UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE TECNOLOGÍAS DEL HOSPITAL FRANCISCO ICAZA BUSTAMANTE

AUTOR:

LUIS ALBERTO MACHUCA DE LA TORRE

DIRECTOR:

JHONNY JAVIER BARRERA JARAMILLO

CUENCA – ECUADOR

2023

Autor:

Luis Alberto Machuca de la Torre
Ingeniero en Sistemas con mención a Telemática.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
lmachuca@gmail.com

Dirigido por:

Jhonny Javier Barrera Jaramillo
Ingeniero en Sistemas Computacionales.
Máster en Ciencia de la Computación y Networking.
jbarrera@ups.edu.ec

LUIS ALBERTO MACHUCA DE LA TORRE
Plan director de seguridad de la información para el departamento de tecnologías del Hospital Francisco Icaza Bustamante

DEDICATORIA

Dedico este trabajo de titulación a Dios; quien mediante mi fe me da las fuerzas cada día para afrontar nuevos retos y desafíos y a mi familia porque sé la alegría y el orgullo que sienten con este nuevo logro y nunca me han abandonado en mi crecimiento personal y profesional.

Luis Alberto Machuca De la Torre

AGRADECIMIENTO

Agradezco a Dios por todas sus bendiciones.

A mis padres Alberto y Elsy quienes son mi motor de vida, mi gran motivación.

A mis hermanas Jessica y Mónica por su gran apoyo y ejemplo.

A mi tutor y amigo Jhonny Barrera que gracias a sus conocimientos, experiencia y guía; sirvieron de mucha ayuda para cumplimiento de este trabajo.

Al Hospital del Niño Francisco Icaza Bustamante por permitirme con mis conocimientos aportar un granito de arena para el crecimiento institucional y profesional.

Gracias a todos por confiar en mí.

Tabla de Contenido

Plan director de seguridad de la información para el Departamento de Tecnologías del Hospital Francisco Icaza Bustamante

Autor:

LUIS ALBERTO MACHUCA DE LA TORRE

Resumen

La tecnología ha facilitado la realización de tareas de la vida diaria en nuestros hogares, así como también en las empresas donde laboramos. La ingeniería social ha evolucionado en conjunto con las nuevas tecnologías; es por ello que en las organizaciones pueden por las vulnerabilidades hacia sus activos informáticos enfrentarse a ataques informáticos amenazando la integridad, disponibilidad y confidencialidad de la información.

El Hospital del Niño Dr. Francisco Icaza Bustamante (FIB) es una institución pública que cuenta con sus respectivos procesos institucionales y activos de mucho valor que apoyan a la cadena de valor, así como los registros digitales de las atenciones médicas y las historias clínicas de los pacientes; además, el Departamento de Tecnología de la Información (TI) no cuenta con procedimientos establecidos para el desarrollo de sus actividades y protección de los activos por lo que en ocasiones se actúa de manera empírica.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es importante, con la finalidad de poder contar con buenas prácticas en temas de la seguridad de la información mediante la implementación del plan director en el Hospital FIB; y cumplir la gestión de seguridad de los activos de la información bajo estándares internacionales que permitan al hospital incrementar su valor como institución y poder proteger sus activos mediante la disponibilidad, integridad y confidencialidad de la información.

Palabras clave:

Plan Director, SGIS, ciberseguridad, Análisis de Riesgos, ISO/IEC 2700

ABSTRACT

The Technology has made to carry out easy tasks of daily life in our homes, as well as in the companies where we work. Social engineering has evolved along with new technologies; that is why in the organizations, due to vulnerabilities towards their computer assets, they can face computer attacks threatening the integrity, availability and confidentiality of information.

The Hospital del Niño Dr. Francisco Icaza Bustamante is a government pubic institution that has institutional processes and valuable assets that support of the value chain, such as the digital records of the medical care of the patients; at present, the Department of TI does not have established procedures for the development of its activities and information assets, for this reason sometimes its carried out empirically.

The implementation of an Information Security Management System (ISMS) is important, in order to have good practices in Security of information issues through the implementation of the master plan in the Hospital FIB, compliance with security management under international standards. allowing the hospital to increase its value as an institution and be able to protect your assets through the availability, integrity and confidentiality of information.

Key Word:

Master Plan, ISMS, cybersecurity, Risk Analysis, ISO/IEC 2700

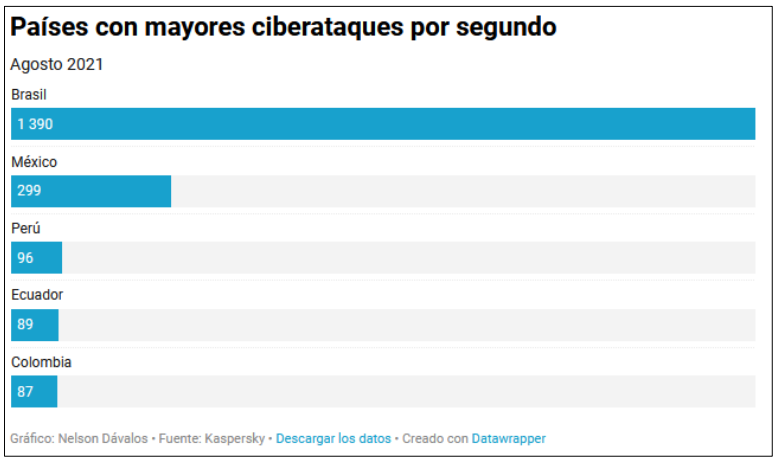
1. INTRODUCCIÓN

En la actualidad, las empresas enfrentan diariamente factores externos e internos que amenazan a la integridad, disponibilidad y confidencialidad de la información a los activos que contribuyen a garantizar la continuidad del negocio. Un Sistema de Seguridad de la Información (SGSI) permite prevenir las amenazas y los riesgos de los sistemas mediante su análisis y evaluación de sus activos de seguridad de la información bajo los siguientes principios:

- Confidencialidad: Un SGSI garantiza que la información de la empresa no estará disponible ni será revelada a personas u organizaciones no autorizados.
- Integridad: El SGSI permite mantener la información exacta y completa, tal como fue finalmente elaborada, así como sus métodos de proceso.
- Disponibilidad: Las personas, organizaciones y procesos que tengan acceso autorizado a la información deberán disponer de ella cuando la requieran (ESAN, 2016).

En los últimos años se ha registrado un incremento de ciberataques o fraudes informáticos según investigaciones realizadas a nivel mundial; los ataques cibernéticos en Latinoamérica aumentaron un 24% en los primeros meses del año pasado; en donde Ecuador es uno de los países más vulnerados, después de Brasil con el 13,3% de usuarios perjudicados como se muestra en la Figura 1.

Figura 1. Estadística de ciberataques 2021



Fuente: Kasperky

El Ecuador no ha sido la excepción de estos ciberataques, desde varios años atrás han sido más frecuentes los incidentes de seguridad en contra de algunas instituciones públicas a sus plataformas informáticas. Durante el primer cuatrimestre del presente año, se notificaron 17.292 ataques, mientras que en el mismo período para el año 2021 hubo 15.847 alertas, lo que demuestra que desde el primer cuatrimestre del año ya se ha superado el número de incidentes reportados del año pasado indicado por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) (El Comercio, 2022). El MINTEL realiza seguimiento delos ciberataques en el Centro de Respuestas a Incidentes Informáticos del Ecuador (EcuCERT) (MINTEL, s.f.)

Antecedentes: Hospital HFIB

El Hospital Francisco Icaza Bustamante (FIB), es un hospital público de referencia nacional ubicado en la avenida Quito y Gómez Rendón en la ciudad de Guayaquil, atiende a una población objetivo de hasta los 15 años de edad. El hospital es considerado de tercer nivel y brinda una atención médica integral gratuita a todos los estratos sociales, económicos y religiosos mediante servicios especializados clínicos, quirúrgicos, consulta ambulatoria y de hospitalización las 24 horas del día, con personal capacitado y responsable en las diferentes especialidades y subespecialidades médicas (FIB, n.d.).

Su infraestructura física está conformada por tres edificaciones en el área:

1. La edificación antigua donde está ubicada los pabellones de hospitalización, el área de cocina, bodega y mantenimiento.
2. La parte central es el área repotenciada que se construyó en el año 2012, donde actualmente se encuentra emergencia, farmacia, laboratorio e imagenología,
3. El nuevo edificio de dos pisos donde se encuentra la consulta externa y sala de quemados (extensión realizada en el año 2012).

En la Tabla 1 se describen los servicios que presta a la comunidad y la ubicación de los departamentos en el hospital.

Tabla 1. Descripción de los servicios de cada departamento – Hospital FIB

Servicio	Ubicación del Departamento por Piso	Ubicación por Edificación
Emergencia	Planta baja	Edificación Repotenciada
Laboratorio	Planta Baja y primer Piso	Edificación Repotenciada
Imagenología	Planta Baja	Edificación Repotenciada
Farmacia	Planta Baja	Edificación Repotenciada
Unidad de Cuidados Intensivos	Primer Piso	Edificación Antigua
Pediátricos (UCIP).	Primer Piso	Edificación Antigua
Unidad de Quemados.	Primer Piso	Edificación Repotenciada
Cirugía General.	Segundo Piso	Edificación Antigua
Cirugía Plástica y Urología	Segundo Piso	Edificación Antigua
Traumatología.	Segundo Piso	Edificación Antigua
Otorrino-Oftalmo-Neuro	Segundo Piso	Edificación Antigua
Medicina 1	Tercer Piso	Edificación Antigua
Medicina 2	Tercer Piso	Edificación Antigua
Medicina 3	Tercer Piso	Edificación Antigua
Gastroenterología	Cuarto Piso	Edificación Antigua
Nefrología	Cuarto Piso	Edificación Antigua
Cardiología	Cuarto Piso	Edificación Antigua
Infectología	Cuarto Piso	Edificación Antigua
Hematología	Quinto Piso	Edificación Antigua
Neumología	Quinto Piso	Edificación Antigua
Oncología	Quinto Piso	Edificación Antigua
Unidad de Cuidados Intensivos Neonatales (UCIN).	Quinto Piso	Edificación Antigua
Consulta Externa	Planta baja, primer y segundo piso	Nuevo Edificio
Área Administrativa	Segundo Piso	Nuevo Edificio

Fuente: Hospital del Niño “Dr. Francisco Icaza Bustamante”

Durante los 35 años de vida del hospital se ha realizado importantes cambios en la infraestructura tecnológica del hospital; en el año 2011 se procedió a la implantación de un sistema de Información y Salud (HIS) para la atención médica de los pacientes, en este se registran de las atenciones médicas de pacientes en los diferentes servicios ambulatorios, de emergencia y hospitalización.

Además, se realizó la adquisición del equipamiento principal de networking, se configuró un bunker de comunicaciones ubicado en la infraestructura vieja y en el edificio nuevo se instaló un centro de datos actualizado (data center) donde se

encuentra todo el core de la red hospitalaria. Además del Wireless controller, los servidores y el sistema de vigilancia de cámaras IP.

El Departamento de Tecnologías está compuesto por dos áreas físicas para la gestión de la infraestructura informática como se describe en la Tabla 2.

Tabla 2. Ubicación de equipos - FIB

Ubicación	Equipamiento	Estado	Descripción
Edificio nuevo – 2do. Piso	Core	En funcionamiento	
	Switch de fibra Cisco	En funcionamiento	
	Switch de distribución Cisco	En funcionamiento	
	Wirelles Controller Cisco	En funcionamiento	Controla un total de 25 Access Points de marca CISCO, instalados en toda el área repotenciada.
	Servidor Blade CISCO	En funcionamiento	Compuesto por dos servidores físicos: ▪ (03) servidores virtuales: ▪ Base de Datos Centos, ▪ Sistema Hosvital., ▪ Proxy 3 y Proxy 5 ▪ (04) servidores virtuales: a. Servidor para uso del aplicativo Hosvital en emergencia, b. Servidor para uso del aplicativo Hosvital en Hospitalización c. Aplicativo WEB. d. Aplicativo Exámenes.
	Sistema de video vigilancia Bosh	Parcialmente en funcionamiento	Controla las 209 cámaras IP instaladas en el hospital.
Edificio antiguo – Bunker	Core	En funcionamiento	
	Switch de fibra Cisco	En funcionamiento	
	Switch de distribución Cisco	En funcionamiento	
	Central Telefónica Mitel	En funcionamiento	
	Respaldo Central Telefónica Mitel	En funcionamiento	
	Switch de Fibra Cisco	En funcionamiento	
	Switch de distribución Cisco	En funcionamiento	
	Servidor IBM M4	En funcionamiento	Compuesto por dos servidores virtuales: ▪ Servidor para uso del aplicativo Hosvital en la consulta externa, farmacia, bodega y compras. ▪ Sistema Hosvital Web.

Ubicación	Equipamiento	Estado	Descripción
	Servidor IBM M3	Dañado	Compuesto por dos servidores virtuales: ▪ Servidor para uso del aplicativo Hosvital en la consulta externa. ▪ Servidor para uso del aplicativo Hosvital en farmacia, bodega y compras.

Fuente: Hospital del Niño "Dr. Francisco Icaza Bustamante"

Los usuarios finales que utilizan equipos tecnológicos como: impresoras, teléfonos IP, computadores de escritorios, equipos livianos y portátiles. Los equipos livianos son los terminales "tontos" que emulan el sistema operativo con la cual acceden al sistema Hosvital, la mayoría de ellos están ubicados en las áreas de consulta externa, emergencia y hospitalización.

En lo que respecta a los sistemas informáticos y aplicaciones en la Tabla 3 se describe los cinco aplicativos en diferentes ámbitos como son el registro de historia clínica, solicitud de órdenes de trabajo de mantenimiento y visualización de exámenes que posee el Hospital.

Tabla 3. Descripción de las aplicaciones – Hospital FIB

Sistema	Descripción	Propio	Observación
Sistema Hosvital	Para registro de historia clínica. Se encuentra también implementados módulos de bodega y compras para la parte financiera.	No	No cuenta actualmente con soporte técnico.
SmProg	Sistema para la solicitud y registro de los mantenimiento realizados por dicha área.	No	No cuenta actualmente con soporte técnico.
Laboratorio	Aplicativo web para visualización de resultados de exámenes.	Si	Se tiene código fuente.
OnlyControl	Sistema para el registro de marcaciones del personal.	No	No cuenta actualmente con soporte técnico.
Aplicativo de Talento Humano	Registro de horarios, vacaciones y permisos.	Si	Se tiene código fuente.

Fuente: Hospital del Niño "Dr. Francisco Icaza Bustamante"

En el año 2011, se instaló el sistema HOSVITAL como parte de una iniciativa para la automatización de la Información y Salud (HIS) para la atención médica de los pacientes; en este sistema se registran las atenciones médicas de los pacientes en los diferentes servicios ambulatorios, de emergencia y hospitalización por parte del

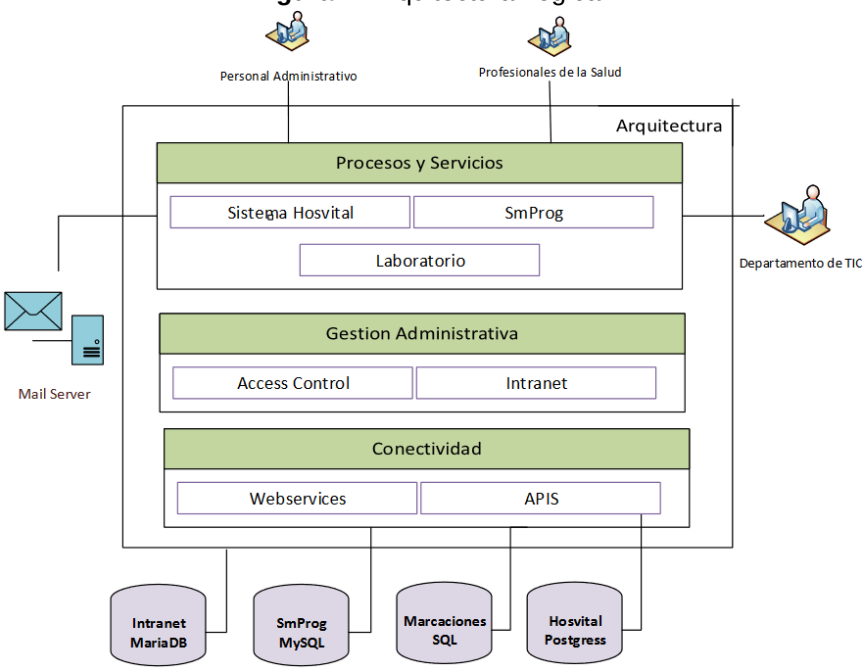
Ministerio de Salud Pública (MSP). En el año 2013, la empresa responsable dejó de brindar soporte al sistema por temas contractuales; sin embargo, a pesar de este inconveniente el hospital lo sigue usando hasta la actualidad.

En el año 2012, El sistema SmProg fue adquirido por el hospital como una solución para el registro de actividades de mantenimiento que se realizan en las diferentes áreas. En la actualidad, el sistema se sigue usando, pero se evidencian varias debilidades como el uso de las licencias y con la limitación que se ejecuta bajo el entorno de Windows XP y este no se cuenta con soporte técnico.

En el año 2016, el aplicativo web para la visualización de los resultados de exámenes fue provisto por el Hospital Abel Gilbert Pontón; el cual cuenta con el código fuente del mismo por lo que ha facilitado la ejecución de cambios y actualizaciones requeridas.

En la Figura 2 se describe la arquitectura lógica de las aplicaciones que posee al momento el Hospital FIB.

Figura 2. Arquitectura Lógica



Fuente: Hospital FIB

A pesar de contar con una importante infraestructura tecnológica, en el nuevo data center, se han detectado varias falencias como la ausencia de personal responsable de su gestión y su control.

2. Determinación del Problema

En el presente capítulo se describe la formulación del problema en el Hospital FIB en temas de seguridad, así mismo se realiza la justificación sobre la importancia de implementar una solución a corto y mediano plazo; además, se detallan los objetivos generales y específicos para el presente proyecto.

2.1. Formulación del problema

Desde sus inicios el hospital ha experimentado varios problemas relacionados con su infraestructura tecnológica que se han resuelto eventualmente; no obstante, estos se han agudizado en los últimos años y son más evidentes sobe todo por las falencias en temas de seguridad de la información.

En el año 2017, el Hospital FIB sufrió un ataque de ransomware[1] que afectó principalmente a un equipo de escritorio configurado como servidor del sistema de contratación pública (USHAY), lo que provocó la pérdida de información importante; por este motivo la alta gerencia decidió vincular un administrador de red, a quien entre otras actividades se le designó las tareas de reestructurar la red actual, establecer políticas de acceso al internet, definir una estrategia para el control de activos informáticos, asimismo, el control a los diferentes sistemas que utiliza el hospital FIB. Lamentablemente estas actividades no se pudieron concretar debido esta persona se desvinculó en el año 2018. Desde la fecha hasta la actualidad, el hospital no ha vinculado personal especializado para la ejecución de dichas actividades y mucho menos para establecer políticas y/o procedimientos que permitan garantizar la disponibilidad, confidencialidad e integridad de la información en el hospital FIB.

Durante la primera etapa de la pandemia en el año 2019, los problemas se agudizaron por la implementación del teletrabajo, por lo que el hospital empezó a

[1] Ransomware: Tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos

utilizar enlaces muy poco técnicos e inseguros basados principalmente en el aplicativo “Anydesk” y durante estas conexiones se pudo evidenciar que no existía ningún control para el acceso de manera remota a los sistemas del Hospital FIB.

El Hospital FIB ha sufrido en varias ocasiones interrupciones importantes en sus operaciones debido a situaciones fortuitas que dejaron al descubierto las vulnerabilidades existentes; uno de los eventos más relevantes ocurrió en el año 2019 por la inundación del centro de datos provisional en el nuevo edificio; esta situación afectó la operación del servidor de marcaciones, respaldos, y el sistema de mantenimiento SMPROG parando operaciones dentro del Hospital. Igualmente, con este evento se pudo detectar que la ubicación del Centro de Datos no es idónea al ubicarse debajo de grandes tuberías de agua.

Otro de los problemas críticos que se han detectado es la falta de mantenimiento del hardware de equipos causando afectación en la operación de los sistemas en el Hospital FIB. Para el año 2020, un servidor físico donde se encuentran tres servidores virtuales: un servidor de correo (Zimbra) y dos servidores para acceso al sistema de atención médica se detuvo abruptamente y por la inexistencia de un plan de contingencia afectó al registro y acceso a la información de historias clínicas de consulta externa y emergencia por una semana aproximadamente.

Desde el mes de marzo 2020, no se realizan los respaldos de las bases de datos debido a que este proceso afecta el desempeño del servidor; esta situación es muy crítica y de alto riesgo para las operaciones del Hospital FIB, sobre todo si se considera que las historias clínicas son documentos legales y la pérdida de dicha información sería altísimo impacto.

A finales del año 2021, el hospital fue objeto de una intervención de la Contraloría General del Estado; uno de los procesos revisados fueron las políticas de seguridad en especial del sistema médico; por lo que los resultados de la auditoría evidenciaron la ausencia de estrategias y mecanismos para la seguridad de la información.

Después del examen especial a los procesos preparatorio, pre contractual, contractual, ejecución, liquidación y pago, para la adquisición de bienes, servicios, consultorías, medicamentos, insumos y equipos médicos; su recepción, distribución, préstamos y uso, para la prestación de los servicios del hospital FIB; a los convenios de pago; y a los hechos relacionados con las investigaciones previas No. 090101817094981, 0901018201111446 y 090101820063328, realizado al Hospital del Niño Dr. Francisco de Icaza Bustamante, por el periodo comprendido entre el 1 de enero de 2017 y el 30 de junio de 2021, donde mediante el informe DPGY-0030-2022 la Contraloría General del Estado recomendó los siguiente:

> *"**Recomendación Nro. 4:** Implementar políticas y procedimientos relacionados con la seguridad de la información en el Hospital Dr. Francisco de Icaza Bustamante, de tal forma que se garantice la integridad, disponibilidad y confidencialidad de la información.*
>
> ***Recomendación Nro. 5:** Implementar políticas y procedimientos y efectuar las gestiones correspondientes a fin de obtener el diccionario de datos de la base de datos de HOSVITAL y estandarizar la información de los campos para la elaboración de reporte con un alto grado de confiabilidad así como también realizar correctivos en la actualización de las versiones de los servidores, implantar un plan de respaldo de la forma automática y periódica del sistema, segmentar correctamente la LAN de los servidores, implementar políticas en cuanto a las credenciales de los usuarios que utilizan el sistema HOSVITAL, implementar el registro de los usuarios que utilizan el sistema, efectuar controles en cuanto al acceso del Data Center."* (Estado, 2021)

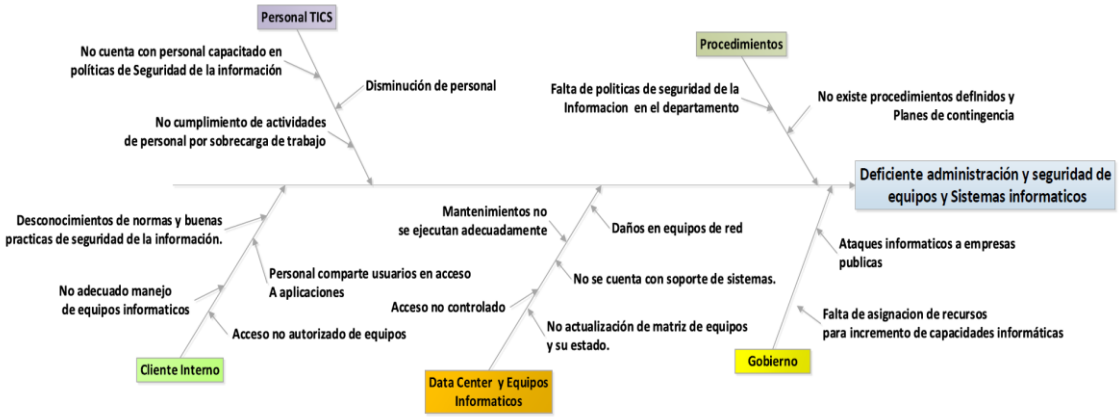
En la actualidad, el departamento de TI no cuenta con un inventario actualizado de los activos de la seguridad de la organización, tales como: computadores, portátiles, impresoras y/o equipos de red y su estado. Así mismo, el equipamiento de red que permite conectividad entre los nodos de los dos edificios es obsoleto por lo que presenta fallas frecuentes e intermitencias en los enlaces, no cuenta con soporte vigente por el fabricante y ni está asegurado ante algún daño.

Otro gran inconveniente identificado es la falta de soporte técnico o planes de mantenimiento preventivo y/o correctivo de los activos del Hospital FIB; al mismo

tiempo, uno de los mayores riesgos latentes es la falta de respaldo de la base de datos de las aplicaciones en especial del sistema HIS Hospital utilizado en la atención médica del paciente y registro de datos, siendo uno de los activos más importantes que posee el Hospital FIB.

En la Figura 3 se presenta análisis de espina realizado con los problemas identificados por el departamento de TI del Hospital FIB.

Figura 3. Árbol de Problemas – Hospital FIB



Fuente: Autor

2.2. JUSTIFICACIÓN DEL PROBLEMA

La seguridad de la información es importante para las empresas que hacen uso de sistemas informáticos y que se ven expuestos a amenazas y ataques a la información, por lo que se deben determinar políticas para la protección de la información y manejar planes de contingencia para hacer frente a las amenazas externas e internas que pueden afectar a la institución.

En el hospital FIB evidencia varios problemas relacionados con la seguridad y sus activos, siendo los más importantes la falta de procedimientos para solventar incidentes de seguridad dentro del departamento de TI y que garanticen una continuidad en la operación en el Hospital; igualmente, la obsolescencia de equipamiento informático y de red lo que provoca la ocurrencia de fallas en el sistema, conectividad y/o aplicaciones afectando la disponibilidad e integridad de la información; esto se acentúa por la limitante provisión de servicios y/o equipos

para mejorar la disponibilidad y confiabilidad de los sistemas que datan en algunos casos desde el año 2000.

Con base a las recomendaciones indicadas por la CGE, el Hospital FIB debe cumplir una política de estado de implementación de políticas y procedimientos para la seguridad aplicando estrategias de respaldos periódica y de forma automática para no tener pérdida de información; asimismo, configurar y segmentar correctamente los equipos de red LAN, Firewall y servidores con el objetivo de mejorar el control de acceso a los equipos informáticos y al centro de datos.

Se requiere un Plan Director de Seguridad en el Hospital FIB que permita la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) con el departamento de TIC, orientado a evaluar los activos de la información y sus riesgos asociados, así mismo concientizar al personal médico y administrativo sobre seguridad. Entre otros los beneficios a obtener son:

- Reducción de Riesgos: Al tener conocimiento de las vulnerabilidades que tiene el Hospital FIB se podrían aplicar planes de contingencia evitando que ocurran o disminuya el impacto a los posibles riesgos; así mismo establecer un soporte informático que pueda garantizar la operatividad de las aplicaciones propias y de terceros.
- Reducción de Costes: Al determinar y evaluar los procesos, activos fijos y aplicaciones del Hospital FIB se puede tener un mejor control y optimización de los recursos informáticos logrando un ahorro en los costos en seguridad descartando las amenazas pocos eficaces con las políticas correctas.
- Integración de la información: Todos los involucrados internos y/o externos son partícipes de las estrategias de seguridad de los activos convirtiéndose en unos de los componentes más importantes en el giro del negocio; esto puede llevarse a cabo mediante campañas de socialización de temas de seguridad y sobre el manejo responsable de la información.
- Cumplimiento de las normativas vigente: El cumplimiento de normativa legales vigentes a nivel nacional como: “Ley orgánica de protección de datos” para el

acceso de la información y su correspondiente protección de información personal (Ecuador, 2021)

- Confiabilidad de la información: Mejorar el acceso de la información al personal médico y administrativo, así como el uso eficiente y adecuado de los activos de seguridad mediante políticas de acceso local y/o remoto a los sistemas propios y de terceros.
- Disponibilidad de la información: Implementación de procesos automatizados y optimización de distribución de equipo informáticos y de red mediante un análisis de recursos y aplicaciones que posee el Hospital FIB; además, de no tener caída de servidores que impida la conexión a internet o el uso de algún otro servicio en línea.
- Reducción de ataques informáticos: Controlar los ataques de virus informáticos en los equipos y en la red del Hospital FIB, así como la denegación de servicios por medio de página web institucional acorde a lo establecido en el plan director.

2.3. Objetivos

3.3.1. Objetivo general

Diseñar un plan director de seguridad de la información para el Departamento de Tecnologías del Hospital Francisco Icaza Bustamante basado en la norma ISO27001 con la finalidad de resguardar los activos referentes a los sistemas de información de salud.

2.3.2. Objetivos específicos

- Análisis de situación del Departamento de TI del Hospital FIB con respecto a la seguridad de la información para determinar el nivel de madurez y establecer una línea base para el plan director.
- Implementar una metodología de gestión de riesgos sobre los procesos críticos y sensibles del departamento de TI mediante la identificación de los activos de

seguridad por medio del análisis de sus amenazas y vulnerabilidades en función de la normativa ISO/IEC 27005.

- Establecer políticas de seguridad de la información y controles necesarios para los activos bajo la normativa ISO27001.
- Definir los proyectos de seguridad con su respectiva planificación y los recursos necesarios para mitigar los riesgos asociados a los procesos críticos en los activos de información que se administran en el departamento de TI del hospital FIB.

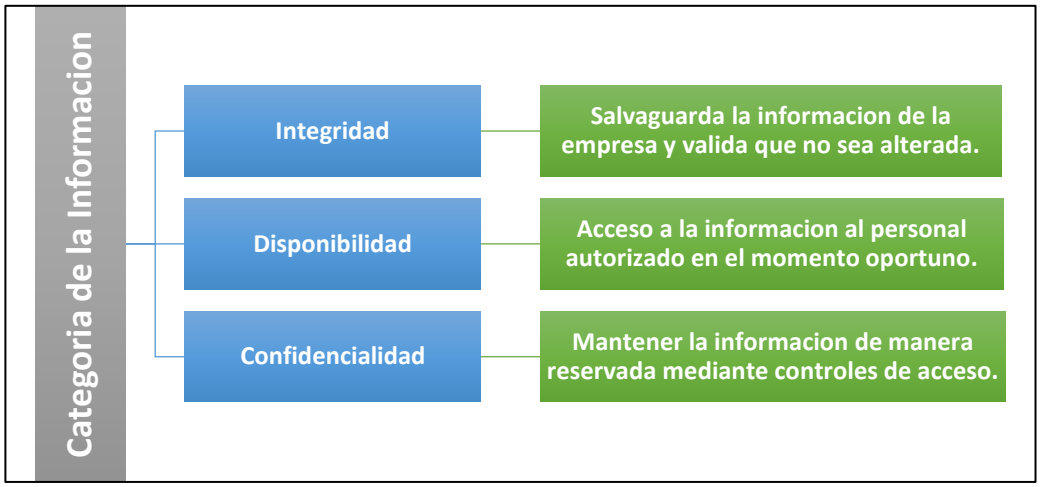
3. Marco Teórico Referencial

En este capítulo se detalla la metodología a usar para llevar a cabo este trabajo de titulación por medio de la implementación de buenas prácticas de normas ISO 27000.

3.1. Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI es un conjunto de procesos, políticas, procedimiento y directrices que permiten organizar y actuar junto a los recursos y actividades de la organización con la finalidad de proteger sus activos mediante el compromiso de la alta dirección alineados a los objetivos de la empresa. Un SGSI nos permitirá gestionar y asegurar de manera eficiente los tres principios fundamentales en énfasis a la seguridad de la información como son: la accesibilidad de la información, la confidencialidad y la disponibilidad. (Alvarado, 2021).

Figura 4 Categoría de la información



Fuente: Lara Guijarro, 2019

El manejo de la información es importante en una institución por ser sensible los datos y poder tener una disponibilidad inmediata para la toma de decisiones gerenciales acorde al mercado con los activos de la información. Los cinco grupos de procesos importantes de un SGS son:

- Procesos alineados a TI y al negocio.
- Proceso para la gestión de riesgos de seguridad.
- Procesos de cumplimiento normativo/legal.
- Proceso de sensibilización y comunicación.
- Procesos de auditoria o revisión del sistema.

3.1.1. Beneficios de un SGSI

Un SGSI en una empresa se obtiene los siguientes beneficios (ISO27000, n.d.):

- Cumplimiento de la Ley: Establecer una metodología de gestión de la seguridad clara y estructurada cumpliendo con los reglamentos, la legislación y las exigencias de la industria.
- Mejora de la imagen Corporativa: Confianza y satisfacción de los requisitos de seguridad por los clientes y otras partes interesadas.
- Asegura la continuidad del negocio: Reducir el riesgo de pérdida o robo de la información con la posibilidad de continuar la actividad después de un incidente grave o evento.
- Optimización de recursos y costes: Gestión de los activos de información que facilite la mejora continua y el ajuste a los objetivos estratégicos en cada momento sin una compra sistemática de productos y tecnología.

3.1.2. Implementación de un SGSI

La implementación de un SGSI requiere de múltiples factores, uno de esos es la participación del personal que conforman la organización; su diseño depende de los requerimientos y objetivos de la empresa (AENOR, 2014), como:

- Concientizar la necesidad de la seguridad de la información.
- Asignar Responsabilidades.
- Incorporar el compromiso de la alta dirección e interesados
- Evaluar los riesgos y determinar controles apropiados.
- Seguridad incorporada como un elemento esencial de las redes y sistemas.

- Gestión de incidentes.
- Garantizar un enfoque integral.
- Reevaluación continúa según corresponda

3.2. Familia de las normas ISO/IEC 27000

Las normas ISO/IEC 27000 está compuesta por varios estándares que se utilizan como guías para de gestión de un SGSI con el objetivo de reducir los riesgos de seguridad por la Organización Internacional de Estándares (ISO). Otros beneficios de implementar estas normas son:

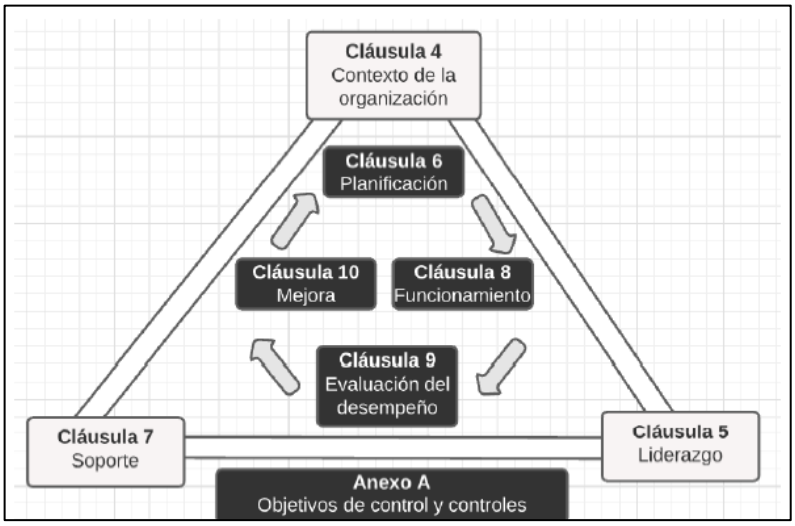
- Permitir la integración de forma coherente los objetivos de la seguridad vs los objetivos del negocio, los procesos y gestión de la empresa, capacitación y sensibilización de los empleados en la organización.
- Permitir adoptar las mejores prácticas internacionalmente aceptadas y adaptarlas a los requerimientos de cada organización.
- Establecer un glosario que permita comunicarse en la organización.
- Promover la confianza de los involucrados.
- Mejorar las expectativas de los resultados de la organización y ayuda a rentabilizar las inversiones en seguridad.

Para el desarrollo del presente trabajo se usó como guía las normas ISO/IEC 27000:

- Norma ISO/IEC 27000 Sistemas de Gestión de la Información: Visión en conjunto y vocabulario relacionados.
- Norma ISO/IEC 27001 SGSI: Establece los requerimientos de gestión y mejorar un SGSI. (GMS , n.d.) Es la única norma certificable y es parte fundamental debido a la mejora continua de la norma (Figura 4).
- Norma ISO/IEC 27002 Código de Prácticas para los controles de seguridad: Guía sobre los controles de seguridad y proporciona una serie de controles y objetivos de control como guía para lograr objetivo de la aplicación en la

selección e implementación de un SGSI con 14 dominios, 35 objetivos de control y 114 controles. (Alonso, 2015)

Figura 5 Norma ISO 27001



Fuente: PECB Group, 2005

- ISO/IEC 27005.- Guía para la gestión de riesgos de seguridad: Guía para implementar la gestión de riesgos y cumplir con lo especificado en la norma ISO/IEC 27001. No incluye específicamente alguna metodología para el análisis y gestión del riesgo, pero si ejemplos de posibles de amenazas e impactos.

