
SW	Microsoft SQL Server	5	Motor de Base de Datos
SW	ERP Alphil (Contable NIIIF/NIC, ERP, Inventarios)	1	Paquete ERP.
SW	MS Office	23	La institución cuenta con pocas licencias de MS Office ya que en general utiliza LibreOffice v7 y es actualizado frecuentemente.
SW	RIS / PACS Agility (AGFA)	2	Software de Apoyo Diagnóstico para Imágenes.
SW	Tharsis	1	Software para estudios de Laboratorio, Molecular y Paraclínicos.
SW	Nomina ERPS - Heinsohn	1	Heinsohn nómina es una solución de software a la medida para los procesos de nómina.
SW	Antivirus KES Kaspersky	900	Kaspersky Endpoint Security es la aplicación de seguridad utilizada en la institución tanto en estaciones de trabajo como en servidores Windows.
SW	LibreOffice v7 (7.0.6 / 7.3.3)	581	LibreOffice es un paquete de software de oficina libre y de código

			abierto desarrollado por The Document Foundation.
SW	Plataforma de Correo electrónico Zimbra	1	Servicio de correo electrónico creado por Zimbra Inc bajo modelo On-premises
SW	GLPI (Mesa de Ayuda)	1	Solución libre de gestión de servicios de tecnología para el seguimiento de incidencias y de solución Service Desk.
SW	NAGIOS (Monitoreo)	1	Sistema de monitorización de redes, servicios y equipos.
SW	Android linux 6.0.1	35	Sistema Operativo
SW	IOS	3	Sistema Operativo
SW	macOS	1	Sistema Operativo
SW	Microsoft Windows 10 Pro	419	Sistema Operativo
SW	Microsoft Windows 11 Pro	7	Sistema Operativo
SW	Microsoft Windows 7 Professional	194	Sistema Operativo
SW	Microsoft Windows 8.1 Pro	160	Sistema Operativo
SW	Microsoft Windows Server 2008 R2 Standard	6	Sistema Operativo
SW	Microsoft Windows Server 2012 R2 Standard	12	Sistema Operativo
SW	Microsoft Windows Server 2016 Standard	3	Sistema Operativo
SW	Microsoft Windows Server 2019 Standard	2	Sistema Operativo
SW	Microsoft Windows Server 2022 Standard	5	Sistema Operativo

SW	OS X	4	Sistema Operativo
SW	Ubuntu 16.04.7 LTS	3	Sistema Operativo
SW	Ubuntu 18.04.4 LTS	2	Sistema Operativo
SW	Ubuntu 22.04	6	Sistema Operativo

Fuente: Elaboración propia.

10.1.3. Fisico

En esta categoría se encuentran todos los activos físicos y tangibles, se incluyen equipos de cómputo, de comunicaciones y de redes.

Tabla 6: Activos físicos

Tipo	**Componente**	**Cantidad**	
FS	Access Point	72	AP Cisco Meraki MR36
FS	Canales de comunicación	4	Une, Movistar, Tigo, C&W
FS	Firewall	2	DELL SonicWall (HA)
FS	Switch de Borde	27	Aruba Instant On 1960
FS	Switch de distribución	14	MS250
FS	Core Cisco Meraki	2	MS425-16
FS	Racks- Armarios	17	Rack Cerrado de 45 U
	Escritorio	**665**	

FS	0967A1S	36	Lenovo, Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	10B7003TLS	14	Lenovo, Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	10J0S57X00	37	Lenovo, Procesador: Intel(R) Core(TM) i7-6700T CPU @ 2.80GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	10M8S2A800	22	Lenovo, Procesador: Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	10MLS15300	4	Lenovo, Procesador: Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	10TY001DLS	19	Lenovo, Procesador: Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	11A9S03M00	2	Lenovo, Procesador: AMD Ryzen 5 PRO 3400G with Radeon Vega Graphics, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	30C6S0JB00	1	Lenovo, Procesador: Intel(R) Xeon(R) E-2124G CPU @ 3.40GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	30C6S0JC00	2	Lenovo, Procesador: Intel(R) Xeon(R) E-2124G CPU @ 3.40GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	30D0S0NL00	18	Lenovo, Procesador: Intel(R) Xeon(R) E-2224G CPU @ 3.50GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	3157C2S	55	Lenovo, Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	3238E9S	7	Lenovo, Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar

FS	3554H5S	13	Lenovo, Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	7269E1S	5	Lenovo, Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	AIO Series Mtouch	1	PCSMART, Procesador: Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	AIO Series Touch	4	PCSMART, Procesador: Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	F0BW002KLD	3	Lenovo, Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP 205 G4 24 All-in-One PC	2	HP, Procesador: AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP 280 G3 SFF Business PC	1	HP, Procesador: Intel(R) Core(TM) i3-8100 CPU @ 3.60GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP ProDesk 400 G6 SFF	10	HP, Procesador: Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP ProOne 400 G4 20.0-in NT AiO	10	HP, Procesador: Intel(R) Core(TM) i5-8500T CPU @ 2.10GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP ProOne 400 G5 20.0-in All-in-One	10	HP, Procesador: Intel(R) Core(TM) i5-9500T CPU @ 2.20GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP ProOne 400 G6 20 All-in-One PC	89	HP, Procesador: Intel(R) Core(TM) i5-10500T CPU @ 2.30GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	MS-7C09	2	Micro-Star International Co., Ltd., Procesador: Intel(R) Core(TM) i5-9400 CPU @ 2.90GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video

			estándar
FS	OptiPlex 3011 AIO	77	Dell Inc., Procesador: Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 3020M	27	Dell Inc., Procesador: Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 3040	77	Dell Inc., Procesador: Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 3070	1	Dell Inc., Procesador: Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 3280 AIO	16	Dell Inc., Procesador: Intel(R) Core(TM) i5-10500T CPU @ 2.30GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 380	11	Dell Inc., Procesador: Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 390	53	Dell Inc., Procesador: Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 5490 AIO	2	Dell Inc., Procesador: Intel(R) Core(TM) i5-10500T CPU @ 2.30GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 7010	3	Dell Inc., Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 9010 AIO	7	Dell Inc., Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	OptiPlex 9020 AIO	11	Dell Inc., Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar

FS	OptiPlex 9030 AIO	3	Dell Inc., Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	Precision Tower 3430	6	Dell Inc., Procesador: Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	Vostro 330	1	Dell Inc., Procesador: Intel(R) Core(TM) i3-10100 CPU @ 3.60GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	Vostro 3471	2	Dell Inc., Procesador: Intel(R) Core(TM) i3-9100 CPU @ 3.60GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
	MAC	**5**	
FS	iMac13,2	1	Apple Inc, Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	iMac14,3	2	Apple Inc, Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	iMac16,2	1	Apple Inc, Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	iMac18,3	1	Apple Inc, Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
	Portátil	**114**	
FS	20DSA05400	17	Lenovo, Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	20FCA08S00	1	Lenovo, Procesador: , Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	20N9S1TR00	5	Lenovo, Procesador: Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	20S5S1DT00	1	Lenovo, Procesador: Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz, Memoria: 8 GB,

			Disco: 500GB, Tarjeta de video estándar
FS	20VYS0RQ00	1	Lenovo, Procesador: 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	2356HCS	1	Lenovo, Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	80SX	6	Lenovo, Procesador: Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	81B0	12	Lenovo, Procesador: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	81W3	1	Lenovo, Procesador: AMD Ryzen 5 4500U with Radeon Graphics, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP 240 G7 Notebook PC	44	HP, Procesador: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP 240 G8 Notebook PC	1	HP, Procesador: Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP 250 G8 Notebook PC	2	HP, Procesador: 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	HP ProBook 440 G8 Notebook PC	1	HP, Procesador: 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	Latitude 3480	3	Dell Inc., Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	Latitude E5430 non-vPro	9	Dell Inc., Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar

FS	Precision 7540	1	Dell Inc., Procesador: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	Vostro 5470	7	Dell Inc., Procesador: Intel(R) Core(TM) i3-10100 CPU @ 3.60GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	Vostro1510	1	Dell Inc., Procesador: Intel(R) Core(TM) i3-10100 CPU @ 3.60GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
	Servidor	**39**	
FS	PowerEdge R240	1	Dell Inc., Procesador: Intel(R) Xeon(R) E-2224 CPU @ 3.40GHz, Memoria: 32 GB, Disco: 500GB, Tarjeta de video estándar
FS	PowerEdge R440	1	Dell Inc., Procesador: Intel(R) Xeon(R) Silver 4208 CPU @ 2.10GHz, Memoria: 16 GB, Disco: 500GB, Tarjeta de video estándar
FS	ProLiant DL160 Gen9	1	HP, Procesador: Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	ProLiant DL360 Gen10	5	HP, Procesador: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz, Memoria: 16 GB, Disco: 500GB, Tarjeta de video estándar
FS	ThinkServer RD550	1	Lenovo, Procesador: Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz, Memoria: 16 GB, Disco: 500GB, Tarjeta de video estándar
FS	VMware Virtual Platform	21	VMware, Inc., Procesador: Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz, Memoria: 16 GB, Disco: 500GB, Tarjeta de video estándar
FS	IBM System x3630 M2	1	IBM, Procesador: Intel(R) Xeon(R) CPU E5-2420 v2 @ 2.20GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar

FS	LENOVO System x3250 M6	1	Lenovo, Procesador: Intel(R) Xeon(R) CPU E3-1240 v6 @ 3.70GHz, Memoria: 16 GB, Disco: 500GB, Tarjeta de video estándar
FS	IBM System x3550 M4	2	IBM, Procesador: Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	BladeCenter LS42	2	IBM, Procesador: Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz, Memoria: 8 GB, Disco: 500GB, Tarjeta de video estándar
FS	ThinkSystem SR550	2	Lenovo, Procesador: Intel(R) Xeon(R) Silver 4208 CPU @ 2.10GHz, Memoria: 32 GB, Disco: 500GB, Tarjeta de video estándar
FS	IBM eServer BladeCenter HS21	1	IBM, Procesador: Intel(R) Xeon(R) CPU E5440 @ 2.83GHz, Memoria: 16 GB, Disco: 500GB, Tarjeta de video estándar
	Tablet	**43**	
FS	AIO Series Mtouch	4	PCSMART, Procesador: Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	Lenovo YT3-850F	35	Lenovo, Procesador: Intel(R) Pentium(R) Dual CPU E2200 @ 2.20GHz, Memoria: 2 GB, Disco: 500GB, Tarjeta de video estándar
FS	MB293E	1	Apple Inc., Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	MGL12CL/A	1	Apple Inc., Procesador: , Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	MUQW2LZ/A	1	Apple Inc., Procesador: Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video estándar
FS	T100TA	1	ASUSTeK COMPUTER INC., Procesador: Intel(R) Core(TM) i3-10100 CPU @ 3.60GHz, Memoria: 4 GB, Disco: 500GB, Tarjeta de video

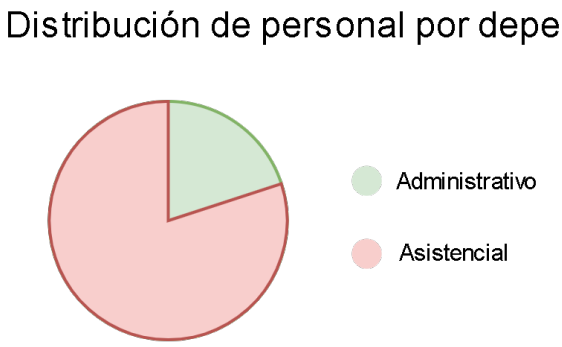
			estándar

Fuente: Elaboración propia.

10.1.4. Personas

La institución cuenta con 1495 funcionarios, el 79% son funcionarios asistenciales y el 23% restantes administrativos.

Ilustración 5: Distribución de personal



Fuente: Elaboración propia.

11. Procesos de negocio

La institución cuenta con 50 dependencias administrativas y un subtotal de 344 funcionarios mientras que por su contraparte asistencia tienen 29 dependencias y 1151 funcionarios. A continuación, se muestra la tabla con la distribución de funcionarios por dependencia.

Tabla 7: Distribución de personal por dependencia

Tipo	Dependencia	Cantidad
PR	Almacén	3
PR	Apoyo Hospitalario	6
PR	Archivo Historias Clínicas	7
PR	Asesor(a) Post Consulta	1
PR	Bioestadística	3
PR	Calidad y Acreditación	22
PR	Cardiologia Pediatrica	1
PR	Cartera y Cobranzas	6
PR	Cirugía	31
PR	Compras	9
PR	Comunicaciones	5
PR	Consulta Externa Especializada	12
PR	Contabilidad	7
PR	Control Interno	3
PR	corazón Colombia	1
PR	Costos	2
PR	Cuentas Médicas	18