Figura 6 Descripción de las Familias ISO 27000

Fuente: https://normaiso27001.es/referencias-normativas-iso-27000/

3.3. Plan director de seguridad

Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos con el objetivo de reducir los riesgos asociados a los que está expuesto la empresa a partir de un análisis de la situación inicial. (CORRECTA - Ciberseguridad | Robotización | Sales Automation | Social Listening, 2021)

El plan director de seguridad está alineado a los objetivos estratégicos del hospital FIB, donde se define el alcance y se genere las buenas prácticas de seguridad a cumplir por los trabajadores de la institución como también de terceros. (Ciberseguridad).

3.3.1. Beneficios del Plan Director de Seguridad

Los beneficios de establecer un plan director es conocer cuáles son las áreas que se encuentran expuestas a ataques y poder implementar medidas de seguridad, planes de contingencia que permiten minimizar los riesgos identificados a los activos de la información mediante la definición de planes, tiempos, plazos y costos implementar dichas medidas que se encuentran más expuestas a posibles ataques.

4. Materiales y Metodología

Para el presente trabajo se seleccionó la Norma ISO/IEC 27000 para determinar el mayor riesgo de sufrir una amenaza interna y/o externa a los activos de la información del hospital FIB; asegurando que la información es uno de los factores claves por lo que se debe evaluar el riesgo y tener un control a nivel de seguridad para la gestión de TI tomando en consideración los diferentes tipos de amenazas y vulnerabilidades.

4.1. Metodología

4.1.1. Tipo de Investigación

Investigación descriptiva

Mediante este estudio se describe las características del fenómeno observado, las diferentes variables miden el objeto de estudio (Mundi, Amazon , s.f.); se detalla la situación actual del departamento de tecnología del HFIB.

Investigación explicativa

Este tipo de estudio de investigación se puede determinar las causas o los orígenes, para este proyecto se identifican los riesgos que ocasionaría ante la pérdida del activo y los diferentes controles que se pueda implementar o los procesos que se pueda evaluar bajo la metodología ISO-20005.

Investigación de Campo

Este tipo se aplica de dos etapas para determinar e implementar las políticas dentro de la institución: la primera se realiza el seguimiento de los procesos a implementar por el departamento de TI del Hospital FIB y la segunda cuando se realice la respectiva observación en la implementación y ejecución de las políticas dentro del departamento.

4.1.2. Recolección de la información

Para el presente trabajo se efectuará mediante fuentes y técnicas de información para tener el plan director como se detalla en la Tabla 4.

Tabla 4. Descripción de tipo de recolección de información

Tipo	Subtipo	Descripción
Fuente	Primaria	Toda la información que se pueda obtener con el contacto directo con el sujeto de estudio, a través de las diferentes técnicas para la recolección de información. Para este caso se tendrá contacto directo con la Gerencia Hospitalaria, pero en especial con el departamento de TIC.
	Secundaria	Ofrecen información por investigar, pero que no son la Fuente original delos hechos o situaciones sino que solo los referencian (Mundi, Amazon, s.f.). Para este caso de estudio se tomará en cuenta las auditorías realizadas por los entes gubernamentales como Contraloría
Técnicas	Lista de chequeos	Evalúan el cumplimiento correcto para la implementación en seguridad, se efectuará mediante lista de chequeos. Estas listas se encuentran establecidas en las Normas ISO 27001, 27002, 27005.
	Entrevistas	Se procederá a realizar entrevistas, las mismas estarán estandarizadas al departamento de TIC y permitirá obtener la contestación de la lista de chequeos entre otra información relevante

Fuente: Autor

4.1.3. Procesamiento de la información

Antes de comenzar con la implantación se debe tener en cuenta aspectos como: el tamaño de la empresa, la madurez en el ámbito tecnológico, el sector al que pertenece, la legislación según su actividad, la información a tratar, el alcance del proyecto y otros elementos de la organización. Estos factores nos permitirán determinar la magnitud y complejidad del resultado del plan director en la organización. (PMG SSI - ISO 27001, 2021).

Para esto se procederá a evaluar un estado inicial del Hospital FIB, posteriormente se identificará los activos de la información y su análisis de riesgo para validar cuales son los activos más importantes y poder establecer un plan director acorde a los objetivos estratégicos del Hospital (ver Figura 7).

Figura 7. Fases del Plan Director

Fuente: Autor

Fase 1: Conocer la situación actual.

En esta fase permite conocer la situación actual del Hospital FIB en el tema de seguridad de la información acorde a la norma ISO/IEC 27001:2013, para lo cual se establece mediante 14 controles de la norma ISO-IEC 27002 validaciones de los activos desde el punto de vista tecnológico, organizacional, regulatorio y/o normativo para efectuar un análisis y determinar el punto de partida. Para su cumplimiento se debe contar con el apoyo de las máximas autoridades de esta manera se garantiza la alineación de los proyectos con los objetivos estratégicos con lo que se puede:

1. Delimitar el alcance.
2. Definir los activos y procesos del negocio

3. Definir los responsables de la gestión de activos y procesos.
4. Valoración inicial para el cumplimiento en los aspectos normativos y regulatorios del sector.
5. Análisis de cumplimiento de la seguridad y determinar la madurez tecnológica.
6. Establecer los objetivos a cumplir en ciberseguridad.

Además, se realiza un análisis técnico donde se deben valorar aspectos como: antivirus, cortafuegos, página web segura, servidores y accesos lógicos y físicos; mediante este análisis se puede comprobar la eficiencia de los controles de seguridad existentes y sus deficiencias según los factores descritos en la Tabla 6.

Tabla 6. Descripción de los controles ISO-IEC 27002

Control	Descripción
Políticas de seguridad de la información	Directrices de gestión en la seguridad.
Organización de la seguridad de la información	Organización interna, dispositivos móviles y teletrabajo.
Seguridad relativa a los recursos humanos	Gestión de personal, su vinculación y desvinculación.
Gestión de activos	Responsabilidad sobre la administración de los activos y su clasificación.
Control de acceso	Requisitos de negocio para el control de acceso y gestión de usuario en el sistema y aplicaciones.
Criptografía	Controles criptográficos.
Seguridad física y del entorno	Áreas seguras y seguridad de los equipos.
Seguridad de las operaciones	Procedimientos operacionales, protección contra el software malicioso, copias de seguridad, control del software en explotación y consideraciones sobre la auditoria de sistemas de información.
Seguridad de las comunicaciones	Gestión de la seguridad de las redes e intercambio de información.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Requisitos de seguridad en los sistemas de información, seguridad en el desarrollo y en los procesos de soporte, y datos de prueba.
Relación con proveedores	Seguridad en las relaciones con proveedores y gestión de la provisión de servicios del proveedor.
Gestión de incidentes de seguridad de la información	Gestión de incidentes y mejoras.
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	Continuidad de la seguridad y redundancias.
Cumplimiento	Cumplimiento de los requisitos legales y contractuales.

Fuente: ISO-IEC 27002

Fase 2: Preparación del SGSI.

En esta fase es necesario conocer los proyectos presentes y futuros de la empresa a largo, mediano y corto plazo mediante la verificación de la visión global de la empresa y determinar su aplicación mediante medidas de seguridad en los activos de la información. Esta actividad se debe realizar en conjunto con los responsables de todos los departamentos implicados junto con las máximas autoridades.

Fase 3: Planificación del SGSI

En esta fase se efectúa un análisis de exposición a los riesgos con la finalidad de garantizar la seguridad de los activos del Hospital FIB; para lo cual se debe seguir las siguientes actividades:

1. Identificar los activos expuestos según la Norma ISO 27000:2013 y sus posibles amenazas determinando el nivel de riesgo al que está expuesto cada activo
2. Determinar la probabilidad y las consecuencias que tiene cada activo estableciendo las amenazas a la que está expuesta y las vulnerabilidades asociadas.
3. Análisis de riesgos de los activos e implementación de controles que reducen el impacto de las amenazas acorde al apetito de riesgo a poder tratar y asumir en el Hospital FIB mediante el análisis cualitativo y cuantitativo.
4. El tratamiento al riesgo se ejecuta para determinar la forma de proteger el activo usando medidas que permitan mitigar o eliminar la amenaza, este se determinará acorde a la relación COSTO-BENEFICIO que asuman el Hospital FIB y el responsable del activo o custodio se encarga de implementar dichos controles.
5. Identificar riesgos residuales del Hospital una vez implementado el tratamiento al riesgo.

Los tipos de amenazas a la seguridad de los activos de la organización a que están expuesto de manera interna; dichas amenazas son realizadas por errores voluntarios, errores involuntarios, descuidos del personal TI o por personal

descontento dentro de la organización (HODEGHATTA, 2014), se detalla en la Tabla 5.

Tabla 5. Matriz de Amenazas y Vulnerabilidades

COD	Tipo de Amenaza	COD	Sub-Tipo Amenaza	COD	Vulnerabilidad
AME-01	*Por desastres naturales*: Eventos que suceden sin tener la intervención del ser humano directamente o indirectamente	AME-01.1	Fuego	VUL-01	Carencia o existencia de sistema de control de incendio de revisión y mantenimiento
		AME-01.2	Daños por agua	VUL-02	Falta de protección estructural contra el agua en un área susceptible a inundación
		AME-01.3	Desastres Naturales	VUL-03	Problemas de origen estructural en el edificio
AME-02	*Por desastres industriales*: Eventos que suceden accidentalmente, ocasionados por la actividad humana	AME-02.1	Falla de suministro eléctrico	VUL-04	Funcionamiento inadecuado de UPS o sistemas eléctricos auxiliares
		AME-02.2	Condiciones inadecuadas de Temperatura	VUL-05	Mal funcionamiento de climatización de la empresa
				VUL-20	Deterioro o daño de los equipo por sobrecalentamiento
		AME-02.3	Desastres industriales	VUL-06	Falta de controles ante posible fuga de químicos o sustancias biológicas
		AME-02.4	Avería de origen físico o lógico	VUL-07	Falta de controles físicos y lógicos o equipos de baja capacidad de equipo
		AME-02.5	Fallo de servicios de comunicaciones	VUL-08	Ausencia de controles en controles de autenticación o mantenimiento insuficiente
AME-03	*Errores o fallos no intencionados*: Eventos que suceden a causa de errores en la activad humano de forma no intencional	AME-03.1	Errores de los usuarios	VUL-09	Falta de controles y capacitación de los aplicativos para los usuarios
		AME-03.2	Alteración de la información	VUL-08	Ausencia de controles en validación de datos y controles de autenticación
		AME-03.3	Destrucción de la información	VUL-10	Fallo o falta de antivirus
		AME-03.4	Fuga de información	VUL-11	Inexistente controles de aseguramiento de la información

COD	Tipo de Amenaza	COD	Sub-Tipo Amenaza	COD	Vulnerabilidad
		AME-03.5	Divulgación de información	VUL-12	Sistemas no protegidos contra accesos físicos y lógicos
		AME-03.6	Vulnerabilidad de los programas	VUL-13	Falta de actualización o problemas con software no depurado
		AME-03.7	Errores de mantenimiento de programas	VUL-14	Controles bajos o nulos en la actualización de software
		AME-03.8	Restauración fallida de respaldos	VUL-15	Falta de procedimientos para general respaldos y restauración de los mismos
		AME-03.9	Errores de mantenimiento de equipos	VUL-14	Controles bajos o nulos en la actualización de software
		AME-03.10	Caída de sistemas	VUL-16	Equipos deficientes y sistemas de comunicaciones inadecuados
				VUL-21	Falta de personal capacitado
		AME-03.11	Falla de los equipos o en el equipo	VUL-08	Ausencia de controles en controles de autenticación o mantenimiento insuficiente
		AME-03.12	Disponibilidad de personal para ejecución de funciones	VUL-22	Falta de personal en las áreas para soporte a los usuarios y sobrecarga de funciones de personal contratado
AME-04	*Por ataques intencionados*: Eventos que suceden a causa de errores en la activad humano de forma intencional.	AME-04.1	Suplantación de identidad	VUL-17	Falta de controles de acceso de personal
		AME-04.2	Divulgación de información	VUL-18	Ausencia de medidas de seguridad de la información y protección de datos y controles
		AME-04.3	Acceso no autorizado	VUL-12	Sistemas no protegidos contra accesos físicos y lógicos
		AME-04.4	Manipulación de equipos	VUL-18	Ausencia de medidas de seguridad de la información y protección de datos y controles
		AME-04.5	Denegación de servicios	VUL-19	Ausencia de cifrado y ausencia de políticas de acceso

COD	Tipo de Amenaza	COD	Sub-Tipo Amenaza	COD	Vulnerabilidad
		AME-04.6	Interceptación de información	VUL-19	Ausencia de cifrado y ausencia de políticas de acceso
		AME-04.7	Ataque destructivo	VUL-19	Ausencia de cifrado y ausencia de políticas de acceso
		AME-04.8	Ingeniería social	VUL-08	Ausencia de controles en controles de autenticación o mantenimiento insuficiente
		AME-04.9	Robo	VUL-07	Falta de controles físicos y lógicos o equipos de baja capacidad de equipo
		AME-04.10	Código Malicioso	VUL-19	Ausencia de cifrado y ausencia de políticas de acceso
		AME-04.11	Denegación de Servicios (DoS)	VUL-12	Sistemas no protegidos contra accesos físicos y lógicos
		AME-04.12	Divulgación de información	VUL-12	Sistemas no protegidos contra accesos físicos y lógicos
		AME-04.13	Manipulación de software	VUL-12	Sistemas no protegidos contra accesos físicos y lógicos
				VUL-15	Falta de procedimientos para general respaldos y restauración de los mismos

Fuente: HODEGHATTA, 2014

Fase 4: Declaración de la Aplicabilidad

La declaración de aplicabilidad permite evidenciar los controles recomendados del Anexo A de la norma ISO/IEC 27002 con el análisis y evaluación del riesgo y determinar el alcance apropiados para el Hospital FIB.

1. Determinar iniciativas o acciones para mejorar los métodos actuales del trabajo para una mejora continua en los controles de seguridad.
2. Emplear acciones en énfasis a los controles físicos y técnicos ausentes que son necesarios para cerrar las brechas de seguridad.
3. Determinar los diferentes proyectos para la gestión de los riesgos y su apetito al riesgo junto con los responsables y acciones a seguir.

Fase 5: Plan Director

Una vez identificados los proyectos e iniciativas para implementar producto del análisis de situación del Hospital FIB se clasifican y priorizan teniendo en cuenta su origen y tipo de acción (criterios) con los objetivos estratégicos; igualmente, se establece los proyectos a corto, mediano y largo plazo, junto con el costo y esfuerzo que se requiere para su implementación con la aprobación de la alta gerencia.

Una recomendación es reunir un grupo de proyectos que requiera poco esfuerzo al implementarla pero que produce mejoras significativas en lo que tiene que ver con seguridad.

Fase 6: Implantación del Plan Director de Seguridad

En esta fase se implementa los proyectos establecidos en el Plan Director según el plazo, se debe tomar en cuenta lo siguiente:

1. Presentación del proyecto al personal y a los departamentos.; además la línea de tiempo con los objetivos que se persiguen para cada proyecto.
2. Asignar responsabilidades y la coordinación de cada proyecto establecido.
3. Determinar métodos de seguimiento de proyectos en el plan.
4. Identificar las auditorías de los riesgos que han sido subsanados.

4.2. Fase I: Conocer la Situación Actual (GAP)

El Hospital FIB tiene como función principal la atención a los pacientes de la ciudad de Guayaquil y alrededores mediante el uso de activos que permitan la continuidad de las operaciones. Se va a realizar un estado inicial para la Seguridad de la Información.

4.2.1. Dominio y Control de Seguridad de la Información

En esta sección se efectúa un análisis de la información tecnológica con el objetivo de determinar un punto de partida (estado inicial) para el cumplimiento de la

seguridad en el hospital FIB; para esto se determinó mediante los 14 controles del Anexo A de la norma ISO/IEC 27001 por medio entrevistas, inspecciones y verificaciones en sitio detallada en el Anexo B

En la Tabla 7 se describen los ocho criterios de evaluación para el cumplimiento de control de la norma ISO/IEC 27001 mediante la verificación de actividades que estén alineadas con el objetivo de la institución y son analizados en conjunto. (NORMA ISO27001, 2021).

Tabla 7. Criterios de Evaluación del ISO/IEC 27001

Estado	Significado
? Desconocido	No ha sido verificado
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Fuente: ISO-IEC 27001

4.3. Fase II: Preparación del SGSI

Para la preparación de un SGSI se debe obtener un punto de partida mediante la identificación del entorno del Hospital FIB y sus activos:

- Comprender la organización y su contexto.
- Determinar el Alcance de SGSI
- Definir la Política y Objetivo de SGSI
- Definir la Estructura Organizacional del SGSI

4.3.1. Analizar el Contexto Organizacional

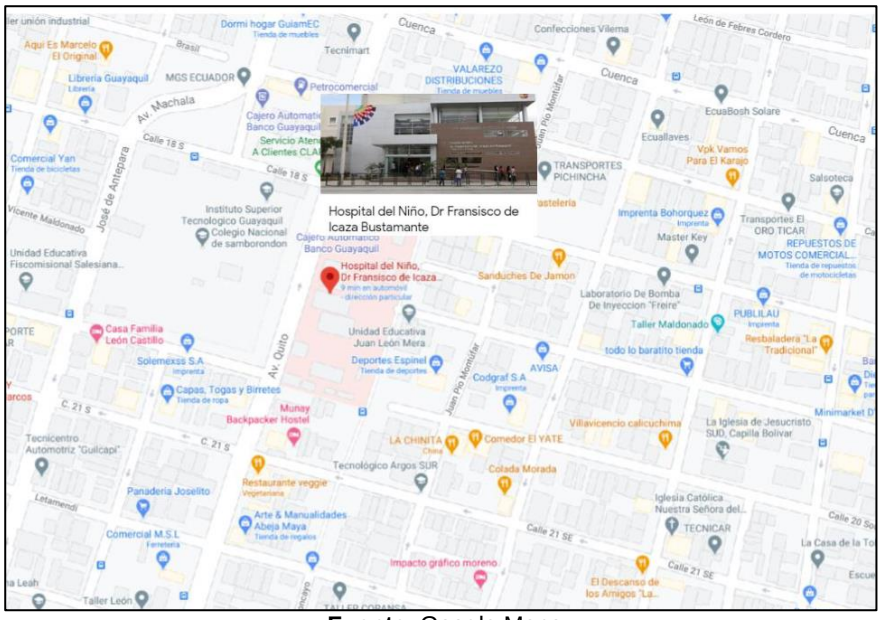
El análisis de contexto organización se debe entender la situación inicial de Hospital FIB con:

- El conocimiento y capacidad de la organización
- La gestión y gobierno de la organización
- Los aspectos tecnológicos

Conocimiento y capacidad de la organización

El Hospital Francisco Icaza Bustamante (FIB) es un hospital público de referencia nacional ubicado en la avenida Quito y Gómez Rendón en la ciudad de Guayaquil en la parroquia Ayacucho, que atiende a población objetivo de hasta los 15 años de edad. El hospital es considerado de tercer nivel; y brinda una atención médica integral y gratuita a todos los estratos sociales, económicos y religiosos, ofrece servicios especializados clínicos, quirúrgicos, consulta ambulatoria y de hospitalización las 24 horas del día, con personal capacitado y responsable en las diferentes especialidades y subespecialidades médicas (FIB, n.d.).

Figura 8 Ubicación del Hospital FIB



Fuente: Google Maps

Visión

"*Prestar servicios de salud con calidad y calidez en el ámbito de la asistencia especializada, a través de su cartera de servicios, cumpliendo con la responsabilidad de promoción, prevención, recuperación, rehabilitación de la salud integral, docencia e investigación, conforme a las políticas del Ministerio de Salud Pública y el trabajo en red, en el marco de la justicia y equidad social*" (HFIB, Plan Estratégico del HFIB, 2017)

Misión

"*Ser reconocidos por la ciudadanía como hospitales accesibles, que prestan una atención de calidad que satisface las necesidades y expectativas de la población bajo principios fundamentales de la salud pública y bioética, utilizando la tecnología y los recursos públicos de forma eficiente y transparente*" (HFIB, Plan Estratégico del HFIB, 2017).

Objetivo Empresarial

Los objetivos estratégicos del Hospital del Niño "Francisco Icaza Bustamante" se alinean con los del Ministerio de Salud Pública (MSP) y demás Hospitales:

- Objetivo 1: Garantizar la equidad en el acceso y gratuidad de los servicios.
- Objetivo 2: Trabajar bajo los lineamientos de atención integral de salud de forma integrada y en red con el resto de unidades operativas de Salud
- Objetivo 3: Mejorar la accesibilidad y el tiempo de espera para recibir atención, considerando la diversidad de género, cultural, socio económica, lugar de origen y discapacidades.
- Objetivo 4: Involucrar a los profesionales en la gestión del hospital, aumentando su motivación, satisfacción y compromiso con la misión del hospital.
- Objetivo 5: Garantizar una atención de calidad y respeto a los derechos de los usuarios para lograr la satisfacción con la atención recibida.
- Objetivo 6: Desarrollar una cultura de excelencia con el fin de optimizar el manejo de los recursos públicos y la rendición de cuentas. (HFIB, 2012)

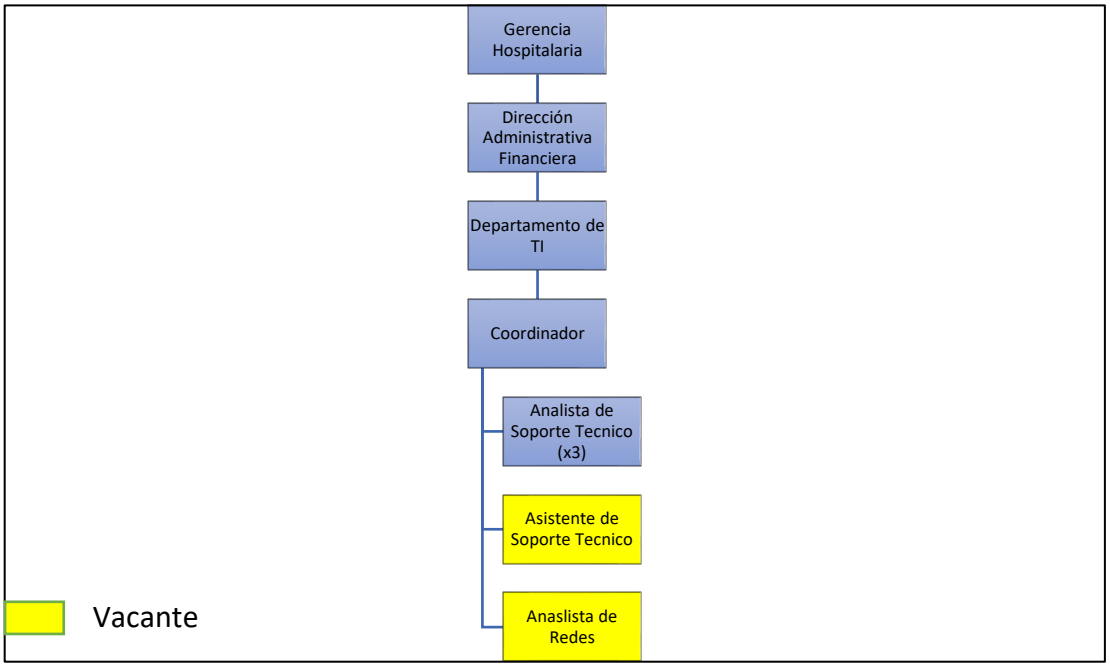
Gestión y gobierno de la organización

La estructura organizacional del Hospital FIB debe estar alineada con la misión del Ministerio de Salud Pública (MSP) junto con el Modelo de Atención y de Gestión Hospitalaria; deben están acorde a las políticas definidas en la "Constitución de la República del Ecuador", Políticas del Estado Ecuatoriano, leyes y otras normas ecuatorianas vigentes. En el Anexo A se muestra la estructura orgánica del Hospital FIB.

Organigrama de TI

El departamento de TI está conformado por un coordinador y tres analistas de soporte técnico; además, no cuenta con un asistente de soporte técnico, ni administrador de red a pesar de tener partidas presupuestarias para dichos perfiles. En la Figura 9 se muestra la estructura del departamento TI del hospital FIB mismo que forma parte de la Dirección Administrativa Financiera.

Figura 9. Estructura del Departamento de TIC



Fuente: Hospital FIB

Aspectos tecnológicos

Los aspectos técnicos de los activos fijos se registraron mediante inspecciones físicas y entrevistas al personal durante las visitas a las instalaciones del Hospital

Francisco Icaza Bustamante (FIB); específicamente al departamento de TI, donde se pudo constatar en el recorrido sobre su infraestructura tecnológica, equipos, políticas, aplicaciones y recurso humano. Cabe recalcar que en este departamento no se evidenciaron políticas o procedimientos establecidos formalmente

La información se clasificó de acuerdo a las siguientes categorías:

- Infraestructura: Detalle del conjunto de medios técnicos como servidores (Físicos y Lógicos), base de datos, estaciones de trabajo para cumplimiento de las actividades diarias, centro de datos, cableado estructurado que se tiene en el hospital, los medios y/o dispositivos de respaldo para la ejecución de trabajos en el Hospital FIB.
- Servicios: Detalle de los servicios internos o externos (subcontratados) como son el software, sistemas de información y/o consultorías que existen en el Hospital FIB para realizar los trabajos diarios.
- Aplicaciones: Describe el tipo de software desarrollado por personal interno o externo que se ejecuta en los computadores para realizar funciones y/o actividades diarias en el Hospital FIB.
- Políticas: Detalle del conjunto de reglas definidas y aplicadas para la seguridad en el Departamento de TI para realizar las actividades del Hospital.

4.3.2. Alcance del Plan de Seguridad

El objetivo planteado por el Departamento de TI del Hospital FIB para el Plan director en los componentes de seguridad es:

- Establecer los recursos necesarios en tiempo, costo y esfuerzo mediante la identificación de los activos que comprende el personal de tecnología, activos tecnológicos e infraestructura del Hospital FIB.
- Diseñar e implementar del plan director acorde al cronograma y presupuesto aprobado por la alta gerencia, este debe incluir los procesos para la seguridad de la información acorde a los objetivos institucionales y mapa del proceso del Hospital FIB.

- Alinear los requisitos y controles de seguridad e preservando los principios de fundamentales de seguridad (integridad, confiabilidad y disponibilidad).

4.3.3. Política y objetivos del plan director de seguridad

Como parte principal del plan director se establece un análisis para la gestión de los activos de la información (ISO, 2015), conjuntamente con las amenazas/vulnerabilidades a los que están expuestos y su análisis al tratamiento del riesgo y poder elaborar las políticas de la seguridad del Hospital FIB, el Plan Director deberá contemplar:

- Definir roles de seguridad dentro de la estructura organizacional del Hospital FIB, que incluya un oficial de seguridad de la información y/o comité de seguridad que serán los encargados de la gestión de los activos en temas de seguridad y manejo de incidentes según las normas ISO 2700 en el Hospital FIB.
- Establecer los lineamientos para el uso apropiado de la gestión de activos acorde a la política de seguridad y socializarlos con los empleados del Hospital FIB.
- Determinar procedimientos para el inventario de los activos y sus controles, en especial de aquellos que contengan información sensible que pudiera afectar la operatividad del Hospital FIB.
- Establecer políticas claras de seguridad relacionadas con las autorizaciones o gestión en el acceso a los activos, copias de seguridad, almacenamiento según su prioridad, seguridad física; asimismo la manipulación de medios de soporte electrónicos.
- Establecer lineamientos de seguridad en las operaciones e instalaciones físicas para el procesamiento de los datos en el Hospital FIB.
- Especificar procedimientos de seguridad en la gestión de las comunicaciones internas y/o externas que permitan una disponibilidad de la información en el Hospital FIB.

Uno de los puntos importantes es la designación del oficial de seguridad de la información, quien es responsable de la(s) política(s) y que supervisará el cumplimiento periódico en cuanto a la protección de la información, monitoreo y control de medidas de seguridad.

4.3.4. Estructura Organizacional (definición de roles y responsabilidades)

El diseño e implementación del Plan director para el Hospital FIB se lo realizará con la designación de responsabilidades mediante los roles descritos en la Tabla 8 para poder resguardar los activos junto con los servicios brindados.

Tabla 8. Roles y Responsabilidades para implementar SGSI – Hospital FIB

Roles	Responsabilidades
Gerencia General Hospitalaria	Toma de decisiones estratégicas acorde a los lineamientos establecidos por el Ministerio de Salud Pública.
Gerente Dirección Administrativa Financiera	Toma de Decisiones para Validación de funciones organizaciones del Hospital
Comité de la Seguridad	Grupo de personas que maneja la gestión de los activos de la información en el Hospital, el cual está integrado por el Gerente Administrativo, administrador de TI y un delegado de Gerencia General.
Equipo de planificación de seguridad de la información	Grupo de personas que durante la implementación del SGSI y del plan director van a trabajar con los departamentos involucrados para la gestión el cambio, resuelve los conflictos y escala en caso de ser necesario a la Dirección Administrativa para establecer el SGSI.
Grupo de interés	Personas u organizaciones que pertenecen a los departamentos involucrados que intervienen directamente en la implementación del SGSI.
Administrador de Sistemas	Persona responsable en de la Administración de los Sistema de TI en el Hospital.
Coordinador de TI	Persona que gestiona los recursos de TI en el Hospital.
Administrador de Redes	Persona responsable de la Seguridad Física y comunicaciones.
Gestor de Riesgo	Persona responsable en la validación de la gestión de riesgos en el Hospital para el área de seguridad de la información.
Oficial de la Seguridad de la Información	Persona responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema de Seguridad de la Información.

Fuente: Autor

4.4. Fase III: Planificación del plan director de seguridad

La planificación del plan director como parte del SGSI comienza con la gestión de activos, valoración de las amenazas y su análisis de riesgos acorde a los objetivos estratégicos del Hospital FIB.

4.4.1. Identificación y clasificación los activos

En esta sección se identifica los activos del Hospital FIB que permita al propietario protegerlo en base a su importancia presentados en la Tabla 9.

Tabla 9. Identificación de activos – Hospital FIB

COD	PROCESO	Tipo Activo	NOMBRE	Descripción del activo
A1	Tecnologías de la información y comunicación	Hardware	Router de frontera	Equipo de conexión a Internet
A2	Tecnologías de la información y comunicación	Redes	Core Cisco	Equipo central de la red de comunicación.
A3	Tecnologías de la información y comunicación	Redes	Firewall Cisco	Puntos de acceso inalámbrico
A4	Tecnologías de la información y comunicación	Redes	Wireless Controller	Equipo para el control de los Access Point
A5	Tecnologías de la información y comunicación	Hardware	Sistema de Video Vigilancia	Equipos para la grabación de videos del sistema BOSCH
A6	Tecnologías de la información y comunicación	Redes	Servidor Cisco 1	Servidor donde se aloja servidores virtuales (Base de Datos Hosvital, proxy 3 y 5)
A7	Tecnologías de la información y comunicación	Redes	Servidor Cisco 2	Servidor donde se aloja servidores virtuales (Server RedHat - Emergencia y Hospitalización, Laboratorio)
A8	Tecnologías de la información y comunicación	Redes	Servidor IBM M3	Servidor donde se aloja servidores virtuales (Server RedHat - Farmacia, Bodega y Compras Públicas)
A9	Tecnologías de la información y comunicación	Redes	Servidor IBM M4	Servidor donde se aloja servidores virtuales (Server RedHat - Consulta Externa)

COD	PROCESO	Tipo Activo	NOMBRE	Descripción del activo
A10	Tecnologías de la información y comunicación	Hardware	PC / Servidor 1	PC donde está instalado SMPROG y Sistema SERCOP
A11	Tecnologías de la información y comunicación	Hardware	PC / Servidor 2	PC donde se encuentra instalado sistema de marcaciones
A12	Tecnologías de la información y comunicación	Hardware	PC / Servidor 3	PC donde se encuentra instalado sistema y base de datos aplicativo de Talento Humano
A13	Tecnologías de la información y comunicación	Hardware	PC / Servidor 4	PC - instalado Base de Datos de Laboratorio
A14	Tecnologías de la información y comunicación	Hardware	PC / Servidor 5	PC donde se encuentra instalado aplicativo Jaspersoft
A15	Tecnologías de la información y comunicación	Hardware	PC / Servidor 6	PC - instalado Servidor de Correo Zimbra
A16	Tecnologías de la información y comunicación	Hardware	PC / Servidor 7	PC donde se encuentra instalado Proxy 56
A17	Tecnologías de la información y comunicación	Hardware	MITEL Principal	Central Telefónica Principal
A18	Tecnologías de la información y comunicación	Hardware	MITEL Secundario	Central Telefónica Respaldo
A19	Tecnologías de la información y comunicación	Hardware	Data Center 1	Centro de datos con la infraestructura actual
A20	Tecnologías de la información y comunicación	Hardware	Data Center 2	Centro de datos con la infraestructura antigua
A21	Tecnologías de la información y comunicación	Hardware	Nodo 1	Rack Swith de Distribución de red
A22	Tecnologías de la información y comunicación	Hardware	Nodo 2	Rack Swith de Distribución de red
A23	Tecnologías de la información y comunicación	Hardware	Nodo 3	Rack Swith de Distribución de red
A24	Tecnologías de la información y comunicación	Hardware	Nodo 4	Rack Swith de Distribución de red
A25	Tecnologías de la información y comunicación	Hardware	Nodo 5	Rack Swith de Distribución de red
A26	Tecnologías de la información y comunicación	Hardware	Nodo 6	Rack Swith de Distribución de red
A27	Tecnologías de la información y comunicación	Hardware	Nodo 7	Rack Swith de Distribución de red
A28	Tecnologías de la información y comunicación	Hardware	Nodo 8	Rack Swith de Distribución de red
A29	Tecnologías de la información y comunicación	Hardware	Nodo 9	Rack Swith de Distribución de red
A30	Tecnologías de la información y comunicación	Hardware	Nodo 10	Rack Swith de Distribución de red
A31	Tecnologías de la información y comunicación	Hardware	Nodo 11	Rack Swith de Distribución de red
A32	Tecnologías de la información y comunicación	Hardware	Nodo 12	Rack Swith de Distribución de red

COD	PROCESO	Tipo Activo	NOMBRE	Descripción del activo
A33	Tecnologías de la información y comunicación	Software	Sistema Hosvital	Software para el registro de Historia Clínica
A34	Tecnologías de la información y comunicación	Software	Sistema De talento Humano	Registro de Horarios de Personal, permisos (médicos y descuento a vacaciones), solicitud de Vacaciones
A35	Tecnologías de la información y comunicación	Software	Sistema MS-PROG	Registro de Ordenes de Trabajo para el Área de Mantenimiento.
A36	Tecnologías de la información y comunicación	Software	Zimbra	Correo Electrónico Institucional
A37	Tecnologías de la información y comunicación	Software	Jaspersoft	Sistema para reportes del Sistema Hosvital
A38	Tecnologías de la información y comunicación	Software	Sistema de Marcaciones	Sistema para la creación del personal y marcaciones
A39	Tecnologías de la información y comunicación	Software	Sistema SERCOP	Módulo facilitador de Contratación Pública
A40	Tecnologías de la información y comunicación	Software	Wireless Controller	Sistema para el control de los Access Point
A41	Tecnologías de la información y comunicación	Software	Sistema Video vigilancia BOSCH	Sistema para el control de alarmas de seguridad y cámaras
A42	Tecnologías de la información y comunicación	Software	Proxy 3	Proxy de Navegación para el área administrativa
A43	Tecnologías de la información y comunicación	Software	Proxy 5	Proxy de Navegación para el área médica
A44	Tecnologías de la información y comunicación	Software	Proxy 56	Proxy de Navegación para el área administrativa / respaldo
A45	Tecnologías de la información y comunicación	Software	Server Red Hat 1	Sistema Operativo virtual para Consulta Externa
A46	Tecnologías de la información y comunicación	Software	Server Red Hat 2	Sistema Operativo virtual para Hospitalización
A47	Tecnologías de la información y comunicación	Software	Server Red Hat 3	Sistema Operativo virtual para Emergencia
A48	Tecnologías de la información y comunicación	Software	Server Red Hat 4	Sistema Operativo virtual para Farmacia, bodega y Compras
A49	Tecnologías de la información y comunicación	Software	Laboratorio	Sistema para visualización de resultados de exámenes
A50	Tecnologías de la información y comunicación	Software	Sistema MITEL	Sistema Administrador de la Central Telefónica
A51	Tecnologías de la información y comunicación	Información	Base de Datos Hosvital	Base de Datos Postgresql para el registro de historia clínica

COD	PROCESO	Tipo Activo	NOMBRE	Descripción del activo
A52	Tecnologías de la información y comunicación	Información	Base de Datos Sistema de Talento Humano	Base de Datos MariaDB para el registro de información de la plataforma de talento humano
A53	Tecnologías de la información y comunicación	Información	Base de Datos MSPROG	Base de Datos MySQL para registro de información del sistema de mantenimiento
A54	Tecnologías de la información y comunicación	Información	Base de Datos Sistema de Marcaciones	Base de Datos MySQL para el registro de marcaciones del personal.
A55	Tecnologías de la información y comunicación	Información	Base de Datos Laboratorio	Base de Datos MySQL para almacenar la información de resultados de exámenes de laboratorio.
A56	Tecnologías de la información y comunicación	Hardware	PC 1	PC del Coordinador del Departamento
A57	Tecnologías de la información y comunicación	Hardware	Portátil 1	Portátil -administración del Sistema Hosvital y Servidores
A58	Tecnologías de la información y comunicación	Recursos Humanos	Administrador de Sistema Hosvital	Personal con conocimientos en el sistema de registro de historia clínica. Bases de Datos y Servidores - procesos que se llevan en el departamento y del hospital.
A59	Tecnologías de la información y comunicación	Recursos Humanos	Administrador de Sistemas	Personal encargado de la administración de los sistemas instalados
A60	Tecnologías de la información y comunicación	Recursos Humanos	Analista de Redes	Personal encargado de la infraestructura de red y base de datos
A61	Tecnologías de la información y comunicación	Recursos Humanos	Responsable de la Seguridad de la información	Personal encargado de la ciberseguridad de la institución
A62	Tecnologías de la información y comunicación	Software	Antivirus corporativo	Software para detección de malware en lo equipos y en la red
A63	Tecnologías de la información y comunicación	Software	Sistema Operativo W10	Sistema operativo instalado en los equipos finales
A64	Tecnologías de la información y comunicación	Hardware	Equipos PC	Equipos de cómputo para uso de usuarios finales
A65	Tecnologías de la información y comunicación	Hardware	Portátiles	Equipos portátiles para uso de usuario finales

COD	PROCESO	Tipo Activo	NOMBRE	Descripción del activo
A66	Tecnologías de la información y comunicación	Organización	Internet	Servicio para proveer de Internet a la institución
A67	Tecnologías de la información y comunicación	Organización	Impresiones	Servicio para proveer al hospital del servicio de impresiones (impresoras y suministros como tóner)

Fuente: Hospital FIB

En el Anexo C se detalla los activos identificados para el Hospital FIB y la descripción de sus columnas se detalla en la Tabla 10.

Tabla 10. Descripción de los campos de activos

Campo	Descripción
Código	Numérico código del activo tecnológico.
Tipo	Se describe el tipo de activo tecnológico que se tiene en el Hospital FIB, puede ser: ▪ Información: Ficheros o base de datos el activo tecnológico, el cual es un archivo abstracto y sirve para soporte o transferir información, configurar datos, código fuente. ▪ Organización: Implementados acorde a los requerimientos de los usuarios, pueden ser: páginas web, correo electrónico, servicio FTP, intranet, sistemas de incidentes. ▪ Software: Aplicaciones informáticas internas y/o externas que hacen referencia para gestionar, analizar y transformar los datos en información acorde a lo requerido en el Hospital. ▪ Equipos Informáticos (Hardware): Medios físicos destinados a sobrellevar los servicios o aplicaciones que tiene el Hospital, estos pueden ser: servidores, equipos de escritorios o portátiles, router, impresoras o dispositivos electrónicos. ▪ Redes: Instalación dedicada para la conectividad de las plataformas informáticas utilizadas en el hospital sea propias o contratados por terceros, como redes locales o inalámbricas. ▪ Soportes de información: Dispositivos que permiten un almacenamiento de la información de forma temporal, permanente o a manera de respaldos. ▪ Recursos Humanos: Personas relacionadas con los sistemas del hospital FIB, pueden ser administradores u operadores responsables de los activos; pueden ser internos y/o externos.
Propietario	Describe el dueño del activo, para este ejercicio puede ser Hospital FIB, alquilado u rentado a terceros.
Custodio	Responsable del activo.
Ubicación	Lugar donde se encuentra ubicado el activo informático, puede ser edificios, cuarto de equipos o vehículos usados de uso exclusivo del personal de TI.
Medio	Indica si el activo tecnológico es físico o digital.

Campo	Descripción
Nivel de Clasificación	Identifica la clasificación del activo de acuerdo a los criterios y medios de comunicación diferentes, puede ser cuatro niveles: ▪ Confidencial: cuando se presenta un nivel mayor de confidencialidad porque causa impacto a los objetivos empresariales a largo plazo o pone en riesgo la operatividad del hospital FIB. ▪ Restringida: nivel medio de confidencialidad, la divulgación tiene un impacto significado a corto plazo. ▪ De uso interno: nivel más bajo de confidencialidad o su divulgación afecta la operación de la empresa en menor grado. ▪ Público: cuando la información es accesible a todo público, su divulgación no causa ningún daño.

Fuente: Autor

4.4.2 Evaluación y valoración de los activos

La valoración y evaluación del activo del Hospital FIB permitirá calcular la probabilidad e impacto en las operaciones y/o actividades mediante un análisis cualitativos y cuantitativos.

VALORACIÓN DE ACTIVOS

Para la valoración del impacto en cada activo del Hospital FIB (VA) se aplicó la siguiente fórmula acorde a los criterios de evaluación descritos en la Tabla 11:

$$VA = \frac{\mathrm{C} + \mathrm{I} + \mathrm{D}}{3}$$

Tabla 11. Criterios de Impacto acorde a ISO 27001

Criterio	Descripción	Impacto	Valor
Confidencialidad (C)	El impacto existe pero es insignificante	Bajo	1
	La divulgación no autorizada tiene impacto limitado para la organización.	Medio	2
	La divulgación no autorizada tiene impacto alto para la organización.	Alto	3
	La divulgación no autorizada tiene impacto a los objetivos empresariales	Muy Alto	4
Integridad	El impacto existe pero es insignificante	Bajo	1

Criterio	Descripción	Impacto	Valor
(I)	La destrucción o modificación tiene un efecto leve para la empresa	Medio	2
	La destrucción o modificación no autorizada tiene un impacto considerable para la organización	Alto	3
	La destrucción o modificación no autorizada tiene un impacto severo para la organización	Muy Alto	4
Disponibilidad (D)	El impacto existe pero es insignificante	Bajo	1
	La interrupción al acceso de los sistemas tienen impacto leve para la organización	Medio	2
	La interrupción al acceso de los sistemas tienen impacto considerable para la organización	Alto	3
	La interrupción al acceso de los sistemas tienen impacto severo para la organización	Muy Alto	4

Fuente: ISO 27001

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES (ANÁLISIS DEL RIESGO)

El análisis de riesgo de los activos identificados junto con las amenazas y/o vulnerabilidades por cada activo del Hospital FIB a lo que están expuestos en la Tabla 12, en la columna de controles implementados valida la existencia de salvaguardas y/o mecanismos implementados en caso de existir en el Hospital; en caso de no existir un control implementado se colocará "---".

Tabla 12. Análisis de Riesgo y Controles Implementados

COD	Activo	Amenaza	Vulnerabilidad	Control
A1	Router de frontera	AME-02.5	VUL-08	A15.2.1
A1	Router de frontera	AME-01.2	VUL-02	---
A2	Core Cisco	AME-02.5	VUL-08	---
A2	Core Cisco	AME-01.2	VUL-02	---
A3	Firewall Cisco	AME-02.5	VUL-08	---
A3	Firewall Cisco	AME-01.2	VUL-02	---
A4	Wireless Controller	AME-02.5	VUL-08	---
A4	Wireless Controller	AME-01.2	VUL-02	---
A5	Sistema de Video Vigilancia	AME-02.5	VUL-08	---
A5	Sistema de Video Vigilancia	AME-01.2	VUL-02	---
A6	Servidor Cisco 1	AME-03.11	VUL-08	---
A6	Servidor Cisco 1	AME-01.2	VUL-02	---
A7	Servidor Cisco 2	AME-03.11	VUL-08	---
A7	Servidor Cisco 2	AME-01.2	VUL-02	---
A8	Servidor IBM M3	AME-03.11	VUL-08	---
A8	Servidor IBM M3	AME-03.10	VUL-16	---
A9	Servidor IBM M4	AME-03.11	VUL-08	---
A9	Servidor IBM M4	AME-03.10	VUL-16	---
A10	PC / Servidor 1	AME-03.11	VUL-08	---
A10	PC / Servidor 1	AME-03.10	VUL-16	---
A11	PC / Servidor 2	AME-03.11	VUL-08	---

COD	Activo	Amenaza	Vulnerabilidad	Control
A11	PC / Servidor 2	AME-01.2	VUL-02	---
A11	PC / Servidor 2	AME-03.10	VUL-16	---
A12	PC / Servidor 3	AME-03.11	VUL-08	---
A12	PC / Servidor 3	AME-03.10	VUL-16	---
A13	PC / Servidor 4	AME-03.11	VUL-08	---
A13	PC / Servidor 4	AME-03.10	VUL-16	---
A14	PC / Servidor 5	AME-03.11	VUL-08	---
A14	PC / Servidor 5	AME-02.1	VUL-04	---
A14	PC / Servidor 5	AME-03.10	VUL-16	---
A15	PC / Servidor 6	AME-03.11	VUL-08	---
A15	PC / Servidor 6	AME-02.1	VUL-04	---
A15	PC / Servidor 6	AME-03.10	VUL-16	---
A16	PC / Servidor 7	AME-03.11	VUL-08	---
A16	PC / Servidor 7	AME-02.1	VUL-04	---
A16	PC / Servidor 7	AME-03.10	VUL-16	---
A17	MITEL Principal	AME-03.11	VUL-08	---
A18	MITEL Secundario	AME-03.11	VUL-08	---
A19	Data Center 1	AME-01.2	VUL-02	---
A19	Data Center 1	AME-02.2	VUL-20	A11.2.2
A19	Data Center 1	AME-04.9	VUL-07	---
A20	Data Center 2	AME-02.1	VUL-04	---
A20	Data Center 2	AME-02.2	VUL-20	A11.2.2
A21	Nodo 1	AME-02.5	VUL-08	---
A21	Nodo 1	AME-03.10	VUL-16	---
A21	Nodo 1	AME-04.9	VUL-07	---
A22	Nodo 2	AME-02.5	VUL-08	---
A22	Nodo 2	AME-03.10	VUL-16	---
A22	Nodo 2	AME-04.9	VUL-07	---
A23	Nodo 3	AME-02.5	VUL-08	---
A23	Nodo 3	AME-03.10	VUL-16	---
A23	Nodo 3	AME-04.9	VUL-07	---
A24	Nodo 4	AME-02.5	VUL-08	---
A24	Nodo 4	AME-03.10	VUL-16	---
A24	Nodo 4	AME-04.9	VUL-07	---
A25	Nodo 5	AME-02.5	VUL-08	---
A25	Nodo 5	AME-03.10	VUL-16	---
A25	Nodo 5	AME-04.9	VUL-07	---
A26	Nodo 6	AME-02.5	VUL-08	---
A26	Nodo 6	AME-03.10	VUL-16	---
A26	Nodo 6	AME-04.9	VUL-07	---
A27	Nodo 7	AME-02.5	VUL-08	---
A27	Nodo 7	AME-03.10	VUL-16	---
A27	Nodo 7	AME-04.9	VUL-07	---
A28	Nodo 8	AME-02.5	VUL-08	---
A28	Nodo 8	AME-03.10	VUL-16	---
A28	Nodo 8	AME-04.9	VUL-07	---
A29	Nodo 9	AME-02.5	VUL-08	---
A29	Nodo 9	AME-03.10	VUL-16	---

COD	Activo	Amenaza	Vulnerabilidad	Control
A29	Nodo 9	AME-04.9	VUL-07	---
A30	Nodo 10	AME-02.5	VUL-08	---
A30	Nodo 10	AME-03.10	VUL-16	---
A30	Nodo 10	AME-04.9	VUL-07	---
A31	Nodo 11	AME-02.5	VUL-08	---
A31	Nodo 11	AME-03.10	VUL-16	---
A31	Nodo 11	AME-04.9	VUL-07	---
A32	Nodo 12	AME-02.5	VUL-08	---
A32	Nodo 12	AME-03.10	VUL-16	---
A32	Nodo 12	AME-04.9	VUL-07	---
A33	Sistema Hosvital	AME-03.10	VUL-16	---
A33	Sistema Hosvital	AME-03.6	VUL-13	---
A33	Sistema Hosvital	AME-03.7	VUL-14	---
A33	Sistema Hosvital	AME-03.4	VUL-11	A9.2.1
A33	Sistema Hosvital	AME-03.10	VUL-16	---
A34	Sistema De talento Humano	AME-03.10	VUL-16	---
A34	Sistema De talento Humano	AME-03.10	VUL-16	---
A35	Sistema MS-PROG	AME-03.10	VUL-16	---
A35	Sistema MS-PROG	AME-03.10	VUL-16	---
A36	Zimbra	AME-03.10	VUL-16	---
A36	Zimbra	AME-04.13	VUL-15	---
A36	Zimbra	AME-03.1	VUL-09	---
A36	Zimbra	AME-03.10	VUL-16	---
A37	Jaspersoft	AME-03.10	VUL-16	---
A37	Jaspersoft	AME-03.10	VUL-16	---
A38	Sistema de Marcaciones	AME-03.10	VUL-16	---
A38	Sistema de Marcaciones	AME-03.10	VUL-16	---
A39	Sistema SERCOP	AME-03.10	VUL-16	---
A40	Wireless Controller	AME-03.10	VUL-16	---
A41	Sistema Video vigilancia BOSCH	AME-03.10	VUL-16	---
A42	Proxy 3	AME-03.10	VUL-16	---
A43	Proxy 5	AME-03.10	VUL-16	---
A44	Proxy 56	AME-03.10	VUL-16	---
A45	Server Red Hat 1	AME-03.10	VUL-16	---
A45	Server Red Hat 1	AME-03.10	VUL-16	---
A46	Server Red Hat 2	AME-03.10	VUL-16	---
A46	Server Red Hat 2	AME-03.10	VUL-16	---
A47	Server Red Hat 3	AME-03.10	VUL-16	---
A47	Server Red Hat 3	AME-03.10	VUL-16	---
A48	Server Red Hat 4	AME-03.10	VUL-16	---
A48	Server Red Hat 4	AME-03.10	VUL-16	---
A49	Laboratorio	AME-03.10	VUL-16	---
A49	Laboratorio	AME-03.10	VUL-16	---
A50	Sistema MITEL	AME-03.10	VUL-16	---
A50	Sistema MITEL	AME-03.10	VUL-16	---
A51	Base de Datos Hosvital	AME-04.13	VUL-15	---
A51	Base de Datos Hosvital	AME-03.10	VUL-16	---
A51	Base de Datos Hosvital	AME-03.10	VUL-16	---

COD	Activo	Amenaza	Vulnerabilidad	Control
A52	Base de Datos Sistema de Talento Humano	AME-04.13	VUL-15	---
A52	Base de Datos Sistema de Talento Humano	AME-03.10	VUL-16	---
A53	Base de Datos MSPROG	AME-04.13	VUL-15	---
A53	Base de Datos MSPROG	AME-03.10	VUL-16	---
A54	Base de Datos Sistema de Marcaciones	AME-04.13	VUL-15	---
A54	Base de Datos Sistema de Marcaciones	AME-03.10	VUL-16	---
A55	Base de Datos Laboratorio	AME-04.13	VUL-15	---
A55	Base de Datos Laboratorio	AME-03.10	VUL-16	---
A56	PC 1	AME-03.11	VUL-08	---
A56	PC 1	AME-03.10	VUL-16	---
A57	Portátil 1	AME-03.11	VUL-08	---
A57	Portátil 1	AME-03.10	VUL-16	---
A57	Portátil 1	AME-04.9	VUL-07	---
A58	Administrador de Sistema Hosvital	AME-03.12	VUL-22	---
A59	Administrador de Sistemas	AME-03.12	VUL-22	---
A60	Analista de Redes	AME-03.12	VUL-22	---
A61	Responsable de la Seguridad de la Información	AME-03.12	VUL-22	---
A62	Antivirus corporativo	AME-04.10	VUL-19	---
A63	Sistemas Operativos Windows 10	AME-03.6	VUL-13	---
A64	Equipos PC	AME-04.13	VUL-12	---
A65	Equipos PC	AME-03.11	VUL-08	---
A64	Equipos PC	AME-03.10	VUL-16	---
A65	Portátiles	AME-04.13	VUL-12	---
A65	Portátiles	AME-04.9	VUL-07	---
A65	Portátiles	AME-03.10	VUL-16	---
A65	Portátiles	AME-03.11	VUL-08	---
A66	Internet	AME-03.10	VUL-16	---
A67	Impresiones	AME-03.10	VUL-21	---
A68	Impresiones	AME-03.11	VUL-08	A15.2.1

Fuente: Autor

EVALUACIÓN DEL RIESGO

El análisis de riesgos de los activos, permite definir los controles que minimizarán el impacto y los efectos en caso de amenaza explote una o varias vulnerabilidades. (Buchtik, 2020); en la Tabla 13 se describe la ocurrencia de la amenaza junto a su valor cualitativo y cuantitativo.

Tabla 13. Probabilidad de ocurrencia de una amenaza

Por tiempo de ocurrencia	Por condición de la ocurrencia	Por el atractivo	Valor Cualitativo	Valor Cuantitativo
Una vez al año	No se identifica historial para este tipo de incidentes.	El atacante no se beneficia con el ataque.	Mínima o muy baja	1
Una vez cada seis meses	Se identifica historial de este tipo de incidentes, pero no hay incidentes registrados en la organización.	El atacante casi no se beneficia con el ataque	Potencial o Baja	2
Una vez cada tres meses	Se identifica historial de este tipo de incidentes. Se esperan posibles incidentes de forma periódica sin frecuencia.	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Creíble o Media	3
Una vez cada mes	Se identifica historial de este tipo de incidentes en la organización identificando el origen. Incidentes o eventos de esta naturaleza ocurren con frecuencia.	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Definida o Alta	4

Fuente: ISO 27001

El nivel de impacto se detalla por cada activo según la pérdida del mismo detallado en la Tabla 14 acorde a la norma ISO27001.

Tabla 14. Nivel de Impacto de una vulnerabilidad

Nivel	Descripción	Impacto	Valor
Mínima, daño inexistente	El sistema se puede recuperar inmediatamente, no hay daños ni pérdidas.	Bajo	1
Perceptible o daño bajo	La Infraestructura queda temporalmente cerrada o no puede operar; sin embargo, pueden continuar la actividad. Existe un daño limitado de activos y la mayoría de las instalaciones no se ven afectadas.	Medio	2
Grave, daño medio	La infraestructura parcialmente dañada. Algunos activos están dañados sin posibilidad de reparación, pero la instalación permanece operativa en su mayoría. Es posible que se deba mover algunos activos a otras ubicaciones10000 < valor > usd 20000.	Alto	3
Catastrófica, daño alto	Daños irreparables a la infraestructura, sin posibilidad de reparación o restauración.	Muy Alto	4

Fuente: ISO 27001

La evaluación del riesgo se calcula por cada activo tecnológico del Hospital FIB acorde a la siguiente fórmula:

$$NIVEL\ DE\ RIESGO\ = \mathrm{VA(CID)} * Ocurrencia\ Amenaza * Nivel\ de\ Vulnerabilidad$$

Criticidad del Riesgo.

La criticidad del riesgo sirve para la priorización de los mismos; en la Tabla 15 muestra los niveles de riesgos de acuerdo a la tolerancia permitida para el Hospital FIB.

Tabla 15. Evaluación del Riesgo

Nivel de Riesgo	Descripción
Muy Alto (16 – En adelante)	El riesgo es completamente inadmisible por lo que es necesario tomar medidas inmediatas para reducir o mitigar los riesgos.
Alto (10 - 15)	El riesgo es intolerable por lo que se debe tomar medidas cuanto antes.
Medio (5 - 9)	El riesgo puede ser aceptable momentáneamente sin embargo es importante considerarlo en planes de mitigación futuros.
Bajo (1 - 4)	Los riesgos son aceptables sin embargo se deben tomar medidas para reducirlos aún más o mitigarlos.

Fuente: Autor

TRATAMIENTO DEL RIESGO.

Una vez realizada la evaluación de los riesgos, se ejecuta un análisis para el tratamiento a la amenaza y que no representen un peligro para el hospital FIB. Las opciones para afrontar el riesgo son:

- Eliminar: Se consigue eliminando los activos a los que el riesgo está asociado. Se trata de una elección generalmente costosa y drástica por lo que suelen buscarse medidas alternativas.
- Transferir: Se realiza por medio de una subcontratación del servicio externamente o la contratación de un seguro que cubra los gastos en el caso de que ocurra una incidencia.
- Mitigar: acorde a la ISO/IEC 27001 consiste en elegir uno o varios de los 114 controles para combatir o disminuir el riesgo e implantar una serie de controles que actúen de salvaguarda para los activos.
- Aceptar: implica que no se van a tomar medidas de protección contra ese riesgo. La decisión debe ser tomada y firmada por la dirección de la empresa. No quiere decir que se olvide, el riesgo debe ser monitoreado para un posterior tratamiento una vez se efectivice.

La Matriz de Evaluación del riesgo de los activos del Hospital FIB se detalla en el Anexo F.

4.5. Fase IV: Declaración de Aplicabilidad

La declaración de aplicabilidad se la registra con una matriz para cada control de seguridad llenando las siguientes columnas:

- Controles Actuales (SI/NO): Describe si esta implementado algún control para el objetivo de control de esa sección; en caso de colocarle NO se justifica porque se excluye dicho control.
- Control a Implementar (SI/NO): Detalla si se va a implementar el control acorde al análisis de riesgos o alguna selección de control.

- Razones de Selección: Se coloca un X en cual quiera de las cuatro opciones en caso que se va a implementar la opción: Normas Legales (LR), Obligación Contractual (CO), Requerimientos del Negocio/ Mejores Prácticas (BR/BPRA) o Resultado de la Valoración del Riesgo (RRA).
- Plan de acción: describe una visión general de la Implementación mediante la implementación de los controles en el hospital FIB.

4.6. Fase V: Plan Director

El plan director se ha establecido agrupando por los dominios según la norma ISO27001 mediante el siguiente formato para la descripción de cada proyecto:

- Nombre de Proyecto: Describe el nombre del proyecto a implementar.
- Prioridad: Muestra la priorización del proyecto ALTA, MEDIA y BAJA.
- Presupuesto: Muestra el costo del proyecto; en caso de requerir solo personal del Hospital FIB para su ejecución se colocará en este campo **NO APLICA.**
- Objetivo: describe el objetivo del proyecto a implementar.
- Actividades: Detalla un breve cronograma a seguir del proyecto
- Beneficios: Detalla las bondades que se tendrá al implementar el proyecto.
- Activos involucrados: Describe los activos asociados a este proyecto.
- Referencias: Describe los controles asociados a este proyecto.

5. Resultados y discusión

En esta sección se describe el análisis y los resultados con base a la metodología descrita en la sección 4.1.3. para la seguridad de la información en el Hospital FIB, la cual debe garantizar la continuidad de los sistemas de información mediante políticas a difundir al personal y poder cumplir a cabalidad las siguientes fases:

- Fase I: Conocer la situación actual
- Fase II: Preparación del SGIS
- Fase III: Planificación del Plan director de seguridad
- Fase IV: Declaración de Aplicabilidad
- Fase V: Plan Director

5.1. Fase I: Conocer la Situación Actual (GAP)

El Anexo B se describe la situación inicial de los controles de seguridad del Hospital FIB según la evaluación realizada conforme al Anexo A de la ISO/IEC 27001:2017; se evidencia que la gestión de la seguridad de la información es insuficiente debido a los pocos controles de seguridad implementados y optimizados.

En la Tabla 16 se muestra el significado de cada estado con su porcentaje de cumplimiento actual para el Hospital FIB; el cual es un 43% de estado inexistente en cumplimiento de normas dentro del hospital mientras se ha cumplido solo un 4% de la norma.

Tabla 16. Estado Inicial y Cumplimiento actual Hospital FIB

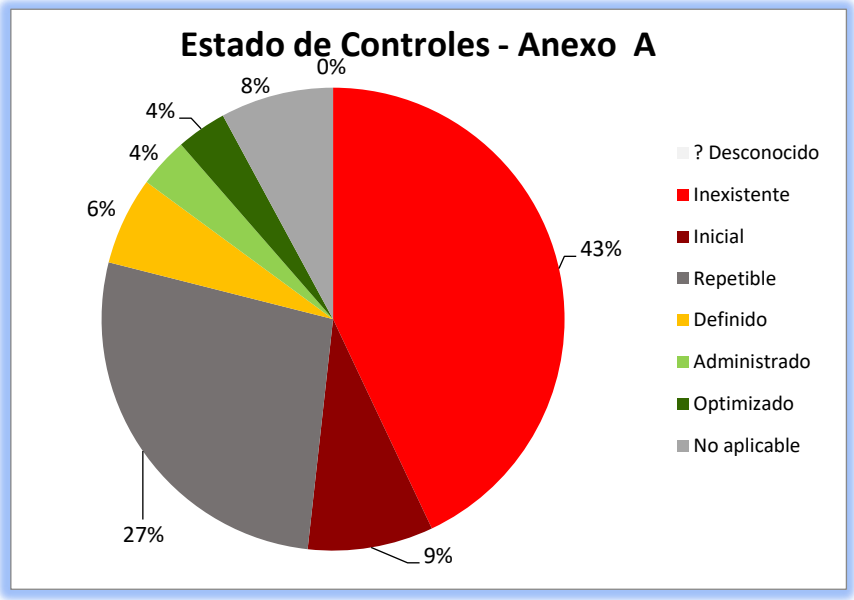
Estado	Significado	% Cumplimiento de Controles de SI
? Desconocido	No ha sido verificado	**0%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información con las políticas, controles, etc.	**43%**
Inicial	Las salvaguardas existen pero no se gestionan, no existe un proceso formal para realizarlas.	**9%**
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales).	**27%**

Estado	Significado	% Cumplimiento de Controles de SI
Definido	El control se aplica conforme a un procedimiento documentado.	**6%**
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	**4%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado.	**4%**
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios.	**8%**
Total		100%

Fuente: Autor

En la Figura 10 se muestra el resumen del estado actual de los controles a manera porcentual según los requisitos de la norma que se tiene en el Hospital FIB.

Figura 10. Estado Actual de los controles ISO 27002 del HFIB



Fuente: Autor

5.2. Fase II: Preparación del SGSI

La preparación del SGSI se cumple conforme al análisis del contexto organización del Hospital FIB acorde a la organización de la empresa, infraestructura, activos y políticas.

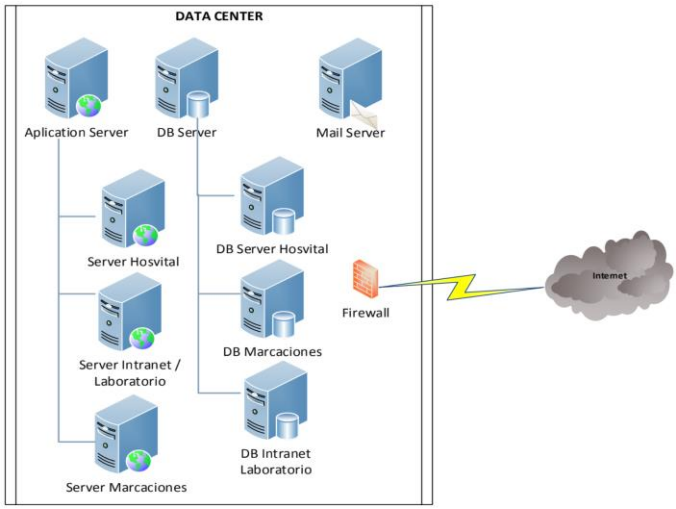
5.2.1. Analizar el Contexto Organizacional

En esta sección se analiza la infraestructura tecnológica del Hospital FIB según la infraestructura, servicios, aplicaciones y políticas.

INFRAESTRUCTURA

La infraestructura de los activos del hospital está a cargo del departamento de TIC, el cual contempla un centro de datos, servidores, dispositivos de respaldo, estaciones de trabajo y servicios que son utilizados para las operaciones diarias del hospital. En la Figura 10 se muestra la Arquitectura Física del Hospital FIB y el detalle del equipamiento junto con su ubicación se describe en la Tabla 11.

Figura 11. Arquitectura Física



Fuente: Hospital FIB

Centro de datos: El hospital FIB cuenta con dos centros de datos; uno antiguo que se encuentra en la infraestructura vieja del nosocomio y el segundo que se considera como el principal y se lo realizó con la repotenciación de las instalaciones.

El centro de datos Principal contiene tecnología CISCO y fue implementado en el año 2012. Está conformado por soportes metálicos (RACKS) que proporcionan protección y organización de los equipos que se encuentran en dicha área. En esta área se encuentra equipos como el CORE, firewall, wireless controller, switches normales como también de fibra, dos servidores cisco, un servidor que pertenece al sistema de video vigilancia, dos computadores de escritorio que funcionan como

servidores, y un UPS. Esta área cuenta con un sistema de aire acondicionado central que mantiene una temperatura ambiente de 21 grados; además, se encuentra bajo seguridades físicas debido que se considera espacio restringido y el acceso es solo para el personal del departamento TIC.

El centro de datos antiguo está conformado por dos áreas, la primera tiene racks metálicos y ahí se encuentran dos switches uno de fibra y otro ethernet, dos servidores IBM, tres computadores de escritorio que funcionan como servidores y equipos obsoletos que se encuentra apagados sin funcionar como el CORE. Esta área, también posee un sistema aire acondicionado grande y dos tipos Split que mantiene la temperatura a 21 grados. En la segunda área se encuentra una estructura tipo bunker donde se encuentra la central telefónica principal y respaldo del mismo. La temperatura se mantiene a 21 grados gracias a dos sistemas de aires acondicionado tipo Split. El acceso de ambas áreas se realiza a través de huellas digitales o por códigos de acceso.

Servidores: El hospital cuenta actualmente con cuatro servidores físicos, tres funcionales y uno que se encuentra en reparación. Estos equipos son virtuales y están ubicados en diferentes servidores (máquinas virtuales) acorde a las prestaciones tecnológicas y necesidades que tiene la institución. En la Tabla 17 se detalla los servidores virtuales creados y su descripción de uso.

Tabla 17. Descripción de servidores del HFIB

Equipamiento	Descripción
Servidor de correo electrónico	El servidor de correo Zimbra cuya versión instalada es la 8.8 del año 2017; es de indicar que previo a este correo el hospital contaba con correo electrónico Zimbra pero por inconveniente con el servidor físico donde se dañaron los servidores dejó de estar operativo y al no tener un plan de respaldo toda la información de los usuarios se perdió.
Servidor Proxy	Existe tres servidores proxy, dos servidores squid virtuales y configurados dependiendo los equipos que se estén usando; uno para los equipos de cómputo de escritorio y portátiles y el otro para configuración solo en los terminales tontos o liviano; un tercer proxy se configuro bajo tecnología en un computador des escritorio y está habilitada para área de mayor navegación en las áreas administrativas.

Equipamiento	Descripción
Servidor de Base de Datos	En el hospital existen varias bases de datos de los diferentes aplicativos que usa el hospital. Uno servidor virtual con sistema operativo centos 6 donde se encuentra instalado postgresql 8.4 con la cual se encuentra la base de datos del sistema de atención médica. En una computadora de escritorio está instalado la base de datos MySQL donde se registra las marcaciones. En un servidor virtual con la base de datos en MySQL donde se guardan los resultados de exámenes de laboratorio y en otro servidor virtual se encuentra la base de datos MariaDB donde se encuentra los registros del aplicativo de talento humano.
Servidor de cámaras IP	Servidor físico HP donde se encuentra instalado el aplicativo para la administración y grabación de video de las 209 cámaras IP de marca Bosch que tiene actualmente el hospital en funcionamiento.
Servidor Virtual de Escritorio Sistema Hosvital	Existen actualmente tres servidores virtuales con el sistema Red Hat Enterprise 8.5, que permite a la parte médica la conexión de los livianos para acceso al sistema de Hosvital.
Servidor de Aplicativos	Servidor que aloja diferentes aplicativos WEB desarrollados en el hospital, como el sistema de Talento Humano, Turnero y Laboratorio
Servidor de Reportes	Equipo de escritorio donde se encuentra instalado el sistema Jaspersoft Ireport 5.6 para extraer información del sistema Hosvital en los diferentes reportes elaborados para áreas como farmacia, admisiones y bodega de las diferentes matrices.

Fuente: Hospital FIB

Cableado Estructurado: Permite la interconexión de las diferentes áreas del hospital permitiendo la navegación web de internet, acceso a los aplicativos que maneja el hospital, a las bases de datos y demás servicios que brinda el departamento de TI.

El cableado del edificio de consulta externa y de las áreas repotenciadas se conectan a través de cable UTP categoría 6 cumpliendo normas básicas como el peinado, identificación de puntos canaletas para uso exclusivo de los cables de red. El centro de datos principal se conecta con los diferentes nodos (área nueva del Hospital) usando enlaces de fibra óptica.

Debido a que el área de hospitalización es una construcción antigua, el personal del Departamento de TI no tiene conocimiento del tipo de cableado y las normas que se usaron para su instalación.

Dispositivos de Respaldo: El hospital FIB no cuenta con dispositivos de almacenamiento de respaldo de la información, ya sea en el mismo servidor o en medios externos.

Estaciones de Trabajo: En la actualidad el hospital cuenta con tres diferentes tipos de estaciones de trabajo ubicados en los diferentes departamentos administrativos y servicios médicos y que son usados por los usuarios finales. Estos equipos se entregan a un custodio que en la mayoría de los casos es el jefe y/o responsable de los departamentos y/o servicios. En caso de computadores portátiles el custodio es directamente la persona que usa el equipo.

Actualmente no existe un procedimiento o política para la entrega de bienes tecnológicos o un inventario actualizado de los equipos entregados. En la Tabla 18 se detalla los diferentes equipos que cuenta el Hospital.

Tabla 18. Descripción de Estaciones de Trabajo del HFIB

Equipamiento	Descripción
Computadores de Escritorio	Equipos tecnológicos que están ubicados en su mayoría en la parte administrativa. Las marcas que usa el hospital son ACER, HP, además, se tiene equipos clones. El 50% de estas computadores fueron adquiridos en el año 2014; lo cual denota su obsolescencia tecnológica.
Portátiles	Se encuentran distribuidas en áreas administrativas sobre todo en las jefaturas, aunque también fueron entregados a los diferentes servicios para el uso de la parte de enfermería. La mayoría de las portátiles datan del año 2013, por lo cual su obsolescencia.
Livianos (Terminales Tontos)	Son equipos de marca Oracle Sunray 3 que permite la virtualización de escritorios. Estos equipos están distribuidos en todo el hospital tanto para la consulta externa, emergencia y hospitalización. Estos equipos son de uso exclusivos para la parte médica. Fueron adquiridos en el 2011 y hasta la presente fecha no se han adquiridos equipos más actualizados.
Impresoras	Equipos monocromáticos de dos tipos, multifuncional que son marcad LEXMARK y solo impresión que son equipos marca HP; ambas datan su fecha de adquisición del 2012 y casi un 30% del mismo se encuentra no operativo. Actualmente se tiene bajo contrato el servicio de impresión que se encarga de proporcionar de suministros e instalación de la impresora en calidad de préstamo en caso de daño de las impresoras de propiedad del hospital. Cabe mencionar que existen equipos como computadores o impresoras que son proporcionados por una empresa que brinda servicios en el área de laboratorio. Los equipos portátiles o de escritorio que son parte de algún equipo médico no se encuentra dentro del inventario del Departamento de TI.