PR	Departamento de T.I.	12
PR	Departamento Juridico	6
PR	Departamento Medico	9
PR	Direccion Comercial	8
PR	Dirección de Compras y Abastecimiento	1
PR	Dirección de Investigaciones	1
PR	Dirección General	1
PR	Docencia Educacion y Biblioteca	9
PR	Electrofisiología	1
PR	Estancia General Habitacional	706
PR	Esterilización	15
PR	Facturación	41
PR	Farmacia	54
PR	Fisioterapia	10
PR	Gastroenterología	1
PR	Gerencia	3
PR	Hemodinamia	2
PR	Imagenologia - Rayos X	41

PR	Ingeniería Biomédica	9
PR	Ingeniería y Mantenimiento	5
PR	Investigación	25
PR	Laboratorio Clínico General	41
PR	Medicina Nuclear	6
PR	Médicos	113
PR	Mercadeo y Ventas Centro Internacional	2
PR	Métodos no Invasivos	2
PR	Nutrición y Dietética	8
PR	Presidencia	2
PR	Redistribución gastos personales imágenes	2
PR	Rehabilitación (terapias)	60
PR	Talento Humano	19
PR	Tesorería	5
PR	Trasplantes	3
PR	UCI Pediátrica	2
PR	Unidad Cuidados Intensivos	11
PR	Urgencias	72

PR	USVEC Unidad de Soporte Vital Extracorpóreo	4
PR	Consulta de Urgencias	46

Fuente: Elaboración propia.

12. Valoración de activos

Los activos disponibles se valorizaron bajo tres categorías, confidencialidad, integridad y disponibilidad partiendo del hecho que el SGSI tiene como fiel propósito el establecimiento de los mecanismos de gestión de estos tres criterios dentro de un conjunto de estándares previamente determinados para evaluar la seguridad.

Tabla 8: Valoración de activos

VALOR	CONFIDENCIALIDAD
5 Muy alto	La información asociada al activo es solo accedida por el personal de alto rango, pues su divulgación afectaría irreversiblemente a la organización.
4 Alto	La información asociada al activo es restringida y sólo personal de un proyecto específico puede acceder a ella pues su divulgación afectaría gravemente a la organización.
3 Medio	La información asociada al activo es confidencial y sólo personal de algunas áreas internas puede acceder a ella, pues su divulgación afectaría a la organización.
2 Bajo	La información asociada al activo es de uso interno y sólo personal de la organización puede acceder a ella, pues su divulgación afectaría parcialmente a la organización.
1 Muy Bajo	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la organización.
VALOR	**DISPONIBILIDAD**
5 Muy alto	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 0% pues la vulneración de su integridad afectaría irreversiblemente a la organización.
4 Alto	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 15% pues la vulneración de su integridad afectaría gravemente a la organización.

3 **Medio**	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50% pues la vulneración de su integridad afectaría considerablemente a la organización.
2 **Bajo**	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 85% pues la vulneración de su integridad afectaría parcialmente a la organización.
1 **Muy Bajo**	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 100% pues la vulneración de su integridad no impacta a la organización.
VALOR	**INTEGRIDAD**
5 **Muy alto**	Se requiere que el activo nunca se encuentre indisponible pues su carencia afectaría irreversiblemente a la organización.
4 **Alto**	Se considera que como máximo el activo puede estar indisponible por 1 hora, pues su carencia afectaría gravemente la organización.
3 **Medio**	Se considera que como máximo el activo puede estar indisponible por 1 día, pues su carencia afectaría considerablemente a la organización.
2 **Bajo**	Se considera que como máximo el activo puede estar indisponible por 1 semana, pues su carencia afecta parcialmente a la organización.
1 **Muy Bajo**	Se considera que como máximo el activo puede estar indisponible por tiempo indefinido, pues su carencia no impacta a la organización.

Fuente: Elaboración propia.

13. Identificación y valoración de amenazas

A Continuación, se enmarcan las amenazas más significativas para la institución, con la probabilidad de que pueda ocurrir dichas amenazas, del 1 al 4, siendo 1 “Bajo”, y 4 “Crítico”.

Tabla 9: Niveles de riesgo para amenazas

Nivel	**Descripción**

4 **Crítico** *(Muy probable)*	Involucra hardware e información que afecta en los procesos de la institución y se detiene el flujo normal. La amenaza se puede materializar más o menos una vez cada día, es muy probable, hay una cantidad grande de antecedentes presentados constantemente.
3 **Alto** *(Probable)*	Involucra hardware e información que afecta los procesos de la institución e interrumpe su flujo normal. La amenaza se puede materializar más o menos una vez cada semana, probable, hay antecedentes presentados en algún patrón o periodicidad.
2 **Medio** *(Poco probable)*	Involucra hardware e información que afecta, pero no interrumpe en los procesos de la institución. La amenaza se puede materializar más o menos una vez cada mes, es poco probable, hay pocos antecedentes.
1 **Bajo** *(Muy poco probable)*	Involucra hardware e información de bajo impacto en los procesos de la institución. La amenaza se puede materializar más o menos una vez cada año, es muy poco probable, no hay antecedentes.