Fuente: Hospital FIB

SERVICIOS

En la Tabla 19 se describe los servicios internos y/o externos utilizados para las actividades del Hospital FIB por los usuarios y que dan soporte el departamento TI.

Tabla 19. Descripción de Servicios del HFIB

Servicios	Descripción
Internet	Este servicio permite la navegación de los usuarios por los diferentes sitios web permitidos, el mismo que utiliza los diferentes servidores proxy para el control de accesos. Existen diferentes grupos definidos donde se otorgan los permisos de accesos como se detallan a continuación: ▪ Navegación Total: Usado para los coordinadores, jefes o responsables de área yo/servicios. Para su efecto se asigna una IP fija y no tiene control de navegación por algún proxy. ▪ Navegación Intermedia: Es de uso para la parte administrativa y para equipos de escritorio asignado en la parte médica. La IP asignada es por DHCP pero se le asigna uno del proxy habilitados. Permite navegación adicional como WhatsApp WEB. ▪ Navegación Básica: Usado solo para equipos portátiles. Está bloqueado el acceso total por medio de un proxy solo permite navegación en páginas institucionales. Si en caso una página no se encuentra habilitada y requiere el uso debe ser solicitada al responsable del área con sus respectivas justificaciones. Este procedimiento no está documentado.
Correo Electrónico	Permite el acceso al usuario a una cuenta en el correo institucional; todo empleado del hospital tiene una cuenta de correo creada donde le permite enviar y recibir mensajes ya se internos como externos con un límite de 02 MB.
Telefonía Fija	Las diferentes áreas hospitalarias están comunicadas mediante extensiones telefónicas por medio de una central telefónica IP; estas extensiones permiten llamadas a convencional o a celular sean autorizadas por la Dirección Administrativa Financiera; este procedimiento no se evidencia que se encuentra documentado.
Soporte Técnico	Este servicio brinda asistencia técnica al usuario interno del hospital en el caso que tenga algún inconveniente con un equipo (hardware) o con el uso de algún aplicativo (Software) que no permita el desarrollo normal de sus actividades. Los soportes son solicitados de manera presencial, telefónica o por correo electrónico. No se cuenta con un sistema para el registro de incidencias o documentación de los diferentes procedimientos en caso de la solicitud, ejecución y término de un soporte técnico.
Base de datos	El departamento de TI administra las diferentes bases de datos con la cual trabaja los diferentes aplicativos del hospital; se pudo evidenciar que no se cuenta con procedimiento de respaldo de dichas bases de datos.
Direccionamiento de carpetas	No se evidencia que este servicio se tenga en el hospital de manera automática o políticas de acceso para determinados archivos.
Mantenimiento de Equipo	El departamento de TIC anualmente realiza un plan para el mantenimiento de equipos tanto de escritorio como de portátiles en un periodo anual; sin embargo, no se evidencia que desde la pandemia se haya realizado. No existe procedimiento documentado para el mantenimiento de los equipos.
Impresión	Servicio de impresión es proporcionado por una empresa externa mediante el prestamos de impresoras y sus suministros, para las impresoras propiedad del FIB esta empresa proporciona los suministros como toners.

Fuente: Hospital FIB

APLICACIONES

Las aplicaciones en el hospital FIB son de tipo mixtas, algunas son para uso web o cliente-servidor; en la Tabla 20 se describe las aplicaciones que posee la institución.

Tabla 20. Descripción de las aplicaciones del Hospital FIB

Aplicaciones	Descripción
Administrativa	No se evidencia que tiene aplicaciones contables u administrativas; el departamento de contabilidad lleva sus registros en EXCEL. Los pagos y administración de nómina junto con la seguridad social se ejecutan por medio de la plataforma SPRING controlado por el Ministerio de Finanzas. Para presupuesto e inventarios están subidos a la plataforma gubernamental Sistema Integrado de Gestión Financiera (eSIGEF) quien es administrado por el Ministerio de Finanzas.
Recursos Humanos	Aplicativo web que permite el control del personal del hospital, donde se puede registrar horarios, diferentes tipos de permisos, creación y modificación de usuarios; este último punto lo realiza solo el personal de talento humano. El departamento de TI solo se encarga de la disponibilidad del aplicativo y del soporte en caso que se requiera.
Antivirus	No se evidencia que se posea un antivirus corporativo sea open o pagado en el hospital.
Cámaras IP	Permite gestionar las grabaciones de las cámaras IP instaladas en el hospital. Este aplicativo solo lo utilizan cuatro personas del departamento de TI. Para revisión de la cámara solo se lo realiza por pedido de talento humano o mediante solicitud del requirente y autorizada por la Dirección Administrativa Financiera; este procedimiento no se encuentra documentado.
SM-prog	Sistema para el registro de solicitudes para el área de mantenimiento. Es un sistema híbrido donde la parte administrativa se accede por aplicativo de escritorio y para el uso del usuario final se accede mediante aplicativo web. El departamento de TI está encargado de la creación y/o modificación de usuarios.
Visualización de Laboratorio	Aplicativo web usado para la parte médica y que sirve para la revisión de los resultados de exámenes de laboratorio. Es de libre acceso y está configurado en los equipos asignados para la atención médica. El departamento de TI se encarga de la disponibilidad del aplicativo.
Hosvital	Sistema implementado por el MSP en el año 2011 y que permite el registro del historial clínico de los pacientes atendidos tanto en consulta externa, emergencia y hospitalización; este sistema es usado también en el área de admisiones, farmacia, bodega y compras. La administración del programa está encargada del departamento de TI. Actualmente, no cuenta con soporte técnico por la empresa proveedora y su última actualización data del año 2015.

Fuente: Hospital FIB

POLÍTICAS

En el Hospital FIB han sido implementadas ciertas políticas de seguridad de manera empírica al no estar documentadas; sin embargo, se puede evidenciar que la mayoría de ellas son ejecutadas por el Departamento de TI, lo que ocasiona que el personal de la empresa sobre todo el recientemente vinculado actúen con discrecionalidad en temas de seguridad.

El personal de TI tiene conocimiento en temas de seguridad y es por ello que se han aplicado ciertas prácticas, pero debido al número reducido de técnicos de esta área y la insuficiente infraestructura no se han podido desplegar ampliamente las políticas de seguridad en los distintos departamentos dando como resultado el crecimiento de vulnerabilidades.

5.3. Fase III: Planificación del plan director de seguridad

En esta sección se detalla el análisis realizado en el Hospital FIB para los activos y su análisis de riesgo, mediante: Identificación y clasificación de activos mediante la norma ISO 27002 y la evaluación y valoración de los activos del Hospital FIB.

5.3.1. Identificación y clasificación los activos

El Hospital FIB no cuenta con un registro de los activos tecnológico por lo que se debió realizar un levantamiento de los activos de la organización mediante un inventario para posteriormente clasificarlos, evaluarlos y valorarlos.

En el anexo E se describe los activos de la organización que fueron identificados, codificados y repartidos en diferentes ubicaciones en el Hospital FIB. En la Tabla 21 se resume la clasificación de los activos agrupados acorde a su tipo en la organización y que fueron identificados.

Tabla 21. Clasificación de activos acorde al tipo

Tipo de Activo	Cantidad
Hardware	29
Información	5
Organización	2
Recursos Humanos	4
Redes	7
Software	20
Total general	**67**

Fuente: Autor

5.3.2. Evaluación y valoración de los activos

Después de la identificación de los activos, se realiza una valoración del mismo según la norma.

VALORACIÓN DE ACTIVOS

En el Anexo F se detalla la valoración del activo y su impacto en el Hospital FIB; mientras que en la Tabla 22 se detalla el promedio de la valoración del activo según su tipo.

Tabla 22. Valoración de activos

Tipo de Activo	Promedio de VA
Hardware	3,44
Información	15,47
Organización	3,33
Recursos Humanos	8,67
Redes	7,24
Software	4,03

Fuente: Autor

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES (ANÁLISIS DEL RIESGO)

Una vez realizado el análisis del riesgo realizado para cada activo, se realiza un análisis de riesgo como se muestra en la Tabla 23 agrupado por tipo de amenaza.

Tabla 23. Amenazas vs Activos – Hospital FIB

Amenazas	Cantidad	Nombre del Activo
AME-01.2	9	Core Cisco / Data Center 1 Firewall Cisco / PC / Servidor 2 Router de frontera / Servidor Cisco 1 Servidor Cisco 2 / Sistema de Video Vigilancia

Amenazas	Cantidad	Nombre del Activo
		Wireless Controller
AME-02.1	4	Data Center 2 / PC - Servidor 5 PC / Servidor 6 / PC - Servidor 7
AME-02.2	2	Data Center 1 / Data Center 2
AME-02.5	17	Core Cisco / Firewall Cisco Nodo 1 / Nodo 10 / Nodo 11 / Nodo 12 Nodo 2 / Nodo 3 / Nodo 4 / Nodo 5 Nodo 6 / Nodo 7 / Nodo 8 / Nodo 9 Router de frontera / Sistema de Video Vigilancia Wireless Controller
AME-03.1	1	Zimbra
AME-03.10	63	Base de Datos Hosvital / Base de Datos Laboratorio Base de Datos MSPROG Base de Datos Sistema de Marcaciones Base de Datos Sistema de Talento Humano Equipos PC / Impresiones Internet / Jaspersoft Laboratorio / Nodo 1 Nodo 10 / Nodo 11 Nodo 12 / Nodo 2 Nodo 3 / Nodo 4 Nodo 5 / Nodo 6 Nodo 7 / Nodo 8 / Nodo 9 PC / Servidor 1 / PC - Servidor 2 PC / Servidor 3 / PC - Servidor 4 PC / Servidor 5 / PC - Servidor 6 PC / Servidor 7 / PC 1 Portátil 1 / Portátiles Proxy 3 / Proxy 5 / Proxy 56 Server Red Hat 1 / Server Red Hat 2 Server Red Hat 3 / Server Red Hat 4 Servidor IBM M3 / Servidor IBM M4 Sistema de Marcaciones / Sistema De talento Humano Sistema Hosvital / Sistema MITEL Sistema MS-PROG / Sistema SERCOP Sistema Video vigilancia BOSCH Wireless Controller / Zimbra
AME-03.11	18	Equipos PC / Impresiones MITEL Principal / MITEL Secundario PC / Servidor 1 / PC - Servidor 2 PC / Servidor 3 / PC - Servidor 4 PC / Servidor 5 / PC - Servidor 6 PC / Servidor 7 / PC 1 Portátil 1 / Portátiles Servidor Cisco 1 / Servidor Cisco 2 Servidor IBM M3 / Servidor IBM M4
AME-03.12	4	Administrador de Sistema Hosvital Administrador de Sistemas / Analista de Redes Oficial de la Seguridad de la Información
AME-03.4	1	Sistema Hosvital
AME-03.6	2	Sistema Hosvital / Sistemas Operativos Windows 10
AME-03.7	1	Sistema Hosvital
AME-04.10	1	Antivirus corporativo

Amenazas	Cantidad	Nombre del Activo
AME-04.13	8	Base de Datos Hosvital / Base de Datos Laboratorio Base de Datos MSPROG / Base de Datos Sistema de Marcaciones / Base de Datos Sistema de Talento Humano Equipos PC / Portátiles Zimbra
AME-04.9	15	Data Center 1 / Nodo 1 Nodo 10 / Nodo 11 Nodo 12 / Nodo 2 Nodo 3 / Nodo 4 Nodo 5 / Nodo 6 Nodo 7 / Nodo 8 Nodo 9 / Portátil 1 Portátiles

Fuente: Autor

EVALUACIÓN DEL RIESGO

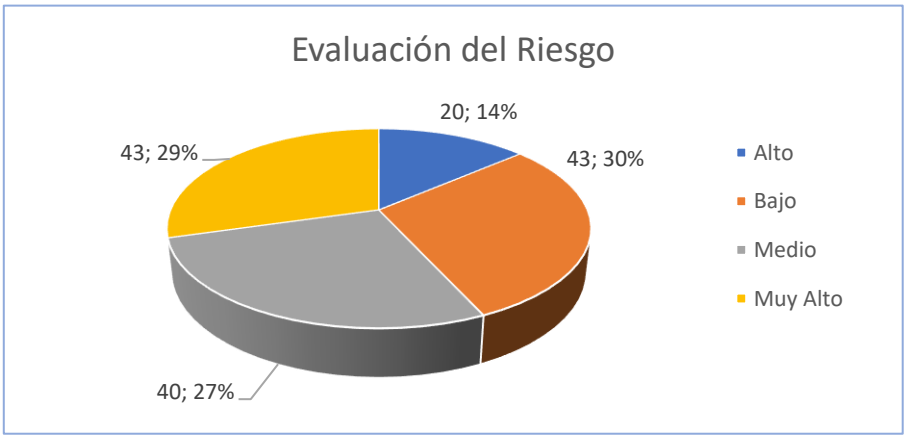
En el Anexo E se muestra el análisis de riesgo para cada activo, de los 66 activos identificados se han detectado 146 vulnerabilidades agrupadas por nivel de Riesgo. En la Tabla 24 se identificaron 43 riesgos con un nivel "Muy Alto", lo que corresponde al 30% del total analizado y se muestra en la Figura 12.

Tabla 24. Número de amenazas identificadas Hospital FIB

Nivel de Riesgo	Cantidad	% del Total
Alto	20	14%
Bajo	43	29%
Medio	40	27%
Muy Alto	43	29%
Total	146	100%

Fuente: Autor

Figura 12. Evaluación del Riesgos – Hospital FIB



Fuente: Autor

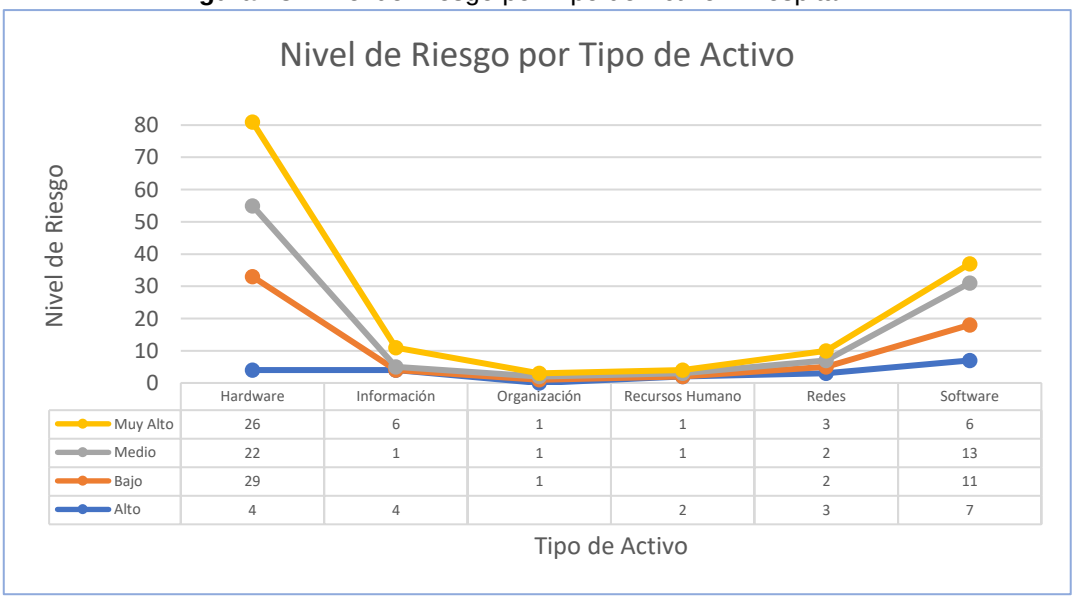
En la Tabla 25 se describe el nivel de riesgo acorde al tipo de activo identificado y en la Figura 13 se muestra de manera visual el nivel de riesgo por tipo del Hospital FIB.

Tabla 25. Nivel de Riesgo por activo – Hospital FIB

Tipo de Activos	Nivel de Riesgo				
	Bajo	Medio	Alto	Muy Alto	Total
Hardware	29	22	4	26	81
Información	--	1	4	6	11
Organización	1	1	--	1	3
Recursos Humanos	--	1	2	1	4
Redes	2	2	3	3	10
Software	11	13	7	6	37
Total	**43**	**40**	**20**	**43**	**14**

Fuente: Autor

Figura 13. Nivel de Riesgo por Tipo de Activo – Hospital FIB



Fuente: Autor

TRATAMIENTO DEL RIESGO.

En el Anexo H se describe el tratamiento a los riesgos de los activos del hospital FIB; así mismo se determina el riesgo aceptable y residual de cada uno (plan de riesgos). Los riesgos residuales aceptables en el Hospital FIB se muestran en la Figura 14; asimismo se tiene en lo Tabla 26 la clasificación del activo por tipo de riesgo.

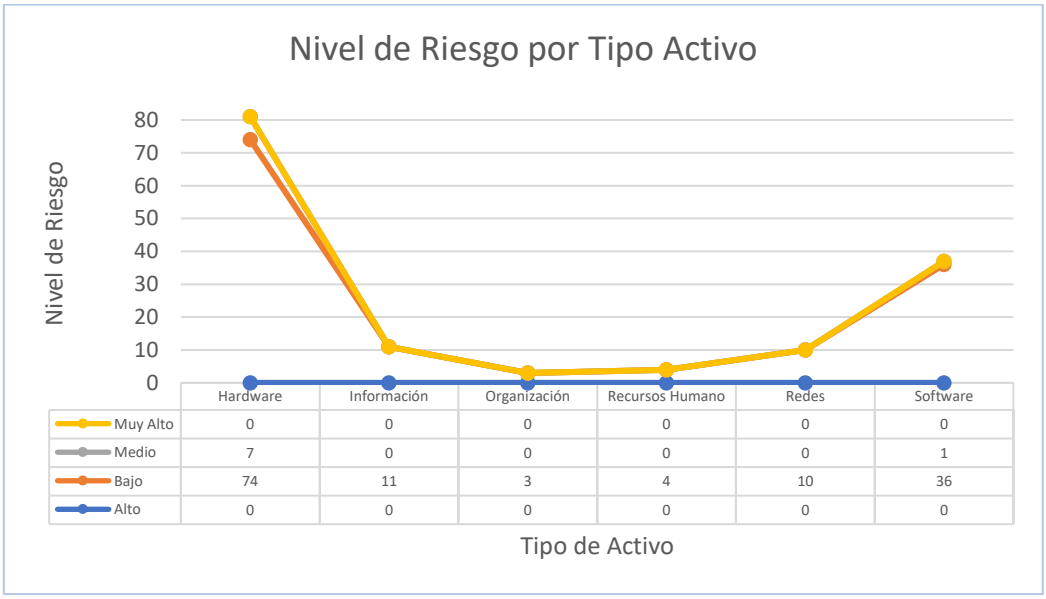
Tabla 26. Nivel de Riesgo por activo – Hospital FIB

Tipo de Activos	Nivel de Riesgo				
	Bajo	Medio	Alto	Muy Alto	Total
Hardware	74	7	--	--	81
Información	11	--	--	--	11
Organización	3	--	--	--	3
Recursos Humanos	4	---	--	--	4
Redes	10	--	--	--	10
Software	36	1	--	--	37
Total	**138**	**8**	**--**	**--**	**146**

Fuente: Autor

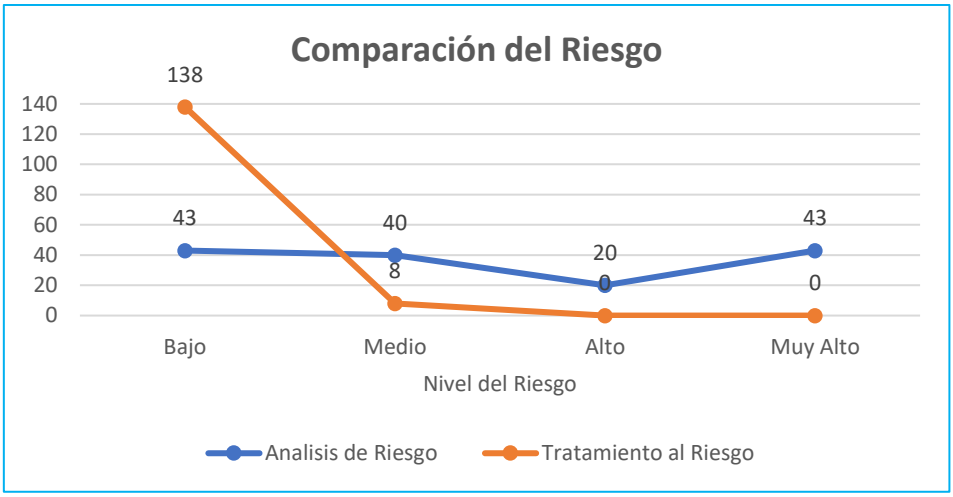
En la Figura 15 se detalla la comparación de los riesgos identificado versus los riesgos que fueron tratados y su aceptación o si es riesgo residual para el caso del Hospital FIB se tiene 32 riesgos aceptables y 113 riesgos residuales

Figura 14. Nivel de Riesgo por Tipo de Activo posterior al tratamiento – Hospital FIB



Fuente: Autor

Figura 15. Nivel de Riesgo por Tipo de Activo posterior al tratamiento – Hospital FIB



Fuente: Autor

5.4. Fase IV: Declaración de Aplicabilidad

En el Anexo G se describe la declaración de aplicabilidad del Hospital FIB y los planes acciones identificados según los 14 dominios del Anexo A de la norma ISO/IEC 27001; mientras en la Tabla 27 se detalla la comparación para el cumplimiento de los controles en la situación actual de la seguridad de la información del hospital FIB una vez implementado los controles del plan director aprobado.

Tabla 27. Nivel de Riesgo por activo – Hospital FIB

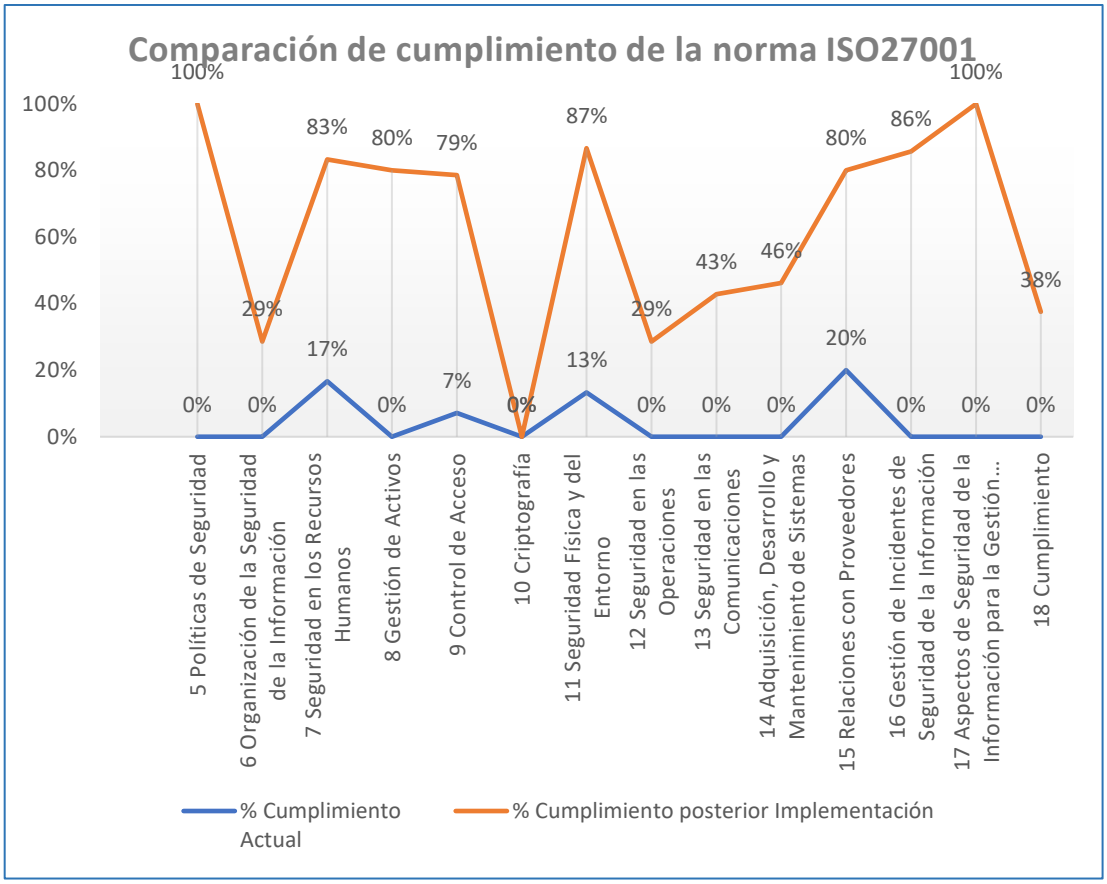
ISO 27001:2013 Controles de Seguridad	No. Control	Control actual		Proyecto asociado	Control a Implementar			% Cumplimiento actual	% Cumplimiento posterior Implementación
		Implementa	No Aplica		Aprobado	No Aprobado	No Aplica		
5 Políticas de Seguridad	2	0	0	Proyecto 1	2	0	0	0%	100%
6 Organización de la Seguridad de la Información	7	0	0	Proyecto 1 Proyecto 9	2	5	0	0%	29%
7 Seguridad en los Recursos Humanos	6	1	0	Proyecto 2	5	1	0	17%	83%
8 Gestión de Activos	10	0	0	Proyecto 3 Proyecto 9	8	2	0	0%	80%
9 Control de Acceso	14	1	0	Proyecto 4 Proyecto 6 Proyecto 8	11	3	0	7%	79%
10 Criptografía	2	0	0	---	0	2	0	0%	0%
11 Seguridad Física y del Entorno	15	2	0	Proyecto 3 Proyecto 5	13	2	0	13%	87%

ISO 27001:2013 Controles de Seguridad	No. Control	Control actual		Proyecto asociado	Control a Implementar			% Cumplimiento actual	% Cumplimiento posterior Implementación
		Implementa	No Aplica		Aprobado	No Aprobado	No Aplica		
12 Seguridad en las Operaciones	14	0	2	Proyecto 6 Proyecto 7 Proyecto 9	4	8	2	0%	29%
13 Seguridad en las Comunicaciones	7	0	0	Proyecto 6 Proyecto 8	3	4	0	0%	43%
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	13	0	6	Proyecto 6 Proyecto 11	6	1	6	0%	46%
15 Relaciones con Proveedores	5	1	1	Proyecto 11	4	0	1	20%	80%
16 Gestión de Incidentes de Seguridad de la Información	7	0	1	Proyecto 10	6	1	0	0%	86%
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	4	0	0	Proyecto 11	4	0	0	0%	100%
18 Cumplimiento	8	0	0	Proyecto 1 Proyecto 4 Proyecto 11	3	5	0	0%	38%
Total de Controles	114	5	10		71	33	10		

Fuente: Autor

En la Figura 16 se muestra el cumplimiento actual vs el cumplimiento que se tendrá posterior a desarrollado los proyectos de plan director.

Figura 16. Cuadro comparativo del cumplimiento de la norma ISO27001



Fuente: Autor

5.5. Fase V: Plan Director

Para el cumplimiento del plan director se han elaborado proyectos a ejecutar asignándoles responsable, tiempo de implementación y prioridades:

- PD-001: Políticas de Seguridad de la Información (Ver Tabla 28).
- PD-002: Seguridad en los Recursos Humanos (Ver Tabla 29).
- PD-003: Gestión de Activos Tecnológicos (Ver Tabla 30).
- PD-004: Control de Acceso y Gestión de Usuarios (Ver Tabla 31).
- PD-005: Seguridad Física y Entorno de áreas críticas (Ver Tabla 32).
- PD-006: Gestión de Software (Ver Tabla 33).
- PD-007: Copias de Seguridad (Ver Tabla 34).
- PD-008: Seguridad de redes y Comunicaciones (Ver Tabla 35)
- PD-009: Uso de dispositivos móviles y portátiles (Ver Tabla 36)
- PD-010: Gestión de incidentes (Ver Tabla 37).
- PD-011: Plan para la continuidad de la seguridad (Ver Tabla 38).

- PD-012 Gestión de Proveedores (Ver Tabla 39).

Tabla 28. Plan Director: PD-001

Nombre:	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**		
Código	PD-001	**Responsable(s):**	Oficial de la Seguridad de la Información
Prioridad:	Alta	**Presupuesto:**	No Aplica
Fecha de Inicio	jueves, 1 de junio de 2023	**Fecha Fin:**	lunes, 31 de julio de 2023
Estado:	Pendiente	**Aprobado por:**	Comité de la Seguridad de la Información.
Objetivos:	Establecer las políticas de seguridad de la información del Hospital del Niño FIB para salvaguardar los diferentes activos de la información y procesos vigentes acorde a los objetivos estratégicos.		
Detalles:	La política de seguridad es importante mediante el compromiso para la seguridad de la información, debe constar objetivos de seguridad, manual de procesos relacionados y establecidos en el SGSI para evitar la ocurrencia de una vulnerabilidad.		
Actividades:	1. Análisis de vulnerabilidades y amenazas de los riesgos asociados a la seguridad de la información. 2. Asignación de responsables de los activos de la información y de sus procesos. 3. Sociabilización a los involucrados en temas de seguridad de la información acorde a la disponibilidad, integridad y confiabilidad de la información. 4. Documentación de los temas de seguridad de la Información.		
Beneficios	1. Mejora en la seguridad de la información, sus procesos y activos. 2. Mantener la continuidad del negocio. 3. Evitar o minimizar el riesgo de los activos 4. Promover la cultura organización para la gestión de activos en la organización		
Activos Involucrados	Todos los activos identificados dentro del proceso del departamento de TIC.		
Referencia:	Norma ISO27001 - Anexo A - Dominio A5 - Objetivo de Control A5.1 Norma ISO27001 - Anexo A - Dominio A6 - Objetivo de Control A6.1 - Control 6.1.1 Norma ISO27001 - Anexo A - Dominio A18 - Objetivo de Control A18.1 - Controles A18.1.4 Norma ISO27001 - Anexo A - Dominio A18 - Objetivo de Control A18.2 - Control A18.2.2		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 29. Plan Director: PD-002

Nombre:	**SEGURIDAD DE RECURSOS HUMANOS**		
Código	PD-002	**Responsable(s):**	Unidad Administrativa de Talento Humano. Coordinador de TI
Prioridad:	Medio	**Presupuesto:**	$ 33.600,00
Fecha de Inicio	lunes, 3 de julio de 2023	**Fecha Fin:**	lunes, 4 de septiembre de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria
Objetivos:	Establecer procedimientos para la gestión de personal, su preparación y su involucración con los procesos de la seguridad de la información.		
Detalles:	Elaborar una planificación que permita capacitar a todo el personal del Hospital con temas relacionados con la seguridad de la información en fases mediante la priorización del personal acorde al rol y/o perfil que se desempeña en el hospital.		
Actividades:	1. Políticas para el uso correcto de activos de la seguridad de la información del hospital. 2. Planes de capacitación del personal para buenas prácticas y manejo de SGSI. 3. Validación de antecedentes del personal. 4. Manual de clasificación de puestos actualizado acorde a los perfiles que cumplan las condiciones relacionadas con la seguridad de la información. 5. Políticas para la vinculación y desvinculación de personal.		
Beneficios	1. Formación y concientización de los empleados del hospital. 2. Menor costos en reposición de activos de información. 3. Selección adecuada del personal a integrar en el hospital acorde a políticas.		
Activos Involucrados	A60 - Analista de Redes. A61 - Responsable de la Seguridad de la información		
Referencia:	Norma ISO27001 - Anexo A - Dominio A7 - Objetivo de Control A7.1 Norma ISO27001 - Anexo A - Dominio A7 - Objetivo de Control A7.2 - Controles A7.2.1, A7.2.2 Norma ISO27001 - Anexo A - Dominio A7 - Objetivo de Control A7.3		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 30. Plan Director: PD-003

Nombre:	**GESTIÓN DE ACTIVOS**		
Código	PD-003	**Responsable(s):**	Departamento de TI
Prioridad:	Medio	**Presupuesto:**	$ 2.500,00
Fecha de Inicio	lunes, 3 de julio de 2023	**Fecha Fin:**	lunes, 4 de septiembre de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria Directora Administrativa Financiera
Objetivos:	Crear una política para la gestión de activos tecnológicos (computadores, impresoras, teléfonos IP) para su buen uso en el Hospital.		
Detalles:	Los equipos tecnológicos son los más representativos para el departamento de TIC del Hospital FIB; por la cual se requiere la implementación de policitas y/o procesos que garanticen un buen uso del activo desde su clasificación, asignación y baja de activos; además, la designación de un custodios para cada activo.		
Actividades:	1. Inventario actualizado de activos tecnológico. 2. Política de custodio de activos. 3. Política de baja de activos. 4. Procedimiento para la disponibilidad de los activos.		
Beneficios	1. Control de activos mediante un inventario digital de activos. 2. Trazabilidad de la ubicación y uso de los activos tecnológicos. 3. Evitar daños de los equipos tecnológicos otorgados al usuario. 4. Garantizar la disponibilidad del activo de información e integridad de la información al usuario.		
Activos Involucrados	A1 - Router de frontera. A2 - Core Cisco. A3 - Firewall Cisco. A4 - Wireless Controller. A5 - Sistema de Video Vigilancia. A6 - Servidor Cisco 1. A7 - Servidor Cisco 2. A8 - Servidor IBM M3. A9 - Servidor IBM M4. A10 - PC / Servidor 1. A11 - PC / Servidor 2. A12 - PC / Servidor	A13 - PC / Servidor 4 A14 - PC / Servidor 5 A15 - PC / Servidor 6 A16 - PC / Servidor 7. A17 - MITEL Principal. A18 - MITEL Secundario. A19 - Data Center 1. A56 - PC 1. A57 - Portátil 1. A64 - Equipos PC. A65 - Portátiles	
Referencia:	Norma ISO27001 - Anexo A - Dominio A6 - Objetivo de Control A6.2. Control A6.2.1 Norma ISO27001 - Anexo A - Dominio A8 - Objetivo de Control A8.1 Norma ISO27001 - Anexo A - Dominio A11 - Objetivo de Control A.11.2 - Control A.11.2.5 al A.11.2.9 Norma ISO27001 - Anexo A - Dominio A12 - Objetivo de Control A12.2 - Controles A.12.2.5, A.12.2.7 y A.12.2.8		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 31. Plan Director: PD-004

Nombre:	**CONTROL DE ACCESO Y GESTIÓN DE USUARIOS**		
Código	PD-004	**Responsable(s):**	Departamento de TI Unidad Administrativa de Talento Humano
Prioridad:	Alta	**Presupuesto:**	No Aplica
Fecha de Inicio	lunes, 4 de septiembre de 2023	**Fecha Fin:**	viernes, 3 de noviembre de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria
Objetivos:	Elaborar procedimientos para la administración de usuarios y políticas para el control de acceso mediante perfiles asignados en los diferentes sistemas de información del hospital FIB.		
Detalles:	Determinar normativas para el control de accesos a los diferentes sistemas de información por los usuarios y restringir los accesos sin autorización y permisos requeridos mediante perfiles de usuarios, acuerdos confidencialidad y uso de medios informáticos en el hospital.		
Actividades:	1. Control de seguridad de acceso a los sistemas de información y a los activos. 2. Registro de usuarios y tiempos de accesos en el sistema 3. Políticas para gestión de usuarios y perfiles en los sistemas del Hospital. 4. Políticas de establecimiento para contraseñas 5. Monitoreo de las cuentas de usuario, grupos, permisos y perfiles que se tiene.		
Beneficios	1. Garantizar la integridad y la disponibilidad de la información. 2. Evitar que la información sensible sea divulgada o perdida. 3. Trazabilidad de los usuarios en los sistemas, permisos y accesos		
Activos Involucrados	A33 - Sistema Hosvital. A34 - Sistema De talento Humano. A35 - Sistema MS-PROG. A36 - Zimbra. A37 - Jaspersoft A38 - Sistema de Marcaciones A39 - Sistema SERCOP.	A49 - Laboratorio. A51 - Base de Datos Hosvital. A52 - Base de Datos Sistema de Talento Humano. A53 - Base de Datos MSPROG. A54 - Base de Datos Sistema de Marcaciones. A55 - Base de Datos Laboratorio.	
Referencia:	Norma ISO27001 - Anexo A - Dominio A9 - Objetivo de Control A.9.1 - Control A9.1.1 Norma ISO27001 - Anexo A - Dominio A9 - Objetivo de Control A9.2 y A9.3 Norma ISO27001 - Anexo A - Dominio A9 - Objetivo de Control A9.4 - Controles 9.4.1 al 9.4.4 Norma ISO27001 - Anexo A - Dominio A13 - Objetivo de Control A13.2 - Controles A13.2.4 Norma ISO27001 - Anexo A - Dominio A18 - Objetivo de Control A18.1 - Controles A18.1.4		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 32. Plan Director: PD-005

Nombre:	**SEGURIDAD FÍSICA Y ENTORNO DE ÁREAS CRÍTICAS**		
Código	PD-005	**Responsable(s):**	Coordinador de TI
Prioridad:	Alta	**Presupuesto:**	$ 12.500,00
Fecha de Inicio	lunes, 3 de julio de 2023	**Fecha Fin:**	viernes, 6 de octubre de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria Director Administrativo Financiero
Objetivos:	Garantizar por la seguridad física de los activos y sistemas de información en énfasis para el acceso al Data Center frente a las amenazas identificadas.		
Detalles:	Determinar los activos críticos de comunicación o de información que están expuestos a terceros mediante accesos restringido y su mal uso en el hospital.		
Actividades:	1. Control de acceso a áreas críticas de TIC mediante procedimientos definidos. 2. Instalación de biométrico para el registro y control del personal al Data Center. 3. Políticas de mantenimiento de equipos y redes. 4. Políticas de escritorio limpios y pantalla limpia		
Beneficios	1. Garantizar la disponibilidad e integridad de la información. 2. Evitar gastos por daños de los activos de la información. 3. Garantizar la disponibilidad del activo. 4. Evitar accesos no autorizados en áreas críticas.		
Activos Involucrados	A1 - Router de frontera. A2 - Core Cisco. A3 - Firewall Cisco. A4 - Wireless Controller. A5 - Sistema de Video Vigilancia. A6 - Servidor Cisco 1. A7 - Servidor Cisco 2. A11 - PC / Servidor 2. A19 - Data Center 1.		
Referencia:	Norma ISO27001 - Anexo A - Dominio A11 - Objetivo de Control A11.1 - Controles A11.1.1, A11.1.2, A11.1.4 y A11.1.6 Norma ISO27001 - Anexo A - Dominio A12 - Objetivo de Control A11.2 - Controles A11.1.1, A11.1.2, A11.1.6 y A11.1.9		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 33. Plan Director: PD-006

Nombre:	**GESTIÓN DE SOFTWARE**		
Código	PD-006	**Responsable(s):**	Departamento de TI
Prioridad:	Media	**Presupuesto:**	No Aplica
Fecha de Inicio	lunes, 3 de julio de 2023	**Fecha Fin:**	lunes, 4 de septiembre de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria Director Administrativo Financiero
Objetivos:	Elaborar procedimientos para la gestión de software de los programas de uso por el usuario interno dentro del hospital FIB.		
Detalles:	Se define en los diferentes equipos tecnológicos como computadoras y portátiles la instalación de software de uso oficial del hospital FIB; para garantizar la disponibilidad de la información.		
Actividades:	1. Gestión de usuario de los equipos tecnológicos. 2. Política de gestión para el control de acceso en los activos.		
Beneficios	1. Control de instalación de software sin autorización o pirata. 2. Disponibilidad y Confidencialidad de la Información mediante las políticas implementadas. 3. Trazabilidad del uso de software en los activos de información.		
Activos Involucrados	A33 - Sistema Hosvital. A34 - Sistema De talento Humano. A35 - Sistema MS-PROG. A36 - Zimbra. A37 - Jaspersoft. A38 - Sistema de Marcaciones. A39 - Sistema SERCOP. A49 - Laboratorio. A64 - Equipos PC. A65 - Portátiles.		
Referencia:	Norma ISO27001 - Anexo A - Dominio A9 - Objetivo de Control A9.1 - Control A9.1.1 Norma ISO27001 - Anexo A - Dominio A9 - Objetivo de Control A9.2 - Control A9.2.1 Norma ISO27001 - Anexo A - Dominio A12 - Objetivo de Control A12.6 - Controles A12.6.2 Norma ISO27001 - Anexo A - Dominio A12 - Objetivo de Control A12.7 Norma ISO27001 - Anexo A - Dominio A13 - Objetivo de Control A13.2 - Controles A13.2.4 Norma ISO27001 - Anexo A - Dominio A14 - Objetivo de Control A14.1 - Controles 14.1.1 Norma ISO27001 - Anexo A - Dominio A18 - Objetivo de Control A18.1 - Controles A18.1.4		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 34. Plan Director: PD-007

Nombre:	**COPIAS DE SEGURIDAD**		
Código	PD-007	**Responsable(s):**	Administrador de red.
Prioridad:	Media	**Presupuesto:**	$ 7.000,00
Fecha de Inicio	lunes, 1 de mayo de 2023	**Fecha Fin:**	viernes, 2 de junio de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria
Objetivos:	Definir políticas y procedimientos para la realización de copias de seguridad de los diferentes sistemas del hospital.		
Detalles:	Extraer copias integrales de todas las bases de datos de las aplicaciones que se ejecute alguna amenaza; estas copias se debe garantizar su acceso cumpliendo los protocolos de niveles de seguridad que avale su autenticación, autorización y responsabilidad.		
Actividades:	1. Políticas de respaldo de las aplicaciones. 2. Programas de restauración de las aplicaciones. 3. Plan de capacitaciones de personal. 4. Arquitectura de soporte para el almacenamiento de las copias de seguridad.		
Beneficios	1. Minimizar las pérdidas de datos sensibles como marcaciones, historial clínico, resultados de laboratorio. 2. Redundancia de datos por los respaldos 3. Garantizar la disponibilidad e integridad de la información		
Activos Involucrados	A51 - Base de Datos Postgresql para el registro de historia clínica. A52 - Base de Datos MariaDB para el registro de información de la plataforma de talento humano. A53 - Base de Datos MySQL para registro de información del sistema de mantenimiento. A54 - Base de Datos MySQL para el registro de marcaciones del personal. A55 - Base de Datos MySQL para almacenar la información de resultados de exámenes de laboratorio.		
Referencia:	Norma ISO27001 - Anexo A - Dominio A12 - Objetivo de Control A12.3		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 35. Plan Director: PD-008

Nombre:	**SEGURIDAD EN LA RED DE DATOS Y COMUNICACIONES**		
Código	PD-008	**Responsable(s):**	Administrador de red.
Prioridad:	Media	**Presupuesto:**	$ 8.900,00
Fecha de Inicio	lunes, 1 de mayo de 2023	**Fecha Fin:**	viernes, 2 de junio de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria
Objetivos:	Definir políticas para el uso y consumo de la red de datos y comunicaciones del hospital.		
Detalles:	Control y Monitoreo de la infraestructura informática de las redes de datos y comunicaciones del hospital de manera física y/o lógica y su optimización de los recursos.		
Actividades:	1. Políticas para uso de redes alámbricas e inalámbricas 2. Planificar la escalabilidad del uso de las redes. 3. Políticas para el uso de mensajería electrónica		
Beneficios	1. Optimizar los recursos de las redes y comunicaciones del hospital 2. Garantizar la disponibilidad de la información. 3. Optimizar el consumo de uso de la red.		
Activos Involucrados	A1 - Router de Frontera A2 - Core CISCO A3 - Firewall CISCO A4 - Wireless Controller		
Referencia:	Norma ISO27001 - Anexo A - Dominio A9 - Objetivo de Control A9.1. - Control 9.1.1 Norma ISO27001 - Anexo A - Dominio A13 - Objetivo de Control A13.1 - Control 13.1.1 Norma ISO27001 - Anexo A - Dominio A13 - Objetivo de Control A13.2 - Control 13.2.3		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 36. Plan Director: PD-009

Nombre:	**USO DE DISPOSITIVOS MOVILES Y PORTATILES**		
Código	PD-009	**Responsable(s):**	Oficial de la Seguridad de la información
Prioridad:	Baja	**Presupuesto:**	No Aplica
Fecha de Inicio	lunes, 1 de mayo de 2023	**Fecha Fin:**	viernes, 2 de junio de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria
Objetivos:	Establecer políticas a los usuarios para el uso correcto de los dispositivos móviles y portátiles con la finalidad de evitar el software malicioso dentro del hospital.		
Detalles:	Inducción sobre el uso de los dispositivos móviles o portables a los usuarios y cumplir con los alineamientos de la seguridad de la información.		
Actividades:	1. Políticas para uso de dispositivos móviles y portátiles. 2. Control de uso de dispositivos móviles y portátiles. 3. Campañas de concientización para el uso de estos dispositivos.		
Beneficios	1. Mitigar el riesgo de software malicioso. 2. Garantizar la disponibilidad de los dispositivos móviles y portátiles		
Activos Involucrados	A57 - Portátil 1. A65 - Portátiles.		
Referencia:	Norma ISO27001 - Anexo A - Dominio A6 - Objetivo de Control A6.2 - Control 6.2.1 Norma ISO27001 - Anexo A - Dominio A8 - Objetivo de Control A8.3 - Control 8.3.1 Norma ISO27001 - Anexo A - Dominio A12 - Objetivo de Control A12.2		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 37. Plan Director: PD-010

Nombre:	**CONTROL DE INCIDENTES**		
Código	PD-010	**Responsable(s):**	Oficial de la Seguridad de la información
Prioridad:	Baja	**Presupuesto:**	No Aplica
Fecha de Inicio	miércoles, 1 de noviembre de 2023	**Fecha Fin:**	jueves, 31 de octubre de 2024
Estado:	Pendiente	**Aprobado por:**	Comité de la Seguridad de la Información.
Objetivos:	Identificar, Analizar y Registrar los incidentes en temas de la seguridad de la información que se puedan producir futuro en el hospital FIB.		
Detalles:	Validar los inconvenientes que se presentan correspondientes en loa seguridad de la información de manera oportuna mediante el monitoreo y activación de los protocolos establecidos en el plan de continuidad de la seguridad de la información en el hospital FIB.		
Actividades:	1. Procesos establecidos en el control de incidentes. 2. Responsabilidades establecidas según el incidente. 3. Registro y documentación de los eventos de seguridad ocurrido. 4. Plan de respuestas a los incidentes de seguridad. 5. Registro de lecciones aprendidas de los incidentes de seguridad.		
Beneficios	1. Autoaprendizaje de los incidentes. 2. Optimización de tiempos de respuestas en caso de ocurrir los incidentes. 3. Garantizar la disponibilidad de la información en caso de ocurrir un incidente. 4. Gestión de Conocimiento mediante las lecciones aprendidas		
Activos Involucrados	A1 - Router de frontera. A2 - Core Cisco. A3 - Firewall Cisco. A4 - Wireless Controller. A5 - Sistema de Video Vigilancia. A6 - Servidor Cisco 1. A7 - Servidor Cisco 2. A8 - Servidor IBM M3. A9 - Servidor IBM M4. A10 - PC / Servidor 1. A11 - PC / Servidor 2. A12 - PC / Servidor 3 A13 - PC / Servidor 4 A14 - PC / Servidor 5 A15 - PC / Servidor 6	A16 - PC / Servidor 7. A17 - MITEL Principal. A18 - MITEL Secundario. A19 - Data Center 1. A19 - Data Center 1. A33 - Sistema Hosvital. A34 - Sistema De talento Humano. A35 - Sistema MS-PROG. A36 - Zimbra. A37 - Jaspersoft. A38 - Sistema de Marcaciones. A39 - Sistema SERCOP. A49 - Laboratorio. A56 - PC 1. A57 - Portátil 1. A64 - Equipos PC. A65 - Portátiles.	
Referencia:	Norma ISO27001 - Anexo A - Dominio A16 - Objetivo de Control A16.1		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 38. Plan Director: PD-011

Nombre:	**CONTROL DE INCIDENTES**		
Código	PD-011	**Responsable(s):**	Coordinador de TI
Prioridad:	Media	**Presupuesto:**	$ 7.500,00
Fecha de Inicio	lunes, 7 de agosto de 2023	**Fecha Fin:**	sábado, 7 de octubre de 2023
Estado:	Pendiente	**Aprobado por:**	Comité de la Seguridad de la Información.
Objetivos:	Desarrollar un plan de continuidad de seguridad de la información para mantener la continuidad de los procesos de la cadena de valor cuando se presente una eventualidad o incidente.		
Detalles:	Mediante un análisis de los riesgo detectados se realiza de un tratamiento al riesgo ante una amenaza y un monitoreo periódico.		
Actividades:	1. Políticas de continuidad de los procesos hospitalarios en casos de un ataque. 2. Responsabilidades establecidas para implementar la seguridad la información según el incidente. 3. Plan de capacitación del Personal del Departamento de TIC para actuar en caso de presentar un incidente. 4. Validar el plan de continuidad acorde a la ley orgánica de salud pública.		
Beneficios	1. Continuidad de los procesos hospitalarios en casos de un ataque. 2. Minimizar el impacto por la no disponibilidad e integridad de la información. 3. Evitar o minimizar las pérdidas económicas ante un acontecimiento cuando se presenta una amenaza.		
Activos Involucrados	A1 - Router de frontera. A2 - Core Cisco. A3 - Firewall Cisco. A4 - Wireless Controller. A5 - Sistema de Video Vigilancia. A6 - Servidor Cisco 1. A7 - Servidor Cisco 2. A8 - Servidor IBM M3. A9 - Servidor IBM M4. A10 - PC / Servidor 1. A11 - PC / Servidor 2. A12 - PC / Servidor 3 A13 - PC / Servidor 4 A14 - PC / Servidor 5 A15 - PC / Servidor 6 A16 - PC / Servidor 7. A17 - MITEL Principal. A18 - MITEL Secundario. A19 - Data Center 1. A33 - Sistema Hosvital. A34 - Sistema De talento Humano. A35 - Sistema MS-PROG. A36 - Zimbra. A37 - Jaspersoft. A38 - Sistema de Marcaciones. A39 - Sistema SERCOP. A49 - Laboratorio. A51 - Base de Datos Hosvital. A52 - Base de Datos Sistema de Talento Humano. A53 - Base de Datos MSPROG. A54 - Base de Datos Sistema de Marcaciones. A55 - Base de Datos Laboratorio.		
Referencia:	Norma ISO27001 - Anexo A - Dominio A17 - Objetivo de Control A17.1 y A17.2 Norma ISO27001 - Anexo A - Dominio A18 - Objetivo de Control A18.1 - Control A18.1.1.		
Propuesto por:		**Firma:**	

Fuente: Autor

Tabla 39. Plan Director: PD-012

Nombre:	**GESTIÓN DE PROVEEDORES**		
Código	PD-012	**Responsable(s):**	Coordinador de TI
Prioridad:	Media	**Presupuesto:**	No Aplica
Fecha de Inicio	lunes, 7 de agosto de 2023	**Fecha Fin:**	sábado, 7 de octubre de 2023
Estado:	Pendiente	**Aprobado por:**	Gerencia Hospitalaria.
Objetivos:	Determinar las políticas de seguridad para la gestión con los proveedores y entrega de servicios del proveedor acorde a la seguridad de la información del hospital.		
Detalles:	Análisis de las políticas para las relaciones con los proveedores para los activos de la organización y pruebas de seguridad de los aplicativos de terceros del hospital.		
Actividades:	1. Políticas de continuidad la gestión de los proveedores con respecto a los activos de la organización. 2. Determinar los cambios que se requieren los servicios del proveedor en el hospital. 3. Validar un correcto plan para la relaciones con los proveedores.		
Beneficios	1. Continuidad de los procesos hospitalarios. 2. Minimizar el impacto por la no disponibilidad e integridad de la información. 3. Mejora en la prestación de los servicios que proporcionan los proveedores para el área informática.		
Activos Involucrados	A66 - Internet. A67 - Impresiones.		
Referencia:	Norma ISO27001 - Anexo A - Dominio A14 - Objetivo de Control A14.2 - Control A14.4.8 y A14.2.9 Norma ISO27001 - Anexo A - Dominio A15 - Objetivo de Control A15.1 Norma ISO27001 - Anexo A - Dominio A15 - Objetivo de Control A18.2 - Control A18.2.1.		
Propuesto por:		**Firma:**	

Fuente: Autor

En la Tabla 40 se describe el resumen económico de cada proyecto del plan director a implementarse y su cronograma; el costo del plan director es de $ 72.000,00, esta planificación va a ejecutarse en un periodo de un año y posteriormente se realizará un análisis de GAP.

Tabla 40. Resumen del Plan Director

No.	Responsable	Fecha Inicio	Fecha Fin	Costo
PD-001	Oficial de Seguridad de la Información	1-jun-23	31-jul-23	No Aplica
PD-003	Departamento de TI	3-jul-23	4-sep-23	$ 2.500,00
PD-006	Departamento de TI	3-jul-23	4-sep-23	No Aplica
PD-010	Oficial de Seguridad de la Información	1-nov-23	31-oct-24	No Aplica
PD-011	Gestión de TIC	7-ago-23	7-oct-23	$ 7.500,00
PD-004	Departamento de TI Unidad Administrativa de DTH	4-sep-23	3-nov-23	No Aplica
PD-008	Administrador de Red	1-may-23	2-jun-23	$ 8.900,00
PD-012	Coordinador de TI	7-ago-23	7-oct-23	No Aplica

No.	Responsable	Fecha Inicio	Fecha Fin	Costo
PD-007	Administrador de Red	1-may-23	2-jun-23	$ 7.000,00
PD-005	Coordinador de TI	3-jul-23	6-oct-23	$ 12.500,00
PD-002	Unidad Administrativa de DTH Coordinador de TI	3-jul-23	4-sep-23	$ 33.600,00
PD-009	Responsable de la Seguridad de la Información	1-may-23	2-jun-23	No Aplica
			Total	**$72.000,00**

Fuente: Autor

6. Conclusiones y Recomendaciones

6.1. Conclusiones:

El análisis de situación inicial realizado en el hospital FIB se evidenció graves deficiencias en la seguridad de la información debido a la carencia de políticas y procedimientos establecidos; incluyendo el desconocimiento del personal en cuanto al manejo de los activos de la información.

La implementación del plan director permitirá un importante incremento de aplicación de los controles de seguridad de la información de 5 a 75, lo que implicaría un cumplimiento del 66% en la aplicación de la norma ISO 27000 en el Hospital FIB

Las políticas de seguridad de la información y sus respectivos controles son esenciales en un plan de mejora en el hospital FIB, con la finalidad de garantizar la continuidad del negocio permitiendo un bajo impacto de las amenazas y un manejo eficiente de incidentes de seguridad mediante la implementación de doce proyectos en un periodo de un año donde se realizará una organización a nivel de gestión de activos y de personal en el hospital.

6.2. Recomendaciones:

- Se sugiere identificar y definir los propietarios de los activos de la información identificados para una aplicación de las respectivas políticas de seguridad garantizando su aplicación y gestión.
- Se recomienda establecer procedimientos planificados para el control y/o monitoreo de los riesgos de los activos, además, de la actualización permanente de su análisis para asegurar la mejora continua en el hospital.
- Es importante sociabilizar y capacitar el plan de seguridad periódicamente al personal de las diferentes áreas y al nuevo personal que ingrese al hospital FIB para concientizar la gestión de activos y cumplimiento de políticas de la seguridad de la información establecidas.
- Es necesario reforzar el Departamento de TI del Hospital FIB con la vinculación de personal especializado en seguridad de información y plan de capacitación al personal actual con el objetivo de afrontar los retos que demandan los procesos de la seguridad de la información en implementación.

REFERENCIAS

27002:2013, I. (2013). Anexo A Normativo Objetivos de control. Madrid, España.

AENOR. (2014). *NORMA ISO 27001 SGSI.* España.

Alonso, C. (03 de 08 de 2015). *GlobalSuite Solutions*. (ISO 27000 y el conjunto de estándares de Seguridad de la Información) Obtenido de https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Alvarado, C. (26 de 03 de 2021). *Pensemos, Software de Gestión Estratégica*. (Sistema de gestión de seguridad de la información: qué es y sus etapas) Obtenido de https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Amazon . (s.f.). (Libri Mundi) Obtenido de https://books.google.com.ec/books?id=Z0kx76jf88wC&pg=PA89&dq=tipos+de+investigaci%C3%B3n+investigacion+descriptiva&hl=es-419&sa=X&ved=2ahUKEwig0I_L0r37AhWBQzABHa92CikQ6AF6BAgLEAI#v=onepage&q=tipos%20de%20investigaci%C3%B3n%20investigacion%20descriptiv

Buchtik, L. (2020). *Gestion de Riesgos.* Uruguay.

Ciberseguridad, I. N. (s.f.). *INCIBE.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

comercio, E. (2022). *www.elcomercio.com.ec*.

CORRECTA - Ciberseguridad | Robotización | Sales Automation | Social Listening. (02 de 02 de 2021). (Plan Director de Seguridad: qué es y por qué lo necesitas en tu empresa) Obtenido de https://www.correcta.es/que-es-un-plan-director-de-seguridad/

Ecuador, G. d. (05 de 2021). *LEY ORGANIZA DE DAOS PERONALES*. Obtenido de www.telecomunicaciones.gob.ec

El Comercio. (29 de Abril de 2022). (Las alertas de ciberataques aumentan) Obtenido de https://www.elcomercio.com/actualidad/seguridad/alertas-ciberataques-aumentan-gobierno-ministerios.html

ESAN. (2016). *Beneficios de un SGSI*. Obtenido de https://www.esan.edu.pe/conexion-esan/importancia-y-beneficios-de-contar-con-un-sistema-de-gestion-de-seguridad-de-informacion

Estado, C. G. (2021). *DPGY-0030-2022.* Guayaquil.

FIB, H. (s.f.). Obtenido de ttps://www.salud.gob.ec/hospital-del-nino-dr-francisco-de-ycaza-primer-hospital-publico-con-acreditacion-internacional/

GMS . (s.f.). (ISO 27001-2013 - GMS Seguridad de la Información) Obtenido de Seguridad de la Información: https://gmsseguridad.com/iso-27001-2013/

HFIB. (2012). Obtenido de www.hfib.gob.ec

HFIB. (2017). Obtenido de Plan Estratégico del HFIB.

HODEGHATTA. (2014). *Introduccion a la Seguridad de la Informacion Handbook.* NY: Apress Media.

ISO. (2015). *Gestion de Activos*. Obtenido de NORMA ISO 27001: https://normaiso27001.es/a8-gestion-de-activos/

ISO27000. (s.f.). (SGSI) Obtenido de https://www.iso27000.es/sgsi.html

Mundi, L. (s.f.). *Amazon*. Obtenido de Metodolgia de la investigacion: https://books.google.com.ec/books?id=h4X_eFai59oC&pg=PA175&dq=recoleccion+de+informacion+fuentes+primarias+y+secundarias&hl=es-419&sa=X&ved=2ahUKEwjEyub1y737AhVJSTABHUncB9UQ6AF6BAgFEAI#v=onepage&q=recoleccion%20de%20informacion%20fuentes%20primarias%2

Mundi, L. (s.f.). *Amazon* . Obtenido de Metodologia de Investigacion: https://books.google.com.ec/books?id=Z0kx76jf88wC&pg=PA89&dq=tipos+de+investigaci%C3%B3n+investigacion+descriptiva&hl=es-419&sa=X&ved=2ahUKEwig0I_L0r37AhWBQzABHa92CikQ6AF6BAgLEAI#v=onepage&q=tipos%20de%20investigaci%C3%B3n%20investigacion%20descriptiv

NORMA ISO27001. (2021). Obtenido de Analisis de Brechas GAP en ISO 27001: https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/#

PMG SSI - ISO 27001. (8 de 4 de 2021). (Fases de implementación de un Plan Director de Seguridad) Obtenido de https://www.pmg-ssi.com/2022/06/fases-de-implementacion-de-un-plan-director-de-seguridad/

ANEXOS

Anexo A: Estructura Orgánica del Hospital FIB.

Anexo B: Estado Inicial de los Controles de Seguridad.

Anexo C: Identificación y Clasificación de activos.

Anexo D: Valoración de los activos.

Anexo E: Evaluación del Riesgo

Anexo F: Tratamiento al Riesgo

Anexo G: Declaración de Aplicabilidad

Anexo A: Estructura Orgánica del Hospital FIB.

ANEXO B: ESTADO INICIAL DE LOS CONTROLES DE SEGURIDAD.

La norma ISO/IEC 27001 describe Anexo A a manera de cuestionario para los controles, objetivos de control y dominios (27002:2013, 2013).

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A5	**Políticas de seguridad de la información**			
A5.1	**Directrices de gestión de la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	Inexistente	**¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada?** Se tiene un marco de la estructura; sin embargo no existen políticas de la seguridad de la información dentro del departamento de TIC. **¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes?** No existen políticas o análisis de riesgos de Seguridad. **¿Cómo se autorizan, comunican, comprenden y aceptan las políticas?** No hay proceso definido **¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores?** No existe documentación formal donde los trabajadores firmen para el compromiso sobre la seguridad de la información. **¿Hay acuerdos adecuados de cumplimiento y refuerzo?** No existe documentación que avale el compromiso o compromiso del empleado. **¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)?** No, incluso cuando se presenta alguna necesidad. El personal de TIC busca la mejor solución para resolver completamente o paliativamente alguna novedad. **¿Están las políticas bien escritas, legible, razonable y viable?** Al no tener políticas establecidas no existe documentación sobre las mismas para su verificación **¿Incorporan controles adecuados y suficientes?** No existen controles, ni tampoco se tiene documentado los riesgos y amenazas de sus activos	El departamento de TIC no cuenta con los procedimientos o directrices para la gestión de seguridad de la información.

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
			¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.? No hay cobertura de ningún activo **Cuán madura es la organización en esta área?** Todas las decisiones respecto al tema de seguridad de la información se lo hace de manera empírica y solo se actúa cuando se presenta algún inconveniente.	
A5.1.2	Revisión de las políticas para la seguridad de la información	Inexistente	**¿Todas las políticas tienen un formato y estilo consistentes?** No existe documentación física de algún formato; además que no están implementado ninguna política de seguridad de la información. **¿Están todos al día, habiendo completado todas las revisiones debidas?** No **¿Se han vuelto a autorizar y se han distribuido?** Al no existir políticas de la seguridad de la información, no existe un proceso claro de autorización o distribución de las políticas de seguridad.	No existe documentación de política en tema de seguridad de la información.
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Roles y responsabilidades en seguridad de la información	Repetible	**¿Se le da suficiente énfasis a la seguridad y al riesgo de la información?** No, ni por parte de la gerencia como tampoco por el departamento de TIC. **¿Hay apoyo de la administración?** No. Al ser un hospital público se enfocan más en las necesidades del paciente. **¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad?** No. Existe poco interés debido que por la naturaleza de la Institución, se enfocan más por el bienestar de los pacientes que son los objetivos institucionales. **¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas?** Organizacionalmente la responsabilidad de la seguridad de la información recae sobre el área de tecnología; sin embargo, no se tiene asignado responsabilidades dentro del personal del área respecto a la seguridad de la información.	La responsabilidad sobre la seguridad de la información recae en el departamento de TIC. Existe poco interés de las autoridades sobre los riesgos y el impacto en la seguridad de la información y la asignación de un responsable para dichas funciones.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información? Existe una asignación de responsabilidades a las actividades correspondiente de TIC sin incluir la seguridad de la información de una manera no formal. No existe documentación de la descripción y asignación de roles y responsabilidades. **¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información?** Por ser un ente público donde no existe ingresos y el estado asigna partidas presupuestarias anuales, la asignación de presupuesto al departamento de TIC es mínima para poder efectuar la compra de partes y piezas de equipos tecnológicos y la contratación de ciertos servicios como impresora o mantenimiento de servidores. **¿Hay coordinación dentro de la organización entre las unidades de negocio?** La comunicación en ocasiones no es eficientes y en muchas ocasiones la coordinación de los demás departamento con el departamento de TIC para la ejecución de tareas, proceso o proyectos. **¿funciona efectivamente en la práctica?** No **¿Existe una conciencia y un apoyo adecuados para la estructura de riesgo y seguridad de la información?** No existe conciencia del impacto a la seguridad de la información dentro de la institución por parte de las máximas autoridades.	
A6.1.2	Segregación de tareas	Repetible	**¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas?** Los deberes y funciones están establecidos en el manual de clasificación de puesto del MSP y es con la cual el departamento de recursos humanos se guía para la asignación de puestos. En el organigrama del departamento de TIC existe un coordinador y actualmente 3 personas con los perfiles de analista de soporte técnico (1) y Asistente de Soporte Técnico (2), a pesar de estar definido en la parte informática las responsabilidades; ninguno asume la seguridad. **¿Existe una política que cubra la segregación de deberes?** No existe una política de segregación de tareas debido que en el departamento la mayoría son para soporte técnico, no existe un encargado de infraestructura	No existe documentación sobre la política de seguridad y tampoco sobre la asignación de roles y en énfasis a la seguridad de la información.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea? **Responsable | Accountable | Consulted | Informed** Las actividades están definidas según el manual de clasificación de puesto del MSP, pero no existe un documento claro donde se defina las responsabilidades de la seguridad de la información. **¿Cómo llegan las decisiones con respecto a tal segregación?** Las tareas son asignadas por el coordinador y lo asignan dependiendo de las funciones, competencias o conocimientos. **¿Quién tiene la autoridad para tomar tales decisiones?** El coordinador del departamento de TIC toma la mejor solución previo consenso en base a las opiniones de todo el personal del departamento de TIC. **¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?** No existe registro de incidencias. En su mayoría los soportes son esporádicos y en algunas veces se asignan tareas mediante el portal QUIPUX con tiempo de ejecución.	
A6.1.3	Contacto con las autoridades	Definido	**¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias?** Dentro del Hospital se tiene un listado de contacto de las autoridades y todos los responsables de área en caso de inconvenientes. En caso de empresas que estén prestando servicios es el responsable de la orden del servicio, que en su mayoría en un personal del departamento de TIC o el coordinador del área posee los contactos para cualquier soporte técnico. Los números de contacto se encuentran actualizados según como exista una modificación en el organigrama. No se cuenta con un proceso periódico de verificación. **¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo?** Por jerarquía, el coordinador del departamento de TIC es quien se comunica con las máximas autoridades al presentar cualquier inconveniente. **¿La lista es actual y correcta?** Si **¿Hay un proceso de mantenimiento?** Los números de contacto se encuentran actualizados según como exista una modificación en el organigrama. No se cuenta con un proceso periódico de verificación.	Se encuentra establecido los pasos a seguir en caso de un incidente, pero no se cuenta con un listado de los contactos actualizado. La mayoría se lo realiza mediante llamada directa o por mensaje de aplicativos.

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A6.1.4	Contacto con grupos de interés especial	Repetible	**¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k?** No existe grupos o contacto regular en cuanto a la seguridad de la información; se procede a la búsqueda de información en noticias a través de la web o en foros públicos. **¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?** No, si se presenta algún inconveniente siempre se encuentra una solución de manera interna; de igual manera no existe muchos eventos de seguridad que se pueda compartir o implementados.	El departamento se encuentra actualizado en temas de seguridad de la información por medio noticias o lectura; sin embargo, al momento de presentar algún evento se vale de las ideas del personal para su resolución.
A6.1.5	Seguridad de la información en la gestión de proyectos	Inexistente	**¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes?** No. Cualquier proyecto informático no van de la mano con los de seguridad, solo buscan implementar la funcionalidad del proyecto . **¿La etapa del proyecto incluye actividades apropiadas?** No se determinan las etapas para el cumplimiento adecuado.	Para la ejecución de un proyecto, en su mayoría; no se encuentran considerados los aspectos de seguridad para nuevos proyectos.
A6.2	**Los dispositivos móviles y el teletrabajo**			
A6.2.1	Política de dispositivos móviles	Inexistente	**¿Existen política y controles seguridad relacionados con los usuarios móviles?** No. Actualmente no existe alguna política de seguridad para todos los dispositivos móviles. **¿Se distinguen los dispositivos personales de los empresariales?** No. En algunas áreas existen personal que usa equipos portátiles personales debido a la brecha tecnológica que existe. **¿Cómo se mantienen y controlan los sistemas portátiles para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad?** Las portátiles personales no entran a revisión por no estar dentro del inventario.	No existe políticas

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco? No se emplea ninguna tipo de gestión tanto MDM o MAM. No tienen conocimiento el área de TIC sobre dichas terminologías. Los equipos portables tiene usuarios permisos administrador lo cual permite la instalación de cualquier aplicativo.	
A6.2.2	Teletrabajo	Repetible	**¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina?** No se usa teletrabajo. El coordinador y otro personal del área acceden remotamente solo para revisión de emergencia fuera del horario laboral por medio del aplicativo anydesk. **¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Always-on-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio?** No se cuenta con una VPN para los usuarios del hospital; sin embargo solo dos personas acceden remotamente mediante Anydesk con contraseña de acceso; a sus máquinas asignadas en el área y de ahí pueden revisar todo lo correspondiente a los servidores y sistemas que existen.	En el hospital no existe el teletrabajo. El acceso remoto en caso de presentar inconvenientes es de responsabilidad de dos personas del departamento de TI.
A7	**Seguridad relativa a los recursos humanos**			
A7.1	**Antes del empleo**			
F	Investigación de antecedentes	Optimizado	**¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo?** Si. Se rige según las normativas establecido por el ministerio de trabajo. **¿Se hace en la empresa o se subcontrata a un tercero?** Se lo realiza en la misma empresa. **Si se subcontrata a un tercero, ¿Se han revisado sus procesos y se han considerado aceptables?** No aplica por hacerlo dentro de la institución. **¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección?** Si, se pide certificado de no impedimento para trabajar en sectores público, asi como también el de no tener antecedentes penales.	procesos de contratación de personal nuevo acorde a lo indicado el ministerio de trabajo y las leyes vigentes.