Fuente: Elaboración propia.

En la tabla se muestra el cálculo del impacto que da a conocer los criterios que se definieron para la medición y el cálculo del riesgo.

Tabla 10: Valores para el cálculo del impacto

Nivel	**Descripción**
4 **Crítico**	La amenaza afecta en los procesos de la institución y se detiene el flujo normal.
3 **Alto**	La amenaza afecta los procesos de la institución e interrumpe su flujo normal.
2 **Medio**	La amenaza afecta, pero no interrumpe en los procesos de la institución.
1 **Bajo**	La amenaza causa bajo impacto en los procesos de la institución.

Fuente: Elaboración propia.

13.1. Fuentes de amenaza

La NTC-ISO/IEC 27001 tiene un amplio rango de amenazas y vulnerabilidades, por tal motivo se acota el listado de fuentes de las amenazas a las siguientes:

- Acceso a la red o al sistema de información por personas no autorizadas.
- Acceso físico no autorizado.
- Ataques terroristas.
- Cambio involuntario de datos en un sistema de información.
- Cambios no autorizados de registros.
- Comprometer información confidencial.
- Código malicioso.
- Daños resultantes de las pruebas de penetración.
- Desastre generado por causas humanas.
- Desastre natural, incendio, inundación, rayo.
- Destrucción de registros.
- Divulgación de contraseñas.
- Error de usuario.
- Errores de software.
- Errores en mantenimiento.
- Espionaje industrial.
- Fallo de los enlaces de comunicación.
- Falsificación de registros.
- Fuga de información.
- Incumplimiento de relaciones contractuales.
- Infracción legal.
- Instalación no autorizada de software.
- Interrupción de procesos de negocio.
- Mal funcionamiento del equipo.
- Malversación y fraude.
- Ocultar la identidad de un usuario.
- Pérdida de electricidad.
- Pérdida de servicios de apoyo.

- Revelación de información.
- Uso indebido de las herramientas de auditoría.
- Uso indebido de los sistemas de información.
- Uso no autorizado de material con copyright.
- Uso no autorizado de software.

14. Identificación y valoración de riesgos

A continuación, se presenta la descripción y evidencias encontradas en la identificación de riesgos para la Fundación Clínica Shaio.

14.1. Cálculo del riesgo

En la fórmula planteada para el cálculo del riesgo, se determina el valor de la amenaza según la probabilidad que llegue a presentar por el impacto derivado dando como resultado la probabilidad del riesgo.

Fórmula 1 Cálculo del riesgo.

Probabilidad * Impacto = Riesgo

Fuente: Elaboración propia.

14.2. Matriz de riesgos

A continuación, se presenta la tabla XX correspondiente a la matriz donde se encuentran listados los posibles riesgos encontrados y su respectiva valorización.

Tabla 11: Lista de posibles riesgos.

#	Riesgo	Probabilidad				Impacto				Riesgo
		Bajo	Medio	Alto	Crítico	Bajo	Medio	Alto	Crítico	Total
Errores y Fallos No Intencionados										
R1	Error del Administrador	1						3		3
R2	Error de Configuración	1					2			2
R3	Fuga de Información	1						3		3
R4	Destrucción de la Información	1					2			2
R5	Alteración de Información Sensible		2						4	8
R6	Diligenciar mal formularios		2					3		6
R7	Vulnerabilidades de Software		2						4	8
R8	Vulnerabilidades de Hardware		2						4	8
R9	Pérdida o Robo de Equipos	1						3		3
R10	Caídas del Sistema por Agotamiento de Recursos			3				3		9
R11	Caídas del Sistema por Fallas en los Equipos		2						4	8
R12	Errores de mantenimiento / actualización Software		2					3		6
R13	Errores de mantenimiento / actualización Hardware		2						4	8
Industrial										
R15	Falla en flujo eléctrico		2				2			4
R16	Condiciones Inadecuadas de Temperatura		2					3		6
R17	Falla en los Servicios de Comunicaciones		2					3		6
R18	Emanaciones Electromagnéticas	1					2			2
Ataques										
R19	Difusión de malware			3				3		9