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
			¿Existen procesos de selección mejorados para los trabajadores en roles críticos? No existen roles críticos. **¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?** Si. El proceso de selección se basa según el manual interno de talento humano y en las regulaciones vigentes del ministerio de trabajo.	
A7.1.2	Términos y condiciones de empleo	Administrado	**¿Están claramente definidos los términos y condiciones de empleo?** Todo está definido en el manual de clasificación de puestos del MSP. **¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general?** Si, excepto en temas de seguridad de la información. **¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles?** No. En el manual de clasificación de puestos no existe asignación en lo que compete a la seguridad de la información. **¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?** No, debido a que no se tiene políticas de seguridad de la información.	Se tiene un manual de clasificación de puestos por el MSP, sin embargo, en su mayoría no se tiene asignación de roles en temas de seguridad de la información
A7.2	**Durante el empleo**			
A7.2.1	Responsabilidades de gestión	Inexistente	**¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia?** No existe un plan de concientización a nivel de seguridad. **¿Se hace de forma regular y está a día?** Nunca se lo ha realizado. **¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados?** No existe documentación o formato para este tipo de actividades. **¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?** No. No existe este tema en la organización	No se entrega o capacita al personal sobre la seguridad o sociabilización de programas de seguridad.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad? No existe interés de las máximas autoridades. Además, como no existe un rol de seguridad de la información y delegan directamente como responsabilidad al departamento de tecnología.	
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inexistente	**¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente?** El personal de TIC no cuenta con seguridad de la información como prioridad, por ende no se preocupa del mantenimiento, actualización de hardware o software, así como preparándose y/o actualización de conocimiento. **¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos?** No existe comunicación para la difusión de la seguridad de la información para los usuarios. **¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos?** Si. **¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas?** No existe documento donde se actualice lo indicado. Tampoco existe capacitaciones. **¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento?** No existe o cursos u capacitaciones correspondiente en lo que compete a tecnología. **¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?** No existe seguimiento para este tópico.	El personal del departamento de TIC, no está consiente sobre los temas de Seguridad de la Información; así como los demás empleados.
A7.2.3	Proceso disciplinario	Inexistente	**¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores?** Hasta la presente, no existe un evento importante que represente alguna infracción de seguridad de la información; el departamento hasta la presente fecha no hay un registro de incidentes o un régimen disciplinario en cuanto a incidentes de la seguridad de la información.	Aunque no ha existe casos de vulnerabilidades a nivel de seguridad de la información.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Cómo se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos? No se evidencia de sanciones emitidas por faltas cometidas en relación a la seguridad de la información. **¿Está esto cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo?** No **¿Se actualiza el proceso de forma regular?** No existe sanciones.	No se contempla un procedimiento de sanciones en caso de faltas cometidas por el personal en temas de seguridad de la información.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**			
A7.3.1	Responsabilidades ante la finalización o cambio	Repetible	**¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización?** Existe procedimientos parciales pero nada establecido por escrito. **¿Se tienen en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos?** Si **¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?** Si	Existen procedimientos establecidos de manera empírica o macro por el ministerio de trabajo.
A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.1	Inventario de activos	Repetible	**¿Hay un inventario de activos de la información?** Sí, pero solo de portátiles, ordenadores de escritorio e impresoras. El inventario actualmente no se encuentra actualizado ni completo. **¿Contiene la siguiente información?** • Datos digitales: Si • Información impresa: No. • Software: No • Infraestructura: Si • Servicios de información y proveedores de servicios: No • Seguridad física: No • Relaciones comerciales: No	El inventario de activos existe; sin embargo, no está actualizado y su comprobación está a voluntad.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			• Las personas. Todos los equipos tecnológicos están bajo custodia el responsable de cada área y/o servicio, debido que algunos equipos son usados por más de dos personas. Solo las portátiles se le asignan custodia personal. **¿A quién pertenece el inventario?** El departamento de TIC cuenta con su propio inventario, muy aparte de lo realizado por el área de activo fijo y bodega. **¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI?** Se trata de lo posible actualizar la información del equipo cuando existe un cambio solicitado por el área de talento humano.	
A8.1.2	Propiedad de los activos	Repetible	**¿Los activos tienen propietario de riesgo?** Todos los equipos críticos como servidores y/o switch que se encuentra en el data center, bunquer o nodos de distribución y que están a cargo por la coordinación de TI. **¿Los activos tienen responsable técnico?** Si. Existe un responsable de inventario dentro del departamento de TIC que se encarga de su asignación para la revisión técnica y/o mantenimiento. Toda revisión que requiera mover un equipo al área de TIC se solicita al jefe de área que envié una solicitud mediante quipux. **¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos?** Todos los equipos críticos están a cargo del coordinador de TIC. **¿Cómo se etiquetan los activos?** Se trata de etiquetar con un código establecido por el área de TIC. **¿Cómo se informa ante incidentes de seguridad de la información que los afectan?** Como hasta la presente fecha no ha existido incidentes con respecto a la seguridad de la información, no se tiene un proceso en referencia para información de incidentes.	Se tiene establecido la custodia de los equipos sin embargo, no existe documentación que la avale o procedimiento. La identificación de los equipos se lo hace de manera empírica y es realizada por el personal encargado.
A8.1.3	Uso aceptable de los activos	Inexistente	**¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.?** No existe ninguna política sobre el uso de los diferentes recursos o herramientas tecnológicas. **¿Cubre el comportamiento del usuario en Internet y en las redes sociales?** No.	No existe política establecida sobre la responsabilidad del activo bajo su cargo.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se permite el uso personal de los activos de la empresa? No existe lineamientos que deben seguir los usuarios sobre todo para equipos portátiles. **En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto?** No existe control para este tema. **En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto?** No existe control para este tema. **¿Se describe de forma explícita lo que constituye un uso inapropiado?** No existe documentación alguna. **¿Se distribuye esta información a toda la empresa?** No existe documentación para distribución. **¿El uso de la criptografía cumple con todas las leyes, acuerdos / contratos y normativas relevantes?** No.	No existe política establecida y en conocimiento del personal interno sobre la responsabilidad del activo bajo su cargo.
A8.1.4	Devolución de activos	Repetible	**¿Existe un procedimiento para recuperar los activos tras una baja o despido?** No existe un procedimiento escrito; ante la salida del personal es el área de activo fijo quien se encarga de verificación de asignación de activo al usuario. **¿Es un procedimiento automatizado o manual?** Manual. **Si es manual, ¿Cómo se garantiza que no haya desvíos?** Se firmas actas de retiro por parte del área de activo fijo. **¿Cómo se abordan los casos en los que los activos no han sido devueltos?** Se procede al respectivo informe técnico para que el personal saliente cubra los valores monetarios según el valor referencial registrado por el área de activo fijo.	Existe un procedimiento a través del llenado de un documento llamado paz y salvo; sin embargo, no existe documentación donde avale la realización de informe técnico en caso de pérdida de equipo.
A8.2	**Clasificación de la información**			
A8.2.1	Clasificación de la información	Inexistente	**¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información?** No existe procedimiento o estándares respecto a la clasificación de la información. **¿La clasificación es impulsada por obligaciones legales o contractuales?** Legal **¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad?** No **¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen?** No	No se pudo evidenciar documentos de políticas o estándares para clasificación

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados? No	
A8.2.2	Etiquetado de la información	Inexistente	**¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica?** No **¿Está sincronizado con la política de clasificación de la información?** No existe política de clasificación. **¿Cómo se garantiza el correcto etiquetado?** No hay garantías. **¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante?** por intermedio de medios informáticos. **¿Cómo se garantiza que no haya acceso no autorizado?** Asignación de roles y parametrización de permisos en los usuarios de los diferentes aplicativos. **¿Se revisan los niveles de clasificación en intervalos predefinidos?** No	No existe actualmente política de etiquetado de información.
A8.2.3	Manipulado de la información	Inexistente	Más allá de A.8.2.1 **¿Están los niveles de clasificación adecuadamente asignados a los activos?** No **¿Se considera los gimiente?** No **Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc.** No hay método establecido para cumplir con esta actividad	No existe método o política establecida en temas de manipulación de información.
A8.3	**Manipulación de los soportes**			
A8.3.1	Gestión de soportes extraíbles	Inexistente	**¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles?** No. **¿Los medios extraíbles están debidamente etiquetados y clasificados?** No **¿Los medios se mantienen y almacenan de forma adecuada?** Si. Se almacena según el motivo y el bien clasificado. **¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?** No hay controles implementados para la confidencialidad de los datos.	No existen controles para los soportes extraíbles

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A8.3.2	Eliminación de soportes	Repetible	Más allá de A.8.3.1 **¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios?** No existe política. **¿Se documenta la aprobación en cada etapa para la eliminación de los medios?** No existe documentación. **¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación?** Si. **¿Se tiene en cuenta los periodos de retención?** Si **¿Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)?** No existe la implementación de tipos de eliminación de forma segura dentro del hospital.	No existe políticas o procedimientos actualmente para la eliminación de medios extraíbles; sin embargo, se lo ejecuta de forma empírica.
A8.3.3	Soportes físicos en tránsito	Definido	**¿Se utiliza un transporte o servicio de mensajería confiable?** Solo para mensajería externa. **¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia?** No **¿Se verifica la recepción por el destino?** Firma de recepción de la empresa externa.	Existe procesos de soportes en tránsito para envío de información.
A9	**Control de acceso**			
A9.1	**Requisitos de negocio para el control de acceso**			
A9.1.1	Política de control de acceso	Repetible	**¿Existe una política de control de acceso?** No existe política de control de acceso al igual que para uso de aplicativos se ingresa mediante usuario y clave. **¿Es consistente con la política de clasificación?** No existe política de clasificación. **¿Hay una segregación de deberes apropiada?** Si. Depende de cada departamento. **¿Existe un proceso documentado de aprobación de acceso?** Existe un proceso donde interviene recursos humanos, y las jefatura de cada área pero no está documentados. **¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?** Departamento de TIC, coordinadores de área y recursos humanos.	Procedimiento para el control de acceso establecido; pero no se encuentra documentado. El personal de TIC ejecuta el control de acceso a los servicios de manera empírica o determina acorde a las necesidades.

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A9.1.2	Acceso a las redes y a los servicios de red	Inexistente	**¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado?** No existe control de acceso a VPN e inalámbricas. **¿Se utiliza autenticación de múltiples-factores para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados?** No. Acceden remotamente a través de anydesk solo dos personas de TIC. **¿Cómo monitoriza la red para detectar acceso no autorizado?** No existe monitoreo. **¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)?**No **¿La organización mide la identificación y los tiempos de respuesta ante incidentes?** No se tiene definido.	No existe actualmente política de sobre el acceso a la red hospitalaria; asimismo el personal es evaluado sobre seguridad de la red (Pentesting.)
A9.2	**Gestión de acceso de usuario**			
A9.2.1	Registro y baja de usuario	Optimizado	**¿Se utiliza un ID de usuario únicos para cada usuario?** Se trabaja con el número de cédula excepto para los correos electrónicos. **¿Se genera en función a una solicitud con aprobaciones y registros apropiados?** Si **¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido?** Se lo realiza a través de un comunicado emitido por talento humano. **¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos?** Si **¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes?** Si. Lo realiza talento humano y es remitido una copia de los resultados. **¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios?** Si. **¿Qué impide que los ID de usuario sean reasignados a otros usuarios?** Debido que el número de cédula de identidad, es un identificador único.	Existe un procedimiento establecido por el manual interno de DTH en el sistema SPRYN.
A9.2.2	Provisión de acceso de usuario	Repetible	**¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio?** Si **¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones?** Se ajusta según a los roles establecidos; sin embargo, no existe política de control de acceso y segregación de funciones. **¿Existe un registro documental de la solicitud y aprobación de acceso?** Todo es solicitado mediante Quipux o correo institucional.	Existe un registro para la aprobación de acceso mediante las funciones establecidas por usuario y se otorga mediante correo institucional o quipux.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A9.2.3	Gestión de privilegios de acceso	Inicial	Más allá de A.9.2.2 **¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios?** **N**o, existe un proceso sin documentar de lo indicado. **¿Se genera un ID de usuario separado para otorgar privilegios elevados?** No, se asigna un perfil o se parametriza los permisos. **¿Se ha establecido una caducidad para los ID de usuario con privilegios?** No. Solo es comunicado de talento humano o responsable del área donde se encuentra el empleado para cambio de perfiles. **¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?** No.	No se evidencia el procedimiento para la gestión de privilegios de acceso por el departamento de TI.
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Repetible	**¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.?** Si. **¿Se verifica rutinariamente si hay contraseñas débiles?** No **¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas?** Solo se procede a cambio de contraseña al validad que el usuario a cambiar sea la misma persona solicitante. **¿Se transmite dicha información por medios seguros?** Si **¿Se generan contraseñas temporales suficientemente fuertes?** Si. **¿Se cambian las contraseñas por defecto de los fabricantes?** Si. **¿Se recomienda a los usuarios usar el software adecuado de protección de contraseñas?** No **¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?** En algunos aplicativos se accede mediante contraseñas.	Se tiene establecido ciertos procedimientos o controles en torno a la gestión de la información secreta o autenticación de usuarios; no se tiene documentación al respecto.
A9.2.5	Revisión de los derechos de acceso de usuario	Inicial	**¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones?** Si se revisa, a pesar que no está documentada.. **¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios?** No. Solo lo hace el personal de TIC.	Revisión periódica sin documentar; los cambios no se realizan sin previa solicitud de DTH.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente? No se hace revisión. De igual manera se revisa con el documento de talento humano sobre cambios existentes del personal.	
A9.2.6	Retirada o reasignación de los derechos de acceso	Repetible	**¿Existe un proceso de ajuste de derechos de acceso?** Existe un proceso pero no está documentado. Todo comienza ni bien el área de talento humano o el responsable de coordinación de las áreas para su respectiva comunicación de los trabajos realizados. **Ocurren ceses o despidos de empleados que las usan?** No se usan credenciales compartida. **¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo?** A todos., Eso incluye personal externo e interno. **¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red?** Si. **¿En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?** No se usan credenciales compartida.	Existe un procedimiento de cambio de los derechos de acceso que no se lo realiza hasta previa solicitud. No existe un control posterior.
A9.3	**Responsabilidades del usuario**			
A9.3.1	Uso de la información secreta de autenticación	Repetible	**¿Cómo se asegura la confidencialidad de las credenciales de autenticación?** Las credenciales son únicas para cada personal; se maneja las contraseñas y perfiles. **¿Existe un proceso de cambio de contraseñas en caso de ser comprometida?** No existe proceso, pero el usuario puede proceder al cambio desde el aplicativo o deben acudir a las oficinas de TIC. **¿Existen controles de seguridad relativas a las cuentas compartidas?** No existe cuentas compartidas, cada personal tiene su usuario y contraseña dentro del sistema acorde a los perfiles y área a la cual pertenece.	Existe un procedimiento para la asignación o cambio de contraseña; pendiente definir la confidencialidad las credenciales
A9.4	**Control de acceso a sistemas y aplicaciones**			
A9.4.1	Restricción del acceso a la información	Repetible	Más allá de A.9.2.2 **¿Existen controles de acceso adecuados?** Si existen por medio del usuario y contraseña. Intentos de inicio, Log, además de perfiles de usuario. **¿Se identifican los usuarios de forma individual individuales?** De forma individual.	El control se lo puede hacer revisando los logs, no hay un registro de cambios de permisos y se lo realiza según las necesidades del área.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas? Se maneja perfiles por usuario. El responsable de área informa a la Gestión de TIC mediante quipux; el perfil otorgado para cada empleado. El mismo procedimiento lo realiza talento humano para asignación de perfiles por tipo de cuenta en quipux.	No se tiene un procedimiento claro.
A9.4.2	Procedimientos seguros de inicio de sesión	Repetible	**¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado?** Si. **¿Cómo se autentican las identidades de usuario durante el proceso de inicio de sesión?** Mediante usuario y contraseña. **¿Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.?** No se usa. **¿La información de inicio de sesión solo se valida una vez imputadas las credenciales?** Si **¿Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas?** En algunos sistemas o aplicativos si se bloquean. **¿Se registran los inicios de sesión exitosos?** Se registra todas las sesiones en log. **¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?** Si. Solo vía telefónica o correo electrónico.	El personal de TIC tiene claro el procedimiento de inicio de sesión seguro, pero se puede mejorar haciendo también el monitoreo de los accesos validos así como de los fallidos.
A9.4.3	Sistema de gestión de contraseñas	Repetible	**¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos?** No. **¿Las reglas tienen en cuenta lo siguiente?** • **Longitud mínima de la contraseña:** Si. • **Evitan la reutilización de un número específico de contraseñas:** No • **Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.):** Si, en ciertos sistemas. • **Requiere el cambio forzado de contraseñas en el primer inicio de sesión:** Si. • **Esconde la contraseña durante la imputación:** Si. **¿Se almacenan y transmiten de forma segura (cifrado)?** Transmite vía telefónica o email.	Se tiene establecido ciertos controles como política para el sistema de gestión de contraseña. No se encuentra documentada y pero se lo realiza de manera empírica y generacional.
A9.4.4	Uso de utilidades con privilegios del sistema	Repetible	**¿Quién controla los servicios privilegiados?** Solo el personal del departamento de TIC **¿Quién puede acceder a ellos, bajo qué condiciones y con qué fines?** Solo el personal del departamento de TIC para la administración del sistema y aplicativos.	Existen controles no formales, se debe documentar.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se verifica que estas personas necesidad comercial para otorgar el acceso según su roles y responsabilidades? Si. Todo dependerá de lo descrito en la solicitud tanto de talento humano como del responsable del área. **¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado?** No existen registros. Solo los Logs de acceso. **¿Se tiene en cuenta la segregación de tareas?** Si.	
A9.4.5	Control de acceso al código fuente de los programas	Inicial	**¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios?** Esta subido en el servidor de aplicaciones WEB donde solo tiene acceso el personal de TIC. **¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.?** No se tiene un control adecuado, ni manejo de versiones. **¿Cómo se modifica el código fuente?** No se tiene indicio debido que actualmente no se cuenta con programador dentro del área desde hace 5 años. **¿Cómo se publica y se compila el código?** No se tiene indicio debido que actualmente no se cuenta con programador dentro del área desde hace 5 años. **¿Se almacenan y revisan los registros de acceso y cambios?** No	Se cuenta con controles que restringe el acceso al código fuente solo acceso personal de TI. No se evidencia manual y/o políticas de control de acceso al código fuente.
A10	**Criptografía**			
A10.1	**Controles criptográficos**			
A10.1.1	Política de uso de los controles criptográficos	Inexistente	**¿Existe una política que cubra el uso de controles criptográficos?** No. **¿Cubre lo siguiente?** • Los casos en los que información debe ser protegida a través de la criptografía: No. • Normas que deben aplicarse para la aplicación efectiva: No. • Un proceso basado en el riesgo para determinar y especificar la protección requerida No existe proceso. • Uso de cifrado para información almacenada o transferida: No. • Los efectos de cifrado en la inspección de contenidos de software: No. • Cumplimiento de las leyes y normativas aplicables: No.	Se puedo evidenciar la carencia de política de cifrado.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se cumple con la política y requerimientos de cifrado? No. No existe política de cifrado.	
A10.1.2	Gestión de claves	Inexistente	**¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)?** No. **¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas?** No. **¿Se generan claves diferentes para sistemas y aplicaciones?** No. **¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)?** No. **¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas?** No. **¿Se generan claves diferentes para sistemas y aplicaciones?** No. **¿Se evitan claves débiles?** No. **¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)?** **N**o. **¿Se hacen copias de respaldo de las claves?** No. **¿Se registran las actividades clave de gestión?** No. **¿Cómo se cumplen todos estos requisitos?** No se tiene conocimiento.	No se tiene definido procesos para el control de las claves de criptografía.
A11	**Seguridad física y del entorno**			
A11.1	**Áreas seguras**			
A11.1.1	Perímetro de seguridad física	Repetible	**¿Las instalaciones se encuentran en una zona de riesgo?** Si. **¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)?** Si. Existe señalética en el edificio. **¿El techo exterior, las paredes y el suelo son de construcción sólida?** Si. **¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado?** No. **¿Las puertas y ventanas son fuertes y con cerradura?** No. Solo una habitación donde se encuentra el bunker. **¿Se monitorea los puntos de acceso con cámaras?** Parcialmente mediante aplicativo. **¿Existe un sistema de detección de intrusos y se prueba periódicamente?** No	No se tiene establecido el control de acceso a ciertos lugares de uso exclusivo por el personal de TIC.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A11.1.2	Controles físicos de entrada	Inicial	**¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)?** Parcialmente. En el Data center existe pero no está habilitado. **¿Hay procedimientos que cubran las siguientes áreas?** • **Cambio regular código de acceso:** No. • **Inspecciones de las guardias de seguridad:** Si • **Visitantes siempre acompañados y registrados en el libro de visitantes:** No existe bitácora de ingreso en áreas críticas de TIC. • **Registro de movimiento de material:** No. • **Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas):** Accede solo con presencia del personal de TIC, mas no por responsabilidades. **¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)?:** No. **¿Se requiere para las áreas críticas?:** Para acceso a áreas críticas como data center o nodos de distribución se requiere autorización del jefe de área de TIC. **¿Existe un registro de todas las entradas y salidas?** No.	A pesar que el acceso a las áreas de TIC siempre es acompañado por un personal del área, no existe registro en bitácoras.
A11.1.3	Seguridad de oficinas, despachos y recursos	Repetible	**¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)?** Si. Excepto para uno de los centros de datos. **¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos?** No **¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?** Se tiene un conocimiento general pero no está detallado como activo en alguna documentación.	Se tiene conocimiento de los activos encontrados en dichas áreas de TI, como también la falta parcial de controles de acceso.
A11.1.4	Protección contra las amenazas externas y ambientales	Inicial	**¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.?** Si. Detectores de humo, extintores y alarmas. **¿Existe un procedimiento de recuperación de desastres?** No hay un procedimiento establecido. **¿Se contemplan sitios remotos?** No.	No se tiene un procedimiento establecido en caso de que ocurran.

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A11.1.5	El trabajo en áreas seguras	Inexistente	**¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo?** No. **¿Se hace un análisis para evaluar que los controles adecuados están implementados?** No. **Controles de acceso físico:** No existe. **Alarmas de intrusión:** No existe. **Monitoreo de CCTV (verificar la retención y frecuencia de revisión):** Existe sistema de video vigilancia, pero no se hace monitoreo. **Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación:** No **Políticas, procedimientos y pautas:** No existe **¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?** No existe algún procedimiento que regule este punto.	No existe procedimiento para asegurar la información de carácter sensible en los lugares de trabajo; así como controles.
A11.1.6	Áreas de carga y descarga	Optimizado	**¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado?** Se hace la entrega recepción en oficina o en el área de bodega general y siempre por un personal del área de TIC. **¿Se verifica que el material recibido coincide con un número de pedido autorizado?** Si. **¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?** Si. Según lo establecido por las políticas de gestión de activos y adquisidores de la organización.	Se ha establecido procedimiento aprobado en lo que corresponde a la gestión de activos.
A11.2	**Seguridad de los equipos**			
A11.2.1	Emplazamiento y protección de equipos	Repetible	**¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas?** Si **¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada?** No. **¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales?** • **Agua / inundación:** No • **Fuego y humo:** Fuego • **Temperatura, humedad y suministro eléctrico:** Temperatura. • **Polvo:** Mantenimiento • **Rayos, electricidad estática y seguridad del personal:** Ninguna	Existen algunas protecciones pero falta establecer mecanismos de protección o políticas de uso de equipos.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se prueban estos controles periódicamente y después de cambios importantes? No.	
A11.2.2	Instalaciones de suministro	Administrado	**¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad?** Si **¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente?** Si **¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante?** Si **¿Son probados con regularidad?** Solo cuando se hace mantenimiento **¿Hay una red de suministro eléctrico redundante?** Si **¿Se realizan pruebas de cambio?** Solo cuando se hace mantenimiento **¿Se ven afectados los sistemas y servicios?** No. **¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos?** Si **¿Están ubicados apropiadamente?** Si **¿Hay unidades redundantes, de repuesto o portátiles disponibles?** Solo en áreas críticas como los dos data center. **¿Hay detectores de temperatura con alarmas de temperatura?** Existe detectores de temperatura pero no con alarma.	Se evidencio que existe un sistema de suministro y climatización optimo y adecuado para lo requerido por el área de TIC. No se tiene un control para comprobar su funcionamiento, pero hasta la fecha cuando sucede un incidente eléctrico no hay pérdida del servicio.
A11.2.3	Seguridad del cableado	Inicial	**¿Hay protección física adecuada para cables externos, cajas de conexiones?** Si **¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias?** Si **¿Se controla el acceso a los paneles de conexión y las salas de cableado?** Está protegido bajo llave. **¿Existen procedimientos adecuados para todo ello?** No.	No se tiene una política de seguridad para incidentes de cableados, se debe establecer una mejor política.-
A11.2.4	Mantenimiento de los equipos	Repetible	**¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)?** Si. Esto se estipula al momento de contratar el servicio de mantenimiento. **¿Hay programas de mantenimiento y registros / informes actualizados?** Si. Una vez al año aunque por temas de presupuestos a veces no se cumple. **¿Se aseguran los equipos?** No	Existen políticas de mantenimiento; sin embargo, en ocasiones no se cumple, ni el mantenimiento preventivo/correctivo de los equipos.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A11.2.5	Retirada de materiales propiedad de la empresa	Repetible	**¿Existen procedimientos relativos al traslado de activos de información?** Si, aunque no está documentado. **¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados?** Cuando existe solicitud expresa por correo del área requirente, el coordinador del área aprueba lo requerido. **¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo?** No aplica **¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?** No aplica	El personal de TIC procede a realizar una acta de entrega o de retiro en caso del movimiento de un activo (no existe procedimiento).
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Inexistente	**¿Existe una "política de uso aceptable" que cubra los requisitos de seguridad y "obligaciones" con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas?** No existe política implementada. **¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras?** Solo de conexiones seguras. **¿Existen controles para asegura todo esto?** Solo para servidores. **¿Cómo se les informa a los trabajadores sobre sus obligaciones?** No se lo realiza. **¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?** No.	No existe una política establecida sobre el uso aceptable de los activos. .
A11.2.7	Reutilización o eliminación segura de equipos	Inexistente	**¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación?** No existe procedimiento; en caso que el equipo sea dado a otra área diferente se procede al respaldo y al borrado de la información. **¿Se utiliza cifrado fuerte o borrado seguro?** No. **¿Se mantienen registros adecuados de todos los medios que se eliminan?** No **¿La política y el proceso cubren todos los dispositivos y medios de TIC?** No existe política o proceso.	No existe procedimiento en torno a la reutilización de los equipos o respaldos de información en caso de retirar una unidad.
A11.2.8	Equipo de usuario desatendido	Inicial	**¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción?** Solo a nivel de aplicativos. **¿Cómo se verifica el cumplimiento?** No se puede verificar cumplimiento	Se tiene conocimiento de las salvaguardas pero no están establecidas como política.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado? Solo el tiempo que está por default al momento de instalar el sistema operativo. **¿Se protegen los bloqueos de pantalla con contraseña?** No. **¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC?** No **¿Cómo se verifica el cumplimiento?** No se puede verificar cumplimiento	
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Inicial	**¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas?** No hay políticas ni normas. **¿Funciona en la práctica?** No se aplica **¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos?** Si **¿Se activa automáticamente tras de un tiempo inactivo definido?** Si **¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?** Si	Existen las salvaguardas requerida para cumplimiento de este control. No se encuentra establecida como política.
A12	**Seguridad de las operaciones**			
A12.1	**Procedimientos y responsabilidades operacionales**			
A12.1.1	Documentación de procedimientos operacionales	Inexistente	**¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.?** No existe. **¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez?** No existe **¿Los procesos son razonablemente seguros y están bien controlados?** Si **¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal?** Las responsabilidades están definidas pero no existe capacitación al personal. **¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)?** No. **¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?** No	Se evidenció la falta de procedimiento de seguridad a pesar que existen roles y responsabilidades establecidos, estas no están acorde a la gestión de la seguridad de la información.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A12.1.2	Gestión de cambios	Inexistente	**¿Existe una política de gestión de cambios?** No **¿Existen registros relacionados a la gestión de cambios?** No **¿Se planifican y gestionan los cambios?** No **¿Se evalúan los riesgos potenciales asociados con los cambios?** No **¿Los cambios están debidamente documentados, justificados y autorizados por la administración?** No aplica.	No existe política sobre gestión de cambios u aprobaciones.
A12.1.3	Gestión de capacidades	Inexistente	**¿Existe una política de gestión de capacidad?** No **¿Existen registros relacionados a la gestión de capacidad?** No **¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante?** No aplica **¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?** No	Actualmente no se cuenta con una política establecida sobre la gestión de capacidades en los equipos críticos.
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	No aplicable	**¿Se segregan entornos de TIC de desarrollo, prueba y operacionales?** **¿Cómo se logra la separación a un nivel de seguridad adecuado?** **¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)?** **¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos?** **¿Cómo se promueve y se lanza el software?** **¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección?** **¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros?** **¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?**	El desarrollo de software o aplicativos no están dentro de los procesos establecidos para la Gestión en el departamento de TIC.
A12.2	**Protección contra el software malicioso (malware)**			

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A12.2.1	Controles contra el código malicioso	Inexistente	**¿Existen políticas y procedimientos asociados a controles antimalware?** No. **¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado?** No. **¿Cómo se compila, gestiona y mantiene la lista y por quién?** No aplica. **¿Hay controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT?** No hay antivirus corporativo instalado. **¿Se actualiza el software antivirus de forma automática?** No hay antivirus corporativo instalado. **¿Se general alertas accionables tras una detección?** No hay antivirus corporativo instalado. **¿Se toma acción de forma rápida y apropiada para minimizar sus efectos?** No aplica **¿Cómo se gestionan las vulnerabilidades técnicas?** Se realiza un estudio para tomar una decisión de solución del momento. **¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte?** No. **¿Existe un mecanismo de escalación para incidentes graves?** No.	No existen políticas o procedimientos establecidos para protección de código malicioso. En la actualidad, no cuenta con un antivirus corporativo.
A12.3	**Copias de seguridad**			
A12.3.1	Copias de seguridad de la información	Inexistente	**¿Existen políticas y procedimientos asociados a las copias de seguridad?** No **¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio?** No. **¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales?** No. **¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido?** No, se guarda en el mismo servidor. **¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica?** No. **¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar?** No. **¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?** Se desconoce.	No existe actualmente políticas establecidas en referencia a la copias de seguridad de la información.
A12.4	**Registros y supervisión**			

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A12.4.1	Registro de eventos	Inexistente	**¿Existen políticas y procedimientos para el registro de eventos?** No. **¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí?** Se hace monitoreo pero no se revisa el registro de eventos. **¿Se registra lo siguiente?** *No se tiene ningún registro*. • cambios en los ID de usuario: • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web **¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados?** No hay responsable asignado. **¿Cuál es el periodo de retención de eventos?** No se tiene registro. **¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?** No existe	No se hace registro de eventos; tampoco existe procedimientos establecidos.
A12.4.2	Protección de la información del registro	Inexistente	**¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable?** No. **¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado?** No se tiene conocimiento. **¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos?** El coordinador de TIC y el personal asignado a la seguridad de la información. **¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención?** No se tiene registro. **¿Existen copias de seguridad de los registros?** No.	Al no existir una política de registros de eventos, este control no se puede cumplir .

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A12.4.3	Registros de administración y operación	Inexistente	**¿Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)?** No. **¿Cómo se recogen, almacenan y aseguran, analizan los registros?** No se tiene registro. **¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?** No se tiene registro.	No se evidencia una política de registros de eventos, este control no se puede cumplir..
A12.4.4	Sincronización del reloj	Inexistente	**¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión?** No. **¿Hay un tiempo de referencia definido (ej. Reloj atómico, GPS o NTP)?** No. **¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales?** No aplica. **¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.?** No. **¿Existe una configuración de respaldo para la referencia de tiempo?** No.	No existe política relacionada a la sincronización del reloj del sistema y mecanismos de control de acceso.
A12.5	**Control del software en explotación**			
A12.5.1	Instalación del software en explotación	No aplicable	¿**Existe una política acerca de la instalación de software?** **¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción?** **¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)?** **¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.?** **¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados?** **¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas?** **¿Existe un control de cambio y aprobación adecuado para la aprobación de software?**	
A12.6	**Gestión de la vulnerabilidad técnica**			

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A12.6.1	Gestión de las vulnerabilidades técnicas	Inexistente	**¿Existe una política la gestión de vulnerabilidades técnicas?** No. **¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada?** No existe proceso de escaneo. **¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes?** Siguen sugerencias emitidas por el coordinador de TIC. **¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes?** No. **¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC?** No. **¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo?** No. **¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución?** Si. **¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados?** No **¿Los procesos para implementar parches urgentes son adecuados?** No. **¿Se emplea una administración automatizada de parches?** No. **¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?** No.	No existe política en referencia a la gestión de vulnerabilidades técnicas a ser consideradas.
A12.6.2	Restricción en la instalación de software	Repetible	**¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados?** Si. **¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos?** Solo se tiene una categoría, no se requiere otra. **¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?** Si.	Existe restricción al momento de instalación de software por terceros sin autorización del TIC, esta no está establecida como una política.
A12.7	**Consideraciones sobre la auditoria de sistemas de información**			

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A12.7.1	Controles de auditoría de sistemas de información	Inexistente	**¿Existe una política que requiera auditorias de seguridad de la información?** No. ¿**Existe un programa definido y procedimientos para auditoría**? No. ¿**Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales?** No aplica. **¿Se define el alcance de la auditoría en coordinación con la administración?** No aplica. **¿El acceso a las herramientas de auditoría de sistemas está controladas para evitar el uso y acceso no autorizado?** No aplica.	No existen políticas establecidas para las auditorias de sistemas de información.
A13	**Seguridad de las comunicaciones**			
A13.1	**Gestión de la seguridad de las redes**			
A13.1.1	Controles de red	Repetible	**¿Existen políticas de redes físicas e inalámbricas?** Si, por segmentación de redes **¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de** red? No. **¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella?** No. **¿Hay un sistema de autenticación para todos los accesos a la red de la organización?** No. **¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos?** Si. **¿Los usuarios se autentican adecuadamente al inicio de sesión?** En algunos de los casos acceden mediante usuario y contraseña. **¿Cómo se autentican los dispositivos de red?** No hay proceso de autenticación de dispositivos de red. **¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.?** Si. **¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?** Si.	Se tiene conocimiento de los controles de red y en especial sobre la segmentación. No se encuentra documentada.
A13.1.2	Seguridad de los servicios de red	Inicial	**¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada?** No. **¿Existe un monitoreo de servicios de red?** No. **¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)?** No se tiene conocimiento. **¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red?** Si. **¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?** No.	Se evidenció tener mecanismos de autenticación en la red; sin embargo, no se encuentran dentro de una política.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A13.1.3	Segmentación de redes	Definido	**¿Existe una política de segmentación de red?** Si. **¿Qué tipo de segmentación existe?** Segmentación de la red pública y de la red privada, como también de redes inalámbrica, entre otros. **¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)?** Es basada en los niveles de confianza. **¿Cómo se monitorea y controla la segregación?** No se controla ni se monitorea. **¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados?** Si. **¿Hay controles adecuados entre ellos?** No. **¿Cómo se controla la segmentación con proveedores y clientes?** No existe este tipo de segmentación. **¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?** no se tiene definidos el nivel de tolerancia en la organización.	El control se aplica correctamente, se ha segmentado sin embargo no se encuentra documentada.
A13.2	**Intercambio de información**			
A13.2.1	Políticas y procedimientos de intercambio de información	Repetible	**¿Existen políticas y procedimientos relacionados con la transmisión segura de información?** No que se haya establecido. **¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.?** mediante Correo electrónico **¿Está basado en la clasificación de la información?** Si. **¿Existen controles de acceso adecuados para esos mecanismos?** No. **¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)?** Desconoce. **¿Se sigue el principio de confidencialidad y privacidad?** Si. **¿Existen un programa de concientización, capacitación y cumplimiento?** No.	Se evidencian el principio de confidencialidad y privacidad con respecto al intercambio de la información, pero se lo realizada de manera informal.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A13.2.2	Acuerdos de intercambio de información	Inexistente	Más allá de A.13.2.1 **¿Qué tipos de comunicaciones se implementan las firmas digitales?** Se desconoce. **¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos?** No se tiene establecido. **¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas?** Si. **¿Cómo se mantiene una cadena de custodia para las transferencias de datos?** No aplica.	No existen acuerdos de intercambio de información.
A13.2.3	Mensajería electrónica	Inexistente	**Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.?** No. • **¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)?** No. • **¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?** No.	No existe políticas o controles establecidos con respectos a la mensajería electrónica.
A13.2.4	Acuerdos de confidencialidad o no revelación	Administrado	**¿Existen acuerdos de confidencialidad?** Solo existe uno de talento humano. **¿Han sido revisados y aprobados por el Departamento Legal?** Si **¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)?** Se desconoce. **¿Han sido aprobados y firmados por las personas adecuadas?** Si. **¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?** Se sanciona de acuerdo al reglamento interno como también a lo de la LOSEP o código de trabajo estipule.	Existen acuerdos de confidencialidad por el tipo de la información que maneja y es entregado actualmente a todo el personal nuevo que ingresa a la organización.
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A14.1	**Requisitos de seguridad en los sistemas de información**			
A14.1.1	Análisis de requisitos y especificaciones de Seguridad de la Información	Inexistente	**¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software?** No. **¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo?** No.	No existe políticas establecidos relacionados al análisis de requisitos de seguridad.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
			¿Se aplican estos controles para sistemas / software comercial, incluidos los productos "a medida" o personalizados? No aplica. **¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.)** No aplica.	
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	No aplicable	¿La **organización usa o proporciona aplicaciones web de comercio electrónico?** **¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio?** **¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad?** **¿Se fuerza https?** **¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)?** **¿Se analizan y documentan las amenazas de forma rutinaria?** **¿Existe una gestión de incidentes y cambios para tratarlos?**	A pesar que se cuenta con una página web institucional, esta no realiza algún tipo de comercio electrónico es solo informativa.
A14.1.3	Protección de las transacciones de servicios de aplicaciones	No aplicable	Más allá de A.14.1.2 ¿Las **transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet?** **¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.?** **¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?**	No se realiza transacciones en los servicios de aplicaciones que el hospital ofrece; es solo informativa.
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**			
A14.2.1	Política de desarrollo Seguro	No aplicable	¿**Existe una política de desarrollo seguro que abarque la arquitectura de seguridad?** **¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios?** **¿Los métodos de desarrollo incluyen pautas de programación segura?** **¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?**	No se aplica este control por motivos que el desarrollo de sistemas no está dentro de los servicios o procesos del departamento de TIC.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A14.2.2	Procedimiento de control de cambios en sistemas	Inexistente	**¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios?** No. **¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión?** Si se verifica la funcionalidad antes de su implementación. **¿Incluye un procedimiento para cambios de emergencia?** No. **¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones?** No. **¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?** No debido que no existe un proceso formal.	Se pudo evidenciar que no existen políticas con respecto a los controles de cambios en los sistemas adquiridos.
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Repetible	**¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado?** Si. **¿Hay registros de estas actividades?** No.	No existe una revisión técnica formal de las aplicaciones cuando existen cambios en el SO.
A14.2.4	Restricciones a los cambios en los paquetes de software	Definido	**¿Se hacen cambios a paquetes software adquiridos?** Si. **¿Se verifica que los controles originales no han sido comprometidos?** Si. **¿Se obtuvo el consentimiento y la participación del proveedor?** Depende del aplicativo. **¿El proveedor continúa dando soporte tras los cambios?** Siempre y cuando este dentro de la garantía técnica o se tenga contratado el soporte técnico. **¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores?** Si. **¿Se hace una comprobación de compatibilidad con otro software en uso?** Si.	Existen controles establecidos con respectos a las restricciones a los cambios en los paquetes de software pero no se encuentran documentadas
A14.2.5	Principios de ingeniería de sistemas seguros	No aplicable	¿**Se siguen principios de SDLC que incluye controles de seguridad?** **¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?**	Este control no se aplica porque no se desarrolla dentro del departamento de TIC
A14.2.7	Externalización del desarrollo de software	Definido	Más allá de A.14.2.6 ¿Se tienen en cuanta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero? • **Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual** Sí.	Se tiene en cuentas ciertos aspectos al momento del desarrollo de software por parte de

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
			• **Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba** Sí. • **Acceso al código fuente si el código ejecutable necesita ser modificado** No. • **Controles de prueba de seguridad de aplicaciones** En su mayoría. • **Evaluación de vulnerabilidad y tratamiento** En su mayoría.	terceros pero no se encuentra documentado.
A14.2.8	Pruebas funcionales de seguridad de sistemas	Definido	Más allá de A.14.2.7 **¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados?** Si.. **¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?** No.	Prueba de funcionamiento para nuevos o actualización de aplicativos; no se documenta.
A14.2.9	Pruebas de aceptación de sistemas	Inexistente	**¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red?** No. **¿Las pruebas replican situaciones y entornos operativos realistas?** No. **¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado?** No. **¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo?** No. **¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?** No.	Solo se realizan pruebas de funcionamiento de la aplicación. No pruebas de seguridad de la información.
A14.3	**Datos de prueba**			
A14.3.1	Protección de los datos de prueba	No aplicable	¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.? ¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas? ¿Existen registros de estas actividades?	El hospital no maneja este tipo de datos de prueba.
A15	**Relación con proveedores**			
A15.1	**Seguridad en las relaciones con proveedores**			

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Inexistente	**¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI?** No. **¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo?** No. **¿Los contratos y acuerdos abordan lo siguiente?** *No aplica* • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada • Información / propiedad intelectual, y obligaciones / limitaciones derivadas • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio • Habilitación de seguridad de los empleados y concienciación • Derecho de auditoría de seguridad por parte de la organización **¿Existe una obligación contractual de cumplimento?** No **¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?** No.	Se pudo evidenciar que no existen políticas con respecto a la seguridad de la información con respecto a las relaciones con proveedores establecidos.
A15.1.2	Requisitos de seguridad en contratos con terceros	Repetible	**¿Los contratos o acuerdos formales con proveedores cubren lo siguiente?** • Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, “robo de empleados”, etc.)	Este control dependerá a lo establecido en los TDR de los servicios requeridos.

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Inexistente	Más allá de A.15.1.1 y A.15.1.2 **¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos?** No existe manera de validar **¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros?** No se tiene conocimiento **¿Se puede rastrear el origen del producto o servicio?** No	No se evidencia una política establecida para la cadena de suministros.
A15.2	**Gestión de la provisión de servicios del proveedor**			
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Optimizado	**¿Existe una monitorización de servicios y quien responsable de esta actividad?** Si. Sería el administrador de la orden de compra o de servicio. **¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia?** No. No se ha visto necesario hasta el momento. **¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas?** Si es necesario. **¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría?** Siempre y cuando estén estipulados en los términos de referencias. **¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?** Todo depende como se estipule en los términos de referencia previa el contrato.	La política está establecida según lo indicado por el Servicio de Compras Públicas y definido en los TDR para el bien o servicio a adquirir.
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No Aplicable	**¿Cómo se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados?** No se ha ejecutado **¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización?** No se ha ejecutado. **¿Se actualizan los acuerdos relacionados con los cambios?** No se tiene procedimientos	Las relaciones con los proveedores de servicio es buena y siempre existen comunicación, no se realizan cambios con los contratos a los proveedores.
A16	**Gestión de incidentes de seguridad de la información**			
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**			

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A16.1.1	Responsabilidades y procedimientos	Inexistente	**¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes?** No **¿Qué cubre?** *No aplica* • El plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad • Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejora **¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?** No existe la gestión de incidentes.	No existe procedimiento a seguir, ni asignación de responsabilidades con respecto a la gestión de incidentes.
A16.1.2	Notificación de los eventos de seguridad de la información	Repetible	**¿Cómo se informan los eventos de seguridad de la información?** Solo vía telefónica. **¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen?** No, debido a que no se tiene esa capacitación **¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución.** No **¿Qué pasa con esos informes?** Solo se hace informe técnico en caso que se requiera.	A pesar que existe reportes de los eventos de seguridad de la información, esta no definida y se conocen las responsabilidades para su ejecución.
A16.1.3	Notificación de puntos débiles de la seguridad	Inexistente	Más allá de A.16.1.2 **¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual?** No. **¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?** No aplica.	No existe obligación a los trabajadores para notificar puntos débiles de seguridad.
A16.1.4	Evaluación y decisión sobre los eventos de	Repetible	**¿Qué tipos de eventos se espera que informen los empleados?** Todo suceso que no esté dentro de los parámetros del normal desarrollo de las actividades. **¿A quién informan?** Al departamento de TIC	Se evalúa y se toma la mejor decisión a la SI, esta no se lo realiza de

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
	seguridad de información		**¿Cómo se evalúan estos eventos para decidir si califican como incidentes?** No se evalúa. **¿Hay una escala de clasificación?** No **¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves?** No. **¿En qué se basa?** No aplica	manera formal y no se indica como los empleados puedan manejar los incidentes.
A16.1.5	Respuesta a incidentes de seguridad de la información	Repetible	**¿Cómo se recolecta, almacena y evalúa la evidencia?** No hay un proceso determinado. **¿Hay una matriz de escalación para usar según sea necesario?** No **¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes? No.** **¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?** Se emite un informe técnico y es enviado a las autoridades.	Solo se emite un informe técnico, todo depende de las capacidades de resolución de los eventos que se presenten.
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inexistente	¿**Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes?** No. ¿**Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias?** No. **Además, ¿Se está utilizado para formación y concienciación**? No. ¿**La organización cuenta con un proceso de gestión de incidentes relativamente maduro**? No. ¿**Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad**? No **¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área?** No se realiza.	No existe un proceso de evaluación y autoaprendizaje en base a los incidentes de seguridad de la información o retroalimentación del mismo.
A16.1.7	Recopilación de evidencias	Inexistente	**¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol? (cadena de evidencia rigurosamente mantenida, evidencia asegurada en almacenamiento, herramientas y técnicas)** No. **¿Quién decide emprender un análisis forense, y en qué criterio se base?** No está definido **¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?** No	Falta de personal capacitado para la gestión de incidentes.
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**			
A17.1	**Continuidad de la seguridad de la información**			

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A17.1.1	Planificación de la continuidad de la seguridad de la información	Inexistente	**¿Cómo se determinan los requisitos de continuidad del negocio?** No se han definido. **¿Existe un plan de continuidad de negocio?** No **¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos?** No. **¿Se identifica el impacto potencial de los incidentes?** No. **¿Se evalúan los planes de continuidad del negocio?** No. **¿Se llevan a cabo ensayos de continuidad?** No.	No se tiene establecido la planificación con respecto a la continuidad de la seguridad de la información.
A17.1.2	Implementar la continuidad de la seguridad de la información	Inexistente	**¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción?** No existe. **¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares?** No aplica **¿La planificación de la continuidad es consistente e identifica las prioridades de restauración?** No se tiene conocimiento. **¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades?** No existe y tampoco está definido los miembros. **¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?** No aplica	No existe controles establecidos para la seguridad de la información para continuidad del negocio.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Inexistente	**¿Existe un método de pruebas del plan de continuidad?** No existe **¿Con qué frecuencia se llevan a cabo dichas pruebas?** No aplica **¿Hay evidencia de las pruebas reales y sus resultados?** No **¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?** No aplica	No existe metodología establecida para verificación de la continuidad de SI.
A17.2	**Redundancias**			

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Definido	**¿Cómo se identifican los requisitos de disponibilidad de servicios?** Se evalúa los servicios críticos que deben funcionar para la institución. **¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga?** Si en {énfasis a lo que tiene que ver la capacidad de rendimiento y balanceo de carga. **¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí?** Si. **¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?** No aplica porque no poseen sitios para recuperación ante un desastre.	Está establecidos los requisitos para la disponibilidad de los recursos; sin embargo no está documentada.
A18	**Cumplimiento**			
A18.1	**Cumplimiento de los requisitos legales y contractuales**			
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Inexistente	**¿Existe una política acerca del cumplimiento de requisitos legales? LOPD, GDPR, etc.** No. **¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables?** No. **¿Hay una persona encargada de mantener, usar y controlar el registro?** No. **¿Cómo se logra y se garantiza el cumplimiento?** No aplica. **¿Existen controles adecuados para cumplir con los requisitos?** No	No se pudo evidenciar una política establecida y que intervengan los diferentes requisitos legales.
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Administrado	**¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?** Si, se tiene como ente regulador para licenciamiento el MINTEL y propiedad intelectual esta la ley.	Los registros se encuentra acorde a la ley y de forma adecuada; falta realizar un poco más de control.
A18.1.3	Protección de los registros de la organización	Inexistente	**¿Existe una política que contemple lo siguiente? Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos.** No. **¿Se almacenan las firmas digitales de forma segura?** No. **¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado?** No **¿Se verifica periódicamente la integridad de los registros?** No. **¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?** Si.	No existe política para la protección de los registros de la organización.

	Sección / Control de Seguridad de la información	Estado	Preguntas	Comentarios
A18.1.4	Protección y privacidad de la información de carácter personal	Inexistente	**¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal?** No. **¿Hay un responsable de privacidad en la organización?** No. **¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización?** No. **¿Cuáles son los controles de acceso a información de carácter personal?** No existe. **¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos?** No se Cuenta definidos	No existe controles de acceso a la información como tampoco existe un responsable de privacidad en la organización.
A18.1.5	Regulación de los controles criptográficos	Inexistente	**¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico?** No **¿Estas actividades cumplen con los requisitos legales y reglamentarios?** No aplica	No existe política con respecto a las regulaciones de controles criptográficos.
A18.2	**Revisiones de la seguridad de la información**			
A18.2.1	Revisión independiente de la seguridad de la información	Inexistente	**¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información?** No **¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos?** No. **¿Están los objetivos y el alcance de auditoria autorizados por la gerencia?** No aplica. **¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información?** No **¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?** No aplica.	Hasta el momento no han existido auditorías internas para la seguridad de la información.
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Inicial	**¿Cómo garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente?** Se espera el cumplimiento de las obligaciones del personal de departamento de TIC. **¿Se hace una verificación periódica?** No	El personal de TIC garantiza que los procedimientos correspondientes de seguridad que se ejecuten.

Sección / Control de Seguridad de la información		Estado	Preguntas	Comentarios
A18.2.3	Comprobación del cumplimiento técnico	Inexistente	**¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares?** No. **¿Las pruebas son realizadas por profesionales debidamente cualificados, competentes y confiables?** No aplica. **¿Cómo informa, analiza y utilizan los resultados de dichas pruebas?** No aplica. **¿La prioridad de tratamiento se basa en un análisis de riesgos?** No aplica. **¿Hay evidencias de medidas tomadas para abordar los problemas identificados?** No aplica.	En la actualidad no existe escaneos de vulnerabilidades o cumplimiento de evaluación.

Fuente: Autor

Anexo C: Identificación y Clasificación de activos.

Este anexo detalla la identificación y clasificación de los activos del Hospital FIB acorde a la norma ISO27002; se codificó, su custodio y su ubicación en el sitio.

COD Activo	Propiedad del Activo		Ubicación y Medio			Clasificación
	Propietario	Custodio	Ubicación	Físico	Digital	
A1	CNT	Luis Villavicencio	Data Center 1	X		Restringida
A2	TIC	Luis Villavicencio	Data Center 1	X		Restringida
A3	TIC	Luis Villavicencio	Data Center 1	X		Restringida
A4	TIC	Luis Villavicencio	Data Center 1	X		Restringida
A5	TIC	Luis Villavicencio	Data Center 1	X		Restringida
A6	TIC	Luis Villavicencio	Data Center 1	X		Restringida
A7	TIC	Luis Villavicencio	Data Center 1	X		Restringida
A8	TIC	Luis Villavicencio	Data Center 2	X		Restringida
A9	TIC	Luis Villavicencio	Data Center 2	X		Restringida
A10	TIC	Luis Villavicencio	Data Center 2	X		Restringida
A11	TIC	Luis Villavicencio	Data Center 1	X		Restringida
A12	TIC	Luis Villavicencio	Data Center 2	X		Restringida
A13	TIC	Luis Villavicencio	Data Center 2	X		Restringida
A14	TIC	Luis Villavicencio	Data Center 2	X		Restringida
A15	TIC	Luis Villavicencio	Oficina de TIC	X		Restringida
A16	TIC	Luis Villavicencio	Oficina de TIC	X		Restringida
A17	TIC	Luis Villavicencio	Data Center 2	X		Restringida
A18	TIC	Luis Villavicencio	Data center 2	X		Restringida
A19	TIC	Luis Villavicencio	Planta Baja - Área remodelada	X		Restringida
A20	TIC	Luis Villavicencio	Planta Baja Hospitalización	X		Restringida
A21	TIC	Luis Villavicencio	Segundo Piso Consulta Externa	X		Restringida
A22	TIC	Luis Villavicencio	Primer Piso Consulta Externa	X		Restringida
A23	TIC	Luis Villavicencio	Planta Baja Consulta Externa	X		Restringida
A24	TIC	Luis Villavicencio	Farmacia	X		Restringida
A25	TIC	Luis Villavicencio	Emergencia	X		Restringida
A26	TIC	Luis Villavicencio	Patología	X		Restringida
A27	TIC	Luis Villavicencio	Laboratorio	X		Restringida
A28	TIC	Luis Villavicencio	Ropería	X		Restringida
A29	TIC	Luis Villavicencio	Quirófano	X		Restringida
A30	TIC	Luis Villavicencio	Tercer Piso Hospitalización	X		Restringida

COD	Propiedad del Activo		Ubicación y Medio			Clasificación
Activo	Propietario	Custodio	Ubicación	Físico	Digital	
A31	TIC	Luis Villavicencio	Cuarto Piso Hospitalización	X		Restringida
A32	TIC	Luis Villavicencio	Quinto Piso Hospitalización	X		Restringida
A33	TIC	Luis Machuca	Data Center		X	Interno
A34	TIC	Luis Villavicencio	Data Center 1		X	Interno
A35	TIC	Luis Villavicencio	Data center 2		X	Interno
A36	TIC	Luis Villavicencio	Oficina de TIC		X	Interno
A37	TIC	Luis Machuca	Oficina de TIC		X	Interno
A38	TIC	Luis Villavicencio	Data Center 1		X	Interno
A39	TIC	Luis Machuca	Data Center 2		X	Interno
A40	TIC	Luis Machuca	Data Center 1		X	Interno
A41	TIC	Arturo Bueno	Data Center 1		X	Interno
A42	TIC	Luis Machuca	Data Center 1		X	Interno
A43	TIC	Luis Machuca	Data Center 1		X	Interno
A44	TIC	Luis Villavicencio	Oficina de TIC		X	Interno
A45	TIC	Luis Machuca	Data Center 2		X	Interno
A46	TIC	Luis Machuca	Data Center 1		X	Interno
A47	TIC	Luis Machuca	Data Center 1		X	Interno
A48	TIC	Luis Machuca	Data Center 1		X	Interno
A49	TIC	Luis Villavicencio	Data Center 1		X	Interno
A50	TIC	Luis Machuca	Data Center 2		X	Interno
A51	TIC	Luis Machuca	Data Center 1		X	Restringida
A52	TIC	Luis Villavicencio	Data Center 1		X	Restringida
A53	TIC	Luis Villavicencio	Data Center 2		X	Restringida
A54	TIC	Luis Villavicencio	Data Center 1		X	Restringida
A55	TIC	Luis Villavicencio	Área de Laboratorio		X	Restringida
A56	TIC	Luis Villavicencio	Departamento de TIC	X		Interno
A57	TIC	Luis Machuca	Departamento de TIC	X		Interno
A58	TIC	Luis Machuca	Departamento de TIC	X		Interno
A59	TIC	No Asignado	Departamento de TIC	X		Interno
A60	TIC	No Asignado	Departamento de TIC	X		Interno
A61	TIC	No Asignado	Departamento de TIC	X		Interno
A62	TIC	No Asignado	Departamento de TIC		X	Interno
A63	TIC	No Asignado	Departamento de TIC		X	Interno
A64	TIC	Varios	Varios	X		Interno

COD Activo	Propiedad del Activo		Ubicación y Medio			Clasificación
	Propietario	Custodio	Ubicación	Físico	Digital	
A65	TIC	Varios	Varios	X		Interno
A66	TIC	Luis Villavicencio	Departamento de TIC		X	Público
A67	TIC	Luis Villavicencio	Departamento de TIC	X		Interno

Fuente: Autor

Anexo D: Valoración de los activos.

Este anexo analiza los activos de la información identificado según su impacto y criterios conforme al direccionamiento estratégico del Hospital FIB.

COD	Tipo de Activo	Nombre	Ubicación	Impacto			
				C	I	D	VA
A1	Hardware	Router de frontera	Data Center 1	3	1	2	2,00
A2	Redes	Core Cisco	Data Center 1	4	1	4	3,00
A3	Redes	Firewall Cisco	Data Center 1	4	1	4	3,00
A4	Redes	Wireless Controller	Data Center 1	4	1	2	2,33
A5	Hardware	Sistema de Video Vigilancia	Data Center 1	1	1	1	1,00
A6	Redes	Servidor Cisco 1	Data Center 1	4	4	4	4,00
A7	Redes	Servidor Cisco 2	Data Center 1	4	1	4	3,00
A8	Redes	Servidor IBM M3	Data Center 2	4	1	4	3,00
A9	Redes	Servidor IBM M4	Data Center 2	4	1	4	3,00
A10	Hardware	PC / Servidor 1	Data Center 2	1	2	2	1,67
A11	Hardware	PC / Servidor 2	Data Center 1	3	4	4	3,67
A12	Hardware	PC / Servidor 3	Data Center 2	2	3	3	2,67
A13	Hardware	PC / Servidor 4	Data Center 2	3	3	3	3,00
A14	Hardware	PC / Servidor 5	Oficina de TIC	1	1	1	1,00
A15	Hardware	PC / Servidor 6	Oficina de TIC	3	4	2	3,00
A16	Hardware	PC / Servidor 7	Oficina de TIC	1	1	1	1,00
A17	Hardware	MITEL Principal	Data Center 2	2	1	3	2,00
A18	Hardware	MITEL Secundario	Data center 2	1	1	3	1,67
A19	Hardware	Data Center 1	Planta Baja - Área remodelada	4	1	4	3,00
A20	Hardware	Data Center 2	Planta Baja Hospitalización	4	1	4	3,00
A21	Hardware	Nodo 1	Segundo Piso Consulta Externa	2	1	4	2,33
A22	Hardware	Nodo 2	Primer Piso Consulta Externa	2	1	4	2,33
A23	Hardware	Nodo 3	Planta Baja Consulta Externa	2	1	4	2,33
A24	Hardware	Nodo 4	Farmacia	2	1	4	2,33
A25	Hardware	Nodo 5	Emergencia	2	1	4	2,33
A26	Hardware	Nodo 6	Patología	2	1	4	2,33
A27	Hardware	Nodo 7	Laboratorio	2	1	4	2,33
A28	Hardware	Nodo 8	Ropería	2	1	4	2,33
A29	Hardware	Nodo 9	Quirófano	2	1	4	2,33

COD	Tipo de Activo	Nombre	Ubicación	Impacto			
				C	I	D	VA
A30	Hardware	Nodo 10	Tercer Piso Hospitalización	2	1	4	2,33
A31	Hardware	Nodo 11	Cuarto Piso Hospitalización	2	1	4	2,33
A32	Hardware	Nodo 12	Quinto Piso Hospitalización	2	1	4	2,33
A33	Software	Sistema Hosvital	Data Center 1	4	3	4	3,67
A34	Software	Sistema De talento Humano	Data Center 1	2	3	2	2,33
A35	Software	Sistema MS-PROG	Data center 2	1	1	1	1,00
A36	Software	Zimbra	Oficina de TIC	3	3	2	2,67
A37	Software	Jaspersoft	Oficina de TIC	1	1	1	1,00
A38	Software	Sistema de Marcaciones	Data Center 1	3	4	3	3,33
A39	Software	Sistema SERCOP	Data Center 2	1	1	1	1,00
A40	Software	Wireless Controller	Data Center 1	2	1	2	1,67
A41	Software	Sistema Video vigilancia BOSCH	Data Center 1	1	2	2	1,67
A42	Software	Proxy 3	Data Center 1	1	1	3	1,67
A43	Software	Proxy 5	Data Center 1	1	1	3	1,67
A44	Software	Proxy 56	Oficina de TIC	1	1	3	1,67
A45	Software	Server Red Hat 1	Data Center 2	2	2	3	2,33
A46	Software	Server Red Hat 2	Data Center 1	2	2	3	2,33
A47	Software	Server Red Hat 3	Data Center 1	2	2	3	2,33
A48	Software	Server Red Hat 4	Data Center 1	2	2	3	2,33
A49	Software	Laboratorio	Data Center 1	1	2	2	1,67
A50	Software	Sistema MITEL	Data Center 2	1	1	2	1,33
A51	Información	Base de Datos Hosvital	Data Center 1	4	4	4	4,00
A52	Información	Base de Datos Sistema de Talento Humano	Data Center 1	4	4	4	4,00
A53	Información	Base de Datos MSPROG	Data Center 2	2	4	2	2,67
A54	Información	Base de Datos Sistema de Marcaciones	Data Center 1	4	4	4	4,00
A55	Información	Base de Datos Laboratorio	Área de Laboratorio	3	4	2	3,00
A56	Hardware	PC 1	Departamento de TIC	1	2	1	1,33
A57	Hardware	Portátil 1	Departamento de TIC	3	2	1	2,00
A58	Recursos Humanos	Administrador de Sistema Hosvital	Departamento de TIC	3	2	4	3,00
A59	Recursos Humanos	Administrador de Sistemas	Departamento de TIC	2	2	2	2,00
A60	Recursos Humanos	Analista de Redes	Departamento de TIC	3	3	4	3,33

COD	Tipo de Activo	Nombre	Ubicación	Impacto			
				C	I	D	VA
A61	Recursos Humanos	Responsable de la Seguridad de la información	Departamento de TIC	3	3	4	3,33
A62	Software	Antivirus corporativo	Varios	3	3	3	3,00
A63	Software	Sistema Operativo W10	Varios	3	3	3	3,00
A64	Hardware	Equipos PC	Varios	2	2	3	2,33
A65	Hardware	Portátiles	Varios	2	2	3	2,33
A66	Organización	Internet	Departamento de TIC	3	2	3	2,67
A67	Organización	Impresiones	Varios	1	1	2	1,33

Fuente: Autor

Anexo E: Evaluación del Riesgo.

La evaluación del riesgo se realiza mediante un análisis de la probabilidad de la ocurrencia por la amenaza y vulnerabilidad para cada activo, una vez dado el análisis cualitativo se tiene el nivel del riesgo.

ANÁLISIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo
COD	Nombre Activo	Amenaza	Vulnerabilidad	Control implementado	CID	Nivel Amenaza	Nivel Vulnerabilidad		
A1	Router de frontera	AME-02.5	VUL-08	A15.2.1	2,00	1	1	2,00	Bajo
A1	Router de frontera	AME-01.2	VUL-02	---	2,00	2	4	16,00	Muy Alto
A2	Core Cisco	AME-02.5	VUL-08	---	3,00	1	4	12,00	Alto
A2	Core Cisco	AME-01.2	VUL-02	---	3,00	2	4	24,00	Muy Alto
A3	Firewall Cisco	AME-02.5	VUL-08	---	3,00	1	4	12,00	Alto
A3	Firewall Cisco	AME-01.2	VUL-02	---	3,00	2	4	24,00	Muy Alto
A4	Wireless Controller	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A4	Wireless Controller	AME-01.2	VUL-02	---	2,33	2	2	9,33	Alto
A5	Sistema de Video Vigilancia	AME-02.5	VUL-08	---	1,00	1	2	2,00	Bajo
A5	Sistema de Video Vigilancia	AME-01.2	VUL-02	---	1,00	2	2	4,00	Bajo
A6	Servidor Cisco 1	AME-03.11	VUL-08	---	4,00	1	3	12,00	Alto
A6	Servidor Cisco 1	AME-01.2	VUL-02	---	4,00	2	4	32,00	Muy Alto
A7	Servidor Cisco 2	AME-03.11	VUL-08	---	3,00	1	3	9,00	Medio
A7	Servidor Cisco 2	AME-01.2	VUL-02	---	3,00	2	4	24,00	Muy Alto
A8	Servidor IBM M3	AME-03.11	VUL-08	---	3,00	1	2	6,00	Medio

ANÁLISIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo
COD	Nombre Activo	Amenaza	Vulnerabilidad	Control implementado	CID	Nivel Amenaza	Nivel Vulnerabilidad		
A8	Servidor IBM M3	AME-03.10	VUL-16	---	3,00	2	1	6,00	Medio
A9	Servidor IBM M4	AME-03.11	VUL-08	---	3,00	1	2	6,00	Medio
A9	Servidor IBM M4	AME-03.10	VUL-16	---	3,00	2	1	6,00	Medio
A10	PC / Servidor 1	AME-03.11	VUL-08	---	1,67	1	2	3,33	Bajo
A10	PC / Servidor 1	AME-03.10	VUL-16	---	1,67	1	1	1,67	Bajo
A11	PC / Servidor 2	AME-03.11	VUL-08	---	3,67	1	2	7,33	Medio
A11	PC / Servidor 2	AME-01.2	VUL-02	---	3,67	2	4	29,33	Muy Alto
A11	PC / Servidor 2	AME-03.10	VUL-16	---	3,67	1	1	3,67	Bajo
A12	PC / Servidor 3	AME-03.11	VUL-08	---	2,67	1	2	5,33	Medio
A12	PC / Servidor 3	AME-03.10	VUL-16	---	2,67	1	2	5,33	Medio
A13	PC / Servidor 4	AME-03.11	VUL-08	---	3,00	1	2	6,00	Medio
A13	PC / Servidor 4	AME-03.10	VUL-16	---	3,00	1	2	6,00	Medio
A14	PC / Servidor 5	AME-03.11	VUL-08	---	1,00	1	2	2,00	Bajo
A14	PC / Servidor 5	AME-02.1	VUL-04	---	1,00	3	1	3,00	Bajo
A14	PC / Servidor 5	AME-03.10	VUL-16	---	1,00	1	1	1,00	Bajo
A15	PC / Servidor 6	AME-03.11	VUL-08	---	3,00	1	2	6,00	Medio
A15	PC / Servidor 6	AME-02.1	VUL-04	---	3,00	3	2	18,00	Muy Alto
A15	PC / Servidor 6	AME-03.10	VUL-16	---	3,00	1	1	3,00	Bajo
A16	PC / Servidor 7	AME-03.11	VUL-08	---	1,00	1	2	2,00	Bajo
A16	PC / Servidor 7	AME-02.1	VUL-04	---	1,00	3	1	3,00	Bajo
A16	PC / Servidor 7	AME-03.10	VUL-16	---	1,00	1	1	1,00	Bajo

ANÁLISIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo
COD	Nombre Activo	Amenaza	Vulnerabilidad	Control implementado	CID	Nivel Amenaza	Nivel Vulnerabilidad		
A17	MITEL Principal	AME-03.11	VUL-08	---	2,00	3	2	12,00	Alto
A18	MITEL Secundario	AME-03.11	VUL-08	---	1,67	3	2	10,00	Alto
A19	Data Center 1	AME-01.2	VUL-02	---	3,00	2	4	24,00	Muy Alto
A19	Data Center 1	AME-02.2	VUL-20	A11.2.2	3,00	3	2	18,00	Muy Alto
A19	Data Center 1	AME-04.9	VUL-07	---	3,00	4	4	48,00	Muy Alto
A20	Data Center 2	AME-02.1	VUL-04	---	3,00	3	2	18,00	Muy Alto
A20	Data Center 2	AME-02.2	VUL-20	A11.2.2	3,00	4	2	24,00	Muy Alto
A21	Nodo 1	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A21	Nodo 1	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A21	Nodo 1	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A22	Nodo 2	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A22	Nodo 2	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A22	Nodo 2	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A23	Nodo 3	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A23	Nodo 3	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A23	Nodo 3	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A24	Nodo 4	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A24	Nodo 4	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A24	Nodo 4	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A25	Nodo 5	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A25	Nodo 5	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo

ANÁLISIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo
COD	Nombre Activo	Amenaza	Vulnerabilidad	Control implementado	CID	Nivel Amenaza	Nivel Vulnerabilidad		
A25	Nodo 5	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A26	Nodo 6	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A26	Nodo 6	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A26	Nodo 6	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A27	Nodo 7	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A27	Nodo 7	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A27	Nodo 7	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A28	Nodo 8	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A28	Nodo 8	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A28	Nodo 8	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A29	Nodo 9	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A29	Nodo 9	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A29	Nodo 9	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A30	Nodo 10	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A30	Nodo 10	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A30	Nodo 10	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A31	Nodo 11	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A31	Nodo 11	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A31	Nodo 11	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A32	Nodo 12	AME-02.5	VUL-08	---	2,33	1	2	4,67	Medio
A32	Nodo 12	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo

ANÁLISIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo
COD	Nombre Activo	Amenaza	Vulnerabilidad	Control implementado	CID	Nivel Amenaza	Nivel Vulnerabilidad		
A32	Nodo 12	AME-04.9	VUL-07	---	2,33	4	4	37,33	Muy Alto
A33	Sistema Hosvital	AME-03.10	VUL-16	---	3,67	2	2	14,67	Alto
A33	Sistema Hosvital	AME-03.6	VUL-13	---	3,67	4	2	29,33	Muy Alto
A33	Sistema Hosvital	AME-03.7	VUL-14	---	3,67	3	1	11,00	Alto
A33	Sistema Hosvital	AME-03.4	VUL-11	A9.2.1	3,67	2	1	7,33	Medio
A33	Sistema Hosvital	AME-03.10	VUL-16	---	3,67	1	4	14,67	Alto
A34	Sistema De talento Humano	AME-03.10	VUL-16	---	2,33	2	2	9,33	Alto
A34	Sistema De talento Humano	AME-03.10	VUL-16	---	2,33	1	3	7,00	Medio
A35	Sistema MS-PROG	AME-03.10	VUL-16	---	1,00	2	2	4,00	Bajo
A35	Sistema MS-PROG	AME-03.10	VUL-16	---	1,00	1	2	2,00	Bajo
A36	Zimbra	AME-03.10	VUL-16	---	2,67	2	2	10,67	Alto
A36	Zimbra	AME-04.13	VUL-15	---	2,67	1	4	10,67	Alto
A36	Zimbra	AME-03.1	VUL-09	---	2,67	3	4	32,00	Muy Alto
A36	Zimbra	AME-03.10	VUL-16	---	2,67	1	2	5,33	Medio
A37	Jaspersoft	AME-03.10	VUL-16	---	1,00	1	1	1,00	Bajo
A37	Jaspersoft	AME-03.10	VUL-16	---	1,00	1	1	1,00	Bajo
A38	Sistema de Marcaciones	AME-03.10	VUL-16	---	3,33	1	2	6,67	Medio
A38	Sistema de Marcaciones	AME-03.10	VUL-16	---	3,33	1	2	6,67	Medio
A39	Sistema SERCOP	AME-03.10	VUL-16	---	1,00	1	1	1,00	Bajo
A40	Wireless Controller	AME-03.10	VUL-16	---	1,67	1	2	3,33	Bajo
A41	Sistema Video vigilancia BOSCH	AME-03.10	VUL-16	---	1,67	1	2	3,33	Bajo

ANÁLISIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo
COD	Nombre Activo	Amenaza	Vulnerabilidad	Control implementado	CID	Nivel Amenaza	Nivel Vulnerabilidad		
A42	Proxy 3	AME-03.10	VUL-16	---	1,67	1	2	3,33	Bajo
A43	Proxy 5	AME-03.10	VUL-16	---	1,67	1	2	3,33	Bajo
A44	Proxy 56	AME-03.10	VUL-16	---	1,67	1	2	3,33	Bajo
A45	Server Red Hat 1	AME-03.10	VUL-16	---	2,33	1	2	4,67	Medio
A45	Server Red Hat 1	AME-03.10	VUL-16	---	2,33	2	4	18,67	Muy Alto
A46	Server Red Hat 2	AME-03.10	VUL-16	---	2,33	1	2	4,67	Medio
A46	Server Red Hat 2	AME-03.10	VUL-16	---	2,33	2	4	18,67	Muy Alto
A47	Server Red Hat 3	AME-03.10	VUL-16	---	2,33	1	2	4,67	Medio
A47	Server Red Hat 3	AME-03.10	VUL-16	---	2,33	2	4	18,67	Muy Alto
A48	Server Red Hat 4	AME-03.10	VUL-16	---	2,33	1	2	4,67	Medio
A48	Server Red Hat 4	AME-03.10	VUL-16	---	2,33	2	4	18,67	Muy Alto
A49	Laboratorio	AME-03.10	VUL-16	---	1,67	1	2	3,33	Bajo
A49	Laboratorio	AME-03.10	VUL-16	---	1,67	2	2	6,67	Medio
A50	Sistema MITEL	AME-03.10	VUL-16	---	1,33	3	2	8,00	Medio
A50	Sistema MITEL	AME-03.10	VUL-16	---	1,33	4	2	10,67	Alto
A51	Base de Datos Hosvital	AME-04.13	VUL-15	---	4,00	3	4	48,00	Muy Alto
A51	Base de Datos Hosvital	AME-03.10	VUL-16	---	4,00	2	2	16,00	Muy Alto
A51	Base de Datos Hosvital	AME-03.10	VUL-16	---	4,00	1	4	16,00	Muy Alto
A52	Base de Datos Sistema de Talento Humano	AME-04.13	VUL-15	---	4,00	2	4	32,00	Muy Alto
A52	Base de Datos Sistema de Talento Humano	AME-03.10	VUL-16	---	4,00	1	3	12,00	Alto

ANÁLISIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo
COD	Nombre Activo	Amenaza	Vulnerabilidad	Control implementado	CID	Nivel Amenaza	Nivel Vulnerabilidad		
A53	Base de Datos MSPROG	AME-04.13	VUL-15	---	2,67	1	4	10,67	Alto
A53	Base de Datos MSPROG	AME-03.10	VUL-16	---	2,67	2	3	16,00	Muy Alto
A54	Base de Datos Sistema de Marcaciones	AME-04.13	VUL-15	---	4,00	2	4	32,00	Muy Alto
A54	Base de Datos Sistema de Marcaciones	AME-03.10	VUL-16	---	4,00	1	3	12,00	Alto
A55	Base de Datos Laboratorio	AME-04.13	VUL-15	---	3,00	1	4	12,00	Alto
A55	Base de Datos Laboratorio	AME-03.10	VUL-16	---	3,00	1	3	9,00	Medio
A56	PC 1	AME-03.11	VUL-08	---	1,33	1	2	2,67	Bajo
A56	PC 1	AME-03.10	VUL-16	---	1,33	1	1	1,33	Bajo
A57	Portátil 1	AME-03.11	VUL-08	---	2,00	1	2	4,00	Bajo
A57	Portátil 1	AME-03.10	VUL-16	---	2,00	1	1	2,00	Bajo
A57	Portátil 1	AME-04.9	VUL-07	---	2,00	2	4	16,00	Muy Alto
A58	Administrador de Sistema Hosvital	AME-03.12	VUL-22	---	3,00	4	1	12,00	Alto
A59	Administrador de Sistemas	AME-03.12	VUL-22	---	2,00	1	1	2,00	Medio
A60	Analista de Redes	AME-03.12	VUL-22	---	3,33	2	4	26,67	Muy Alto
A61	Responsable de la Seguridad de la Información	AME-03.12	VUL-22	---	3,33	1	4	13,33	Alto
A62	Antivirus corporativo	AME-04.10	VUL-19	---	3,00	1	3	9,00	Medio
A63	Sistemas Operativos Windows 10	AME-03.6	VUL-13	---	3,00	1	3	9,00	Medio
A64	Equipos PC	AME-04.13	VUL-12	---	2,33	4	2	18,67	Muy Alto
A65	Equipos PC	AME-03.11	VUL-08	---	2,33	4	2	18,67	Muy Alto

ANÁLISIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo
COD	Nombre Activo	Amenaza	Vulnerabilidad	Control implementado	CID	Nivel Amenaza	Nivel Vulnerabilidad		
A64	Equipos PC	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A65	Portátiles	AME-04.13	VUL-12	---	2,33	4	2	18,67	Muy Alto
A65	Portátiles	AME-04.9	VUL-07	---	2,33	1	4	9,33	Alto
A65	Portátiles	AME-03.10	VUL-16	---	2,33	1	1	2,33	Bajo
A65	Portátiles	AME-03.11	VUL-08	---	2,33	4	2	16,64	Muy Alto
A66	Internet	AME-03.10	VUL-16	---	2,67	3	2	16,02	Muy Alto
A66	Impresiones	AME-03.10	VUL-21	---	1,33	4	1	5,32	Medio
A66	Impresiones	AME-03.11	VUL-08	A15.2.1	2,00	2	1	4,00	Bajo

Fuente: Autor

Anexo F: Tratamiento al Riesgo.