R20	Suplantación de identidad del usuario			3				3		9
R21	Mala manipulación de los equipos - daño		2						4	8
R22	Ataque de Ransomware		2						4	8
R23	Ingenieria Social		2						4	8
Desastres Naturales										
R24	Fuego	1							4	4
R25	Daños por humedad		2						4	8
R26	Daños por Desastres Naturales	1							4	4

Fuente: Elaboración propia

Posterior del proceso de identificación y valorización posterior se genera un mapa de riesgo inherente, él nos da una visibilidad de la probabilidad vs el impacto de cada uno de los riesgos, según la categorización planteada.

Tabla 12: Matriz de Riesgo inherente.

Probabilidad	Crítico				
	Alto			R10, R19, R20	
	Medio		R15	R6, R12, R15, R17	R5, R7, R8, R11, R13, R21, R22, R23, R25
	Bajo		R2, R4, R 18	R1, R3, R9	R24, R26
		Bajo	Medio	Alto	Crítico
		Impacto			

Fuente: Elaboración propia.

15. Declaración de aplicabilidad

A continuación, se muestra la declaración de aplicabilidad (SOA), que incluye para cada control la justificación de su inclusión o exclusión.

Ver el Anexo “SOA ISO27001-2022.xlsx”

En el proceso de evaluación de la declaración de aplicabilidad (SOA) se identificaron que, de los 93 controles, aplican para la Fundación Clínica Shaio 82 y no aplican 11 controles.

16. Modelo de declaración de aplicabilidad

16.1. Documentación de la gestión de riesgos

Se pretende que, posterior a la implementación de los controles relacionados y los controles sugeridos específicamente para mitigación de riesgos, se evidencie la reducción del nivel de amenaza o el de vulnerabilidad al menos en un punto.

16.2. Valoración de amenazas tras la aplicación de medidas

Se realiza nuevamente la valoración de las amenazas, teniendo como referencia la declaración de aplicabilidad (SOA).

Tabla 15: Lista de posibles riesgos.

#	Riesgo	Probabilidad				Impacto				Riesgo
		Bajo	Medio	Alto	Crítico	Bajo	Medio	Alto	Crítico	Total
Errores y Fallos No Intencionados										
R1	Error del Administrador	1					2			2
R2	Error de Configuración	1				1				1
R3	Fuga de Información	1					2			2
R4	Destrucción de la Información	1				1				1
R5	Alteración de Información Sensible	1					2			2
R6	Diligenciar mal formularios		2				2			4
R7	Vulnerabilidades de Software	1						3		3
R8	Vulnerabilidades de Hardware	1						3		3
R9	Pérdida o Robo de Equipos	1					2			2
R10	Caídas del Sistema por Agotamiento de Recursos		2				2			4

R11	Caídas del Sistema por Fallas en los Equipos	1						3		3
R12	Errores de mantenimiento / actualización Software		2				2			4
R13	Errores de mantenimiento / actualización Hardware		2				2			4
Industrial										
R15	Falla en flujo eléctrico		2				2			4
R16	Condiciones Inadecuadas de Temperatura		2				2			4
R17	Falla en los Servicios de Comunicaciones		2				2			4
R18	Emanaciones Electromagnéticas	1				1				1
Ataques										
R19	Difusión de malware		2				2			4
R20	Suplantación de identidad del usuario		2				2			4
R21	Mala manipulación de los equipos - daño	1						3		3
R22	Ataque de Ransomware		2					3		6
R23	Ingenieria Social		2					3		6
Desastres Naturales										
R24	Fuego	1					2			2
R25	Daños por humedad	1					2			2
R26	Daños por Desastres Naturales	1						3		3

Fuente: Elaboración propia

16.3. Cálculo de riesgos residuales

Tabla 16: Matriz de Riesgo Residual.

Probabilidad					
	Crítico				
	Alto				
	Medio		R6,R10,R12,R13, R15,R16,R17,R19 ,R20	R6, R12, R17,R22,R23	
	Bajo	R2, R4,R18	R1, R3, R5,R9,R24,R25	R7, R8, R9,R11,R21,R26	
		Bajo	Medio	Alto	Crítico
		Impacto			

Fuente: Elaboración propia.

16.4. Referencias

Los documentos de referencia para la realización de este procedimiento de gestión de incidencias son:

- Políticas de Seguridad.
- Norma ISO / IEC 27002.