El análisis del riesgo se realiza por cada activo validando un análisis costo beneficio y el apetito al riesgo para lo cual se toma una opción para la oportunidad o amenaza; además de la descripción de su riesgo residual.

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
		Impacto	Probabilidad de Ocurrencia							Probabilidad de Ocurrencia				
COD	Nombre Activo	CID	Amenaza	Vulnerabilidad	Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Amenaza	Vulnerabilidad	Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
A1	Router de frontera	2,00	1,00	1,00	2,00	Bajo	Aceptar	Control Preventivo	A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,00	Bajo	Residual
A1	Router de frontera	2,00	2,00	4,00	16,00	Muy Alto	Aceptar	Control Preventivo	A11.2.1	1,00	1,00	2,00	Bajo	Aceptable
A2	Core Cisco	3,00	1,00	4,00	12,00	Alto	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	3,00	Bajo	Residual
A2	Core Cisco	3,00	2,00	4,00	24,00	Muy Alto	Aceptar	Control Preventivo	A11.2.1	1,00	1,00	3,00	Bajo	Aceptable
A3	Firewall Cisco	3,00	1,00	4,00	12,00	Alto	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	3,00	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A3	Firewall Cisco	3,00	2,00	4,00	24,00	Muy Alto	Aceptar	Control Preventivo	A11.2.1	1,00	1,00	3,00	Bajo	Aceptable
A4	Wireless Controller	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4	1,00	1,00	2,33	Bajo	Residual
A4	Wireless Controller	2,33	2,00	2,00	9,33	Alto	Aceptar	Control Preventivo	A15.1.1	1,00	1,00	2,33	Bajo	Aceptable
A5	Sistema de Video Vigilancia	1,00	1,00	2,00	2,00	Bajo	Transferir	Control Preventivo	A15.1.2	1,00	1,00	1,00	Bajo	Residual
A5	Sistema de Video Vigilancia	1,00	2,00	2,00	4,00	Bajo	Aceptar	Control Preventivo	A15.1.3	1,00	1,00	1,00	Bajo	Aceptable
A6	Servidor Cisco 1	4,00	1,00	3,00	12,00	Alto	Transferir	Control Preventivo	A11.2.1	1,00	1,00	4,00	Bajo	Residual
A6	Servidor Cisco 1	4,00	2,00	4,00	32,00	Muy Alto	Aceptar	Control Preventivo	A11.2.4	1,00	1,00	4,00	Bajo	Aceptable
A7	Servidor Cisco 2	3,00	1,00	3,00	9,00	Medio	Transferir	Control Preventivo	A15.1.1	1,00	1,00	3,00	Bajo	Residual
A7	Servidor Cisco 2	3,00	2,00	4,00	24,00	Muy Alto	Aceptar	Control Preventivo	A15.1.2	1,00	1,00	3,00	Bajo	Aceptable
A8	Servidor IBM M3	3,00	1,00	2,00	6,00	Medio	Transferir	Control Preventivo	A15.1.3	1,00	1,00	3,00	Bajo	Residual
A8	Servidor IBM M3	3,00	2,00	1,00	6,00	Medio	Transferir	Control Correctivo	A11.2.1	1,00	1,00	3,00	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A9	Servidor IBM M4	3,00	1,00	2,00	6,00	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	3,00	Bajo	Residual
A9	Servidor IBM M4	3,00	2,00	1,00	6,00	Medio	Transferir	Control Correctivo	A8.1.1	1,00	1,00	3,00	Bajo	Residual
A10	PC / Servidor 1	1,67	1,00	2,00	3,33	Bajo	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	1,67	Bajo	Residual
A10	PC / Servidor 1	1,67	1,00	1,00	1,67	Bajo	Mitigar	Control Correctivo	A8.1.1	1,00	1,00	1,67	Bajo	Residual
A11	PC / Servidor 2	3,67	1,00	2,00	7,33	Medio	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	3,67	Bajo	Residual
A11	PC / Servidor 2	3,67	2,00	4,00	29,33	Muy Alto	Aceptar	Control Preventivo	A11.2.1	1,00	1,00	3,67	Bajo	Aceptable
A11	PC / Servidor 2	3,67	1,00	1,00	3,67	Bajo	Mitigar	Control Correctivo	A8.1.1	1,00	1,00	3,67	Bajo	Residual
A12	PC / Servidor 3	2,67	1,00	2,00	5,33	Medio	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	2,67	Bajo	Residual
A12	PC / Servidor 3	2,67	1,00	2,00	5,33	Medio	Mitigar	Control Correctivo	A8.1.1	1,00	1,00	2,67	Bajo	Residual
A13	PC / Servidor 4	3,00	1,00	2,00	6,00	Medio	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	3,00	Bajo	Residual
A13	PC / Servidor 4	3,00	1,00	2,00	6,00	Medio	Mitigar	Control Correctivo	A8.1.1	1,00	1,00	3,00	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A14	PC / Servidor 5	1,00	1,00	2,00	2,00	Bajo	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	1,00	Bajo	Residual
A14	PC / Servidor 5	1,00	3,00	1,00	3,00	Bajo	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	2,00	1,00	2,00	Medio	Residual
A14	PC / Servidor 5	1,00	1,00	1,00	1,00	Bajo	Mitigar	Control Correctivo	A8.1.1	1,00	1,00	1,00	Bajo	Residual
A15	PC / Servidor 6	3,00	1,00	2,00	6,00	Medio	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	3,00	Bajo	Residual
A15	PC / Servidor 6	3,00	3,00	2,00	18,00	Muy Alto	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	2,00	1,00	6,00	Medio	Residual
A15	PC / Servidor 6	3,00	1,00	1,00	3,00	Bajo	Mitigar	Control Correctivo	A8.1.1	1,00	1,00	3,00	Bajo	Residual
A16	PC / Servidor 7	1,00	1,00	2,00	2,00	Bajo	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	1,00	Bajo	Residual
A16	PC / Servidor 7	1,00	3,00	1,00	3,00	Bajo	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	2,00	1,00	2,00	Bajo	Residual
A16	PC / Servidor 7	1,00	1,00	1,00	1,00	Bajo	Mitigar	Control Correctivo	A8.1.1	1,00	1,00	1,00	Bajo	Residual
A17	MITEL Principal	2,00	3,00	2,00	12,00	Alto	Transferir	Control Preventivo	A11.2.4 A15.1.1	1,00	1,00	2,00	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO								
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A18	MITEL Secundario	1,67	3,00	2,00	10,00	Alto	Transferir	Control Preventivo	A15.1.2 A15.1.3 A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	1,67	Bajo	Residual
A19	Data Center 1	3,00	2,00	4,00	24,00	Muy Alto	Aceptar	Control Correctivo	A11.2.1	1,00	1,00	3,00	Bajo	Aceptable
A19	Data Center 1	3,00	3,00	2,00	18,00	Muy Alto	Mitigar	Control Preventivo	A17.1.1 A17.1.2 A17.1.3	3,00	1,00	9,00	Medio	Residual
A19	Data Center 1	3,00	4,00	4,00	48,00	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	3,00	Bajo	Residual
A20	Data Center 2	3,00	3,00	2,00	18,00	Muy Alto	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	2,00	1,00	6,00	Medio	Residual
A20	Data Center 2	3,00	4,00	2,00	24,00	Muy Alto	Mitigar	Control Preventivo	A17.1.1 A17.1.2 A17.1.3	3,00	1,00	9,00	Medio	Residual
A21	Nodo 1	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A21	Nodo 1	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A21	Nodo 1	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A22	Nodo 2	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A22	Nodo 2	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A22	Nodo 2	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A23	Nodo 3	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A23	Nodo 3	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A23	Nodo 3	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A24	Nodo 4	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A24	Nodo 4	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A24	Nodo 4	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A25	Nodo 5	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A25	Nodo 5	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A25	Nodo 5	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A26	Nodo 6	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A26	Nodo 6	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A26	Nodo 6	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A27	Nodo 7	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A27	Nodo 7	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A27	Nodo 7	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A28	Nodo 8	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A28	Nodo 8	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A28	Nodo 8	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A29	Nodo 9	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A29	Nodo 9	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A29	Nodo 9	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A30	Nodo 10	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A30	Nodo 10	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A30	Nodo 10	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A31	Nodo 11	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A31	Nodo 11	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A31	Nodo 11	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A32	Nodo 12	2,33	1,00	2,00	4,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A32	Nodo 12	2,33	1,00	1,00	2,33	Bajo	Transferir	Control Correctivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A32	Nodo 12	2,33	4,00	4,00	37,33	Muy Alto	Transferir	Control Correctivo	A11.1.2	1,00	1,00	2,33	Bajo	Residual
A33	Sistema Hosvital	3,67	2,00	2,00	14,67	Alto	Transferir	Control Preventivo	A15.1.1 A15.1.2 A15.1.3	1,00	1,00	3,67	Bajo	Aceptable

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A33	Sistema Hosvital	3,67	4,00	2,00	29,33	Muy Alto	Transferir	Control Correctivo	A15.1.1 A15.1.2 A15.1.3	1,00	1,00	3,67	Bajo	Aceptable
A33	Sistema Hosvital	3,67	3,00	1,00	11,00	Alto	Mitigar	Control Preventivo	A9.1.1 A9.2.2 A9.2.3 A9.2.6	1,00	1,00	3,67	Bajo	Residual
A33	Sistema Hosvital	3,67	2,00	1,00	7,33	Medio	Mitigar	Control Preventivo	A.11.2.4. A9.1.1 A9.2.2 A9.2.3 A9.2.6	1,00	1,00	3,67	Bajo	Residual
A33	Sistema Hosvital	3,67	1,00	4,00	14,67	Alto	Mitigar	Control Correctivo	A.11.2.4. A17.1.1 A17.1.2 A17.1.3	1,00	1,00	3,67	Bajo	Aceptable
A34	Sistema De talento Humano	2,33	2,00	2,00	9,33	Alto	Transferir	Control Preventivo	A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,33	Bajo	Residual
A34	Sistema De talento Humano	2,33	1,00	3,00	7,00	Medio	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	2,33	Bajo	Aceptable
A35	Sistema MS-PROG	1,00	2,00	2,00	4,00	Bajo	Aceptar	Control Preventivo	A11.2.4 A15.1.1	1,00	1,00	1,00	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO								
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A35	Sistema MS-PROG	1,00	1,00	2,00	2,00	Bajo	Mitigar	Control Correctivo	A15.1.2 A15.1.3 A17.1.1 A17.1.2 A17.1.3	1,00	1,00	1,00	Bajo	Aceptable
A36	Zimbra	2,67	2,00	2,00	10,67	Alto	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	2,67	Bajo	Residual
A36	Zimbra	2,67	1,00	4,00	10,67	Alto	Mitigar	Control Preventivo	A12.3.1 A17.1.1 A17.1.2 A17.1.3	1,00	1,00	2,67	Bajo	Residual
A36	Zimbra	2,67	3,00	4,00	32,00	Muy Alto	Mitigar	Control Preventivo	A.11.2.4 A13.2.4	1,00	3,00	8,00	Medio	Aceptable
A36	Zimbra	2,67	1,00	2,00	5,33	Medio	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	2,67	Bajo	Aceptable
A37	Jaspersoft	1,00	1,00	1,00	1,00	Bajo	Aceptar	Control Preventivo	A11.2.4	1,00	1,00	1,00	Bajo	Residual
A37	Jaspersoft	1,00	1,00	1,00	1,00	Bajo	Aceptar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	1,00	Bajo	Aceptable

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO								
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A38	Sistema de Marcaciones	3,33	1,00	2,00	6,67	Medio	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	3,33	Bajo	Residual
A38	Sistema de Marcaciones	3,33	1,00	2,00	6,67	Medio	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	3,33	Bajo	Aceptable
A39	Sistema SERCOP	1,00	1,00	1,00	1,00	Bajo	Aceptar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	1,00	Bajo	Aceptable
A40	Wireless Controller	1,67	1,00	2,00	3,33	Bajo	Mitigar	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	1,67	Bajo	Residual
A41	Sistema Video vigilancia BOSCH	1,67	1,00	2,00	3,33	Bajo	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	1,67	Bajo	Residual
A42	Proxy 3	1,67	1,00	2,00	3,33	Bajo	Aceptar	Control Preventivo	A11.2.4	1,00	1,00	1,67	Bajo	Residual
A43	Proxy 5	1,67	1,00	2,00	3,33	Bajo	Aceptar	Control Preventivo	A11.2.4	1,00	1,00	1,67	Bajo	Residual
A44	Proxy 56	1,67	1,00	2,00	3,33	Bajo	Aceptar	Control Preventivo	A11.2.4	1,00	1,00	1,67	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A45	Server Red Hat 1	2,33	1,00	2,00	4,67	Medio	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	2,33	Bajo	Residual
A45	Server Red Hat 1	2,33	2,00	4,00	18,67	Muy Alto	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	2,33	Bajo	Aceptable
A46	Server Red Hat 2	2,33	1,00	2,00	4,67	Medio	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	2,33	Bajo	Residual
A46	Server Red Hat 2	2,33	2,00	4,00	18,67	Muy Alto	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	2,33	Bajo	Aceptable
A47	Server Red Hat 3	2,33	1,00	2,00	4,67	Medio	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	2,33	Bajo	Residual
A47	Server Red Hat 3	2,33	2,00	4,00	18,67	Muy Alto	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	2,33	Bajo	Aceptable
A48	Server Red Hat 4	2,33	1,00	2,00	4,67	Medio	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	2,33	Bajo	Residual
A48	Server Red Hat 4	2,33	2,00	4,00	18,67	Muy Alto	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	2,33	Bajo	Aceptable
A49	Laboratorio	1,67	1,00	2,00	3,33	Bajo	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	1,67	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A49	Laboratorio	1,67	2,00	2,00	6,67	Medio	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	1,67	Bajo	Residual
A50	Sistema MITEL	1,33	3,00	2,00	8,00	Medio	Mitigar	Control Preventivo	A11.2.4	3,00	1,00	4,00	Bajo	Residual
A50	Sistema MITEL	1,33	4,00	2,00	10,67	Alto	Mitigar	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	1,33	Bajo	Aceptable
A51	Base de Datos Hosvital	4,00	3,00	4,00	48,00	Muy Alto	Mitigar	Control Preventivo	A12.3.1	1,00	1,00	4,00	Bajo	Residual
A51	Base de Datos Hosvital	4,00	2,00	2,00	16,00	Muy Alto	Transferir	Control Preventivo	A11.2.4 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	4,00	Bajo	Aceptable
A51	Base de Datos Hosvital	4,00	1,00	4,00	16,00	Muy Alto	Mitigar	Control Correctivo	A17.1.1 A16.1.1	1,00	1,00	4,00	Bajo	Aceptable
A52	Base de Datos Sistema de Talento Humano	4,00	2,00	4,00	32,00	Muy Alto	Mitigar	Control Preventivo	A12.3.1	1,00	1,00	4,00	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A52	Base de Datos Sistema de Talento Humano	4,00	1,00	3,00	12,00	Alto	Mitigar	Control Correctivo	A17.1.1 A16.1.1	1,00	1,00	4,00	Bajo	Residual
A53	Base de Datos MSPROG	2,67	1,00	4,00	10,67	Alto	Mitigar	Control Preventivo	A12.3.1	1,00	1,00	2,67	Bajo	Residual
A53	Base de Datos MSPROG	2,67	2,00	3,00	16,00	Muy Alto	Mitigar	Control Correctivo	A17.1.1 A16.1.1	1,00	1,00	2,67	Bajo	Aceptable
A54	Base de Datos Sistema de Marcaciones	4,00	2,00	4,00	32,00	Muy Alto	Mitigar	Control Preventivo	A12.3.1	1,00	1,00	4,00	Bajo	Residual
A54	Base de Datos Sistema de Marcaciones	4,00	1,00	3,00	12,00	Alto	Mitigar	Control Correctivo	A17.1.1 A16.1.1	1,00	1,00	4,00	Bajo	Aceptable
A55	Base de Datos Laboratorio	3,00	1,00	4,00	12,00	Alto	Mitigar	Control Preventivo	A12.3.1	1,00	1,00	3,00	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A55	Base de Datos Laboratorio	3,00	1,00	3,00	9,00	Medio	Mitigar	Control Correctivo	A17.1.1 A16.1.1	1,00	1,00	3,00	Bajo	Aceptable
A56	PC 1	1,33	1,00	2,00	2,67	Bajo	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	1,33	Bajo	Residual
A56	PC 1	1,33	1,00	1,00	1,33	Bajo	Mitigar	Control Preventivo	A8.1.1	1,00	1,00	1,33	Bajo	Residual
A57	Portátil 1	2,00	1,00	2,00	4,00	Bajo	Mitigar	Control Preventivo	A11.2.4	1,00	1,00	2,00	Bajo	Residual
A57	Portátil 1	2,00	1,00	1,00	2,00	Bajo	Mitigar	Control Preventivo	A8.1.1	1,00	1,00	2,00	Bajo	Residual
A57	Portátil 1	2,00	2,00	4,00	16,00	Muy Alto	Mitigar	Control Preventivo	A8.1.1 A8.1.2 A8.1.3 A8.1.4	1,00	2,00	4,00	Bajo	Residual
A58	Administrador de Sistema Hosvital	3,00	4,00	1,00	12,00	Alto	Mitigar	Control Correctivo	A7.2.1	1,00	1,00	3,00	Bajo	Residual
A59	Administrador de Sistemas	2,00	1,00	1,00	2,00	Medio	Mitigar	Control Preventivo	A7.2.1	1,00	1,00	2,00	Bajo	Residual
A60	Analista de Redes	3,33	2,00	4,00	26,67	Muy Alto	Mitigar	Control Preventivo	A7.2.1	1,00	1,00	3,33	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO							
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A61	Responsable de la Seguridad de la Información	3,33	1,00	4,00	13,33	Alto	Mitigar	Control Preventivo	A6.1.1 A7.2.1	1,00	1,00	3,33	Bajo	Residual
A62	Antivirus corporativo	3,00	1,00	3,00	9,00	Medio	Transferir	Control Preventivo	A12.2.1 A15.1.1 A15.1.2 A15.1.3	1,00	1,00	3,00	Bajo	Residual
A63	Sistemas Operativos Windows 10	3,00	1,00	3,00	9,00	Medio	Transferir	Control Preventivo	A15.1.1 A15.1.2 A15.1.3	1,00	1,00	3,00	Bajo	Residual
A64	Equipos PC	2,33	4,00	2,00	18,67	Muy Alto	Mitigar	Control Preventivo	A9.1.1 A9.2 A9.3 A11.2.7	1,00	1,00	2,33	Bajo	Residual
A64	Equipos PC	2,33	4,00	2,00	18,67	Muy Alto	Mitigar	Control Preventivo	A11.2.4	3,00	1,00	7,00	Medio	Residual
A64	Equipos PC	2,33	1,00	1,00	2,33	Bajo	Mitigar	Control Preventivo	A8.1.1	1,00	1,00	2,33	Bajo	Residual
A65	Portátiles	2,33	4,00	2,00	18,67	Muy Alto	Mitigar	Control Preventivo	A9.1.1 A9.2 A9.3	1,00	1,00	2,33	Bajo	Residual

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO								
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A65	Portátiles	2,33	1,00	4,00	9,33	Alto	Mitigar	Control Preventivo	A11.2.7 A12.6.2 A12.7.1 A6.2.1 A8.1.1 A8.1.2 A8.1.3 A8.1.4 A11.2.5 A11.2.6 A11.2.7 A11.2.8 A11.2.9	1,00	2,00	4,67	Medio	Residual
A65	Portátiles	2,33	1,00	1,00	2,33	Bajo	Aceptar	Control Preventivo	A8.1.1	1,00	1,00	2,33	Bajo	Aceptable
A65	Portátiles	2,33	4,00	2,00	18,67	Muy Alto	Mitigar	Control Preventivo	A11.2.4	3,00	1,00	7,00	Medio	Aceptable
A66	Internet	2,67	3,00	2,00	16,00	Muy Alto	Transferir	Control Correctivo	A17.1.1 A17.1.2 A17.1.3	1,00	1,00	2,67	Bajo	Residual
A67	Impresiones	1,33	4,00	1,32	5,32	Medio	Aceptar	Control Preventivo	A8.1.2 A8.1.3	1,00	1,00	1,00	Bajo	Aceptable

EVALUACIÓN DEL RIESGO							TRATAMIENTO DEL RIESGO								
COD	Nombre Activo	Impacto	Probabilidad de Ocurrencia		Evaluación riesgos	Nivel de riesgo	Método de tratamiento de riesgos	Tipo de control	Control a implementar	Probabilidad de Ocurrencia		Cálculo evaluación riesgos	Nivel de riesgo	Riesgo Residual
		CID	Amenaza	Vulnerabilidad						Amenaza	Vulnerabilidad			
A67	Impresiones	2,00	2,00	1,00	4,00	Bajo	Transferir	Control Preventivo	A15.1.1 A15.1.2 A15.1.3	1,00	1,00	1,00	Bajo	Aceptable

Fuente: Autor

Anexo G: Declaración de Aplicabilidad

La declaración de aplicabilidad se elabora con base al análisis y tratamiento a los riesgos considerando los planes de acción a implementar para cerrar las brechas identificadas de la implementación para la seguridad de la información en el Hospital FIB.

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
5. Políticas de Seguridad									
5.1	**Dirección de la alta gerencia para la seguridad de la información**								
5.1.1	Políticas de seguridad de la información			Si			X		Elaborar un SGSI que contenga las políticas de seguridad.
5.1.2	Revisión de las políticas de seguridad de la información			Si			X		Elaborar un SGSI, que contenga las políticas de seguridad para un adecuada mejora continua.
6. Organización de la Seguridad de la Información									
6.1	**Organización interna**								
6.1.1	Roles y responsabilidad de seguridad de la información			Si				X	Determinar responsabilidades con la alta gerencia para determinar roles de la seguridad de la información.
6.1.2	Segregación de deberes			No					
6.1.3	Contacto con autoridades			No					
6.1.4	Contacto con grupos de interés especial			No					
6.1.5	Seguridad de la información en la gestión de proyectos			No					

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
6.2	**Dispositivos móviles y teletrabajo**								
6.2.1	Política de dispositivos móviles			Si				X	Elaborar políticas para el ingreso, configuración y uso de equipos para reducir los riesgos de conexión de los activos.
6.2.2	Teletrabajo			No					
7. Seguridad en los Recursos Humanos									
7.1	**Previo al empleo**								
7.1.1	Verificación de antecedentes	Si							
7.1.2	Términos y condiciones del empleo			Si				X	Contratar personal con perfil y cumplan con las condiciones relacionadas con la seguridad.
7.2	**Durante el empleo**								
7.2.1	Responsabilidades de la Gestión			Si	X			X	Determinar actividades asignadas en el manual de clasificación de puestos del Ministerio de Salud para Hospitales de > 200 camas.
7.2.2	Conciencia, educación y entrenamiento de seguridad de la información			Si				X	Elaborar plan de capacitación al personal en coordinación con Dirección de Talento Humano.
7.2.3	Proceso disciplinario			No					
7.3	**Terminación y cambio de empleo**								
7.3.1	Termino de responsabilidades o cambio de empleo			Si				X	Elaborar procedimiento para la gestión de usuarios en los diferentes sistemas informáticos.

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
8.	**Gestión de Activos**								
8.1	**Responsabilidad de los activos**								
8.1.1	Inventario de activos			Si				X	Elaborar planificación anual de comprobación de inventarios de equipos tecnológicos.
8.1.2	Propiedad de activos			Si				X	Elaborar políticas para la gestión de activos acorde a la políticas de seguridad.
8.1.3	Uso aceptable de los activos			Si				X	Elaborar políticas para la gestión de activos acorde a la políticas de seguridad.
8.1.4	Devolución de activos			Si				X	Elaborar políticas para la gestión de activos acorde a la políticas de seguridad.
8.2	**Clasificación de la información**								
8.2.1	Clasificación de la información			Si				X	Elaborar políticas para la gestión de activos acorde a la políticas de seguridad.
8.2.2	Etiquetado de la información			Si				X	Elaborar políticas para la gestión de activos acorde a la políticas de seguridad.
8.2.3	Manejo de activos			Si				X	Elaborar políticas para la gestión de activos acorde a la políticas de seguridad.
8.3	**Manejo de medios**								
8.3.1	Gestión de medios removibles			Si				X	Elaborar políticas para la gestión de dispositivos móviles y portátiles.
8.3.2	Eliminación de medios			No					

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
8.3.3	Transporte de medios físicos			No					
9. Control de Acceso									
9.1	**Requerimientos de negocio para el control de acceso**								
9.1.1	Política de control de acceso			Si				X	Elaborar procedimiento para gestión de usuarios en los diferentes sistemas informáticos.
9.1.2	Acceso a redes y servicios de red			No					
9.2	**Gestión de accesos de usuario**								
9.2.1	Registro y baja del usuario	Si							
9.2.2	Provisión de acceso a usuarios			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.2.3	Gestión de derechos de acceso privilegiados			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.2.4	Gestión de información de autenticación secreta de usuarios			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.2.5	Revisión de derechos de acceso de usuarios			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.2.6	Eliminación o ajuste de derechos de acceso			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.3	**Responsabilidades del usuario**								
9.3.1	Uso de información de autenticación secreta			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.4	**Control de acceso de sistemas y aplicaciones**								
9.4.1	Restricción de acceso a la información			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.4.2	Procedimientos de inicio de sesión seguro			Si				X	Elaborar de procedimiento para la gestión de usuarios.

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
9.4.3	Sistema de gestión de contraseñas			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.4.4	Uso de programas y utilidades privilegiadas			Si				X	Elaborar de procedimiento para la gestión de usuarios.
9.4.5	Control de acceso al código fuente del programa			No					
10.	**Criptografía**								
10.1	**Controles criptográficos**								
10.1.1	Política en el uso de controles criptográficos			No					
10.1.2	Gestión de llaves			No					
11.	**Seguridad Física y del Entorno**								
11.1	**Áreas seguras**								
11.1.1	Perímetro de seguridad físico			Si	X			X	Establecer procedimiento para el registro de acceso a las áreas restringidas de TIC de acuerdo a las funciones del personal.
11.1.2	Controles físicos de entrada			Si	X			X	Control de acceso de usuario en las áreas sensibles de TIC con la implementación de biométricos.
11.1.3	Seguridad de oficinas, habitaciones y facilidades			No					
11.1.4	Protección contra amenazas externas y del ambiente			Si				X	Elaborar plan para la continuidad para los servicios tecnológicos ante cualquier incidente.
11.1.5	Trabajo en áreas seguras			No					
11.1.6	Áreas de entrega y carga	Si							

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
11.2	**Equipo**								
11.2.1	Instalación y protección de equipo			Si				X	Establecer procedimiento para gestión de equipos tecnológicos y minimizar accesos no autorizados.
11.2.2	Servicios de soporte	Si							
11.2.3	Seguridad en el cableado			Si	X			X	Establecer procedimientos para control de acceso.
11.2.4	Mantenimiento de equipos			Si				X	Establecer procedimiento para la gestión de equipos tecnológicos.
11.2.5	Retiro de activos			Si				X	Elaborar política para la gestión de activos para el retiro de personal interno y externo.
11.2.6	Seguridad del equipo y activos fuera de las instalaciones			Si				X	Establecer procedimiento para la gestión de equipos tecnológicos.
11.2.7	Eliminación segura o re-uso del equipo			Si				X	Establecer procedimiento para la gestión de equipos tecnológicos para la reutilización de activos y eliminación de la información.
11.2.8	Equipo de usuario desatendido			Si				X	Establecer procedimiento para la gestión de equipos tecnológicos.
11.2.9	Política de escritorio limpio y pantalla limpia			Si				X	Establecer procedimiento para la gestión de equipos tecnológicos.
12.	**Seguridad en las Operaciones**								
12.1	**Procedimientos Operacionales y Responsabilidades**								
12.1.1	Documentación de procedimientos operacionales			No					
12.1.2	Gestión de cambios			No					
12.1.3	Gestión de la capacidad			No					

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No	El desarrollo de software y/o aplicativos no se tiene procesos establecidos.						
12.2	**Protección de Software Malicioso**								
12.2.1	Controles contra software malicioso			Si			X		Protección con malware para la administración de antivirus corporativo y controles que prohíban el uso de software no autorizado.
12.3	**Respaldo**								
12.3.1	Respaldo de información			Si	X		X		Establecer políticas de respaldo para el software y hardware.
12.4	**Bitácoras y monitoreo**								
12.4.1	Bitácoras de eventos			No					
12.4.2	Protección de información en bitácoras			No					
12.4.3	Bitácoras de administrador y operador			No					
12.4.4	Sincronización de relojes			No					
12.5	**Control de software operacional**								
12.5.1	Instalación de software en sistemas operacionales	No	El desarrollo de software no están dentro de los procesos establecidos para la Gestión de TIC o son desarrollados por terceros.						
12.6	**Gestión de vulnerabilidades técnicas**								

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
12.6.1	Gestión de vulnerabilidades técnicas			No					
12.6.2	Restricciones en la instalación de software			Si				X	Elaborar política de gestión de software.
12.7	**Consideraciones de auditoria de sistemas de información**								
12.7.1	Controles de auditoría de sistemas de información			Si				X	Elaborar política de gestión de software.
13.	**Seguridad de las Comunicaciones**								
13.1	**Gestión de seguridad en red**								
13.1.1	Controles de red			Si			X		Elaborar política de uso de red alámbrica e inalámbrica; además de controles y procedimientos para las configuraciones de los dispositivos.
13.1.2	Seguridad en los servicios en red			No					
13.1.3	Segregación en redes			No					
13.2	**Transferencia de información**								
13.2.1	Políticas y procedimientos para la transferencia de información			No					
13.2.2	Acuerdos en la transferencia de información			No					
13.2.3	Mensajería electrónica			Si				X	Elaborar políticas de Seguridad sobre uso del correo institucional para el intercambio de información.
13.2.4	Acuerdos de confidencialidad o no-revelación			Si	X			X	Elaborar acuerdos de confidencialidad para uso de

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
									medios electrónicos e información confidencial.
14.	**Adquisición, Desarrollo y Mantenimiento de los Sistemas**								
14.1	**Requerimientos de seguridad en sistemas de información**								
14.1.1	Análisis y especificación de requerimientos de seguridad			Si			X		Elaborar política de gestión de software.
14.1.2	Aseguramiento de servicios de aplicación en redes públicas	No	Página web institucional es tipo informativa; esta no realiza algún tipo de comercio electrónico.						
14.1.3	Protección de transacciones en servicios de aplicación	No	No se realiza transacciones en las aplicaciones que usa el hospital.						
14.2	**Seguridad en el proceso de desarrollo y soporte**								
14.2.1	Política de desarrollo seguro	No	El desarrollo de software y/o aplicativos no están dentro de los procesos establecidos del departamento de TIC o por terceros.						
14.2.2	Procedimientos de control de cambios del sistema			No					
14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa			No					
14.2.4	Restricción de cambios en paquetes de software			No					
14.2.5	Principios de seguridad en la ingeniería de sistemas	No	El desarrollo de software y/o aplicativos no están dentro						

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
			de los procesos establecidos del departamento de TIC o terceros.						
14.2.6	Entorno de desarrollo seguro	No	El desarrollo de software y/o aplicativos no están dentro de los procesos establecidos para la Gestión de TIC o por terceros.						
14.2.7	Externalización del desarrollo de software			No					
14.2.8	Pruebas de seguridad del sistema			Si			X		Establecer términos de referencia al software de terceros las respectivas pruebas e informe de seguridad del sistema.
14.2.9	Pruebas de aceptación del sistema			Si			X		Establecer términos de referencia al software de terceros las respectivas pruebas.
14.3	**Datos de prueba**								
14.3.1	Protección de datos de prueba	No	No hay ambiente de pruebas de los aplicativos instalados debidos que es software de terceros instalados.						
15.	**Relaciones con Proveedores**								
15.1	**Seguridad de la información en relaciones con el proveedor**								
15.1.1	Política de seguridad de la información en las relaciones con el proveedor			Si				X	Establecer políticas para el ingreso, configuración y uso de equipos que no pertenezcan a la institución.

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor			Si				X	Establecer políticas para el ingreso, configuración y uso de equipos que no pertenezcan a la institución.
15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones			Si				X	Establecer políticas para el ingreso, configuración y uso de equipos que no pertenezcan a la institución.
15.2	**Gestión de entrega de servicios de proveedor**								
15.2.1	Monitoreo y revisión de servicios del proveedor	Si							
15.2.2	Gestión de cambios a los servicios del proveedor	No	No se efectúan cambios en los contratos de servicios con los proveedores.						
16. Gestión de Incidentes de Seguridad de la Información									
16.1	**Gestión de incidentes de seguridad de la información y mejoras**								
16.1.1	Responsabilidad y procedimientos			Si				X	Elaborar procedimiento para para el registro y gestión de incidentes de seguridad.
16.1.2	Reporte de eventos de seguridad de la información			Si				X	Elaborar procedimiento para para el registro y gestión de incidentes de seguridad.
16.1.3	Reporte de debilidades de seguridad de la información			Si				X	Elaborar procedimiento para para el registro y gestión de incidentes de seguridad.
16.1.4	Valoración y decisión de eventos de seguridad de la información			Si				X	Elaborar procedimiento para para el registro y gestión de incidentes de seguridad.

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
16.1.5	Respuesta a incidentes de seguridad de la información			Si				X	Elaborar procedimiento para para el registro y gestión de incidentes de seguridad.
16.1.6	Aprendizaje de incidentes de seguridad de la información			Si				X	Elaborar procedimiento para para el registro y gestión de incidentes de seguridad.
16.1.7	Colección de evidencia			No					
17.	**Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio**								
17.1	**Continuidad de la seguridad de la información**								
17.1.1	Planeación de la continuidad de la seguridad de la información			Si				X	Elaborar plan para la continuidad de la seguridad de la información de servicios tecnológicos ante cualquier incidente.
17.1.2	Implementación de la continuidad de la seguridad de la información			Si				X	Elaborar plan para la continuidad de la seguridad de la información de servicios tecnológicos ante cualquier incidente.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información			Si				X	Elaborar plan para la continuidad de la seguridad de la información de servicios tecnológicos ante cualquier incidente.
17.2	**Redundancias**								
17.2.1	Disponibilidad de facilidades de procesamiento de información			Si				X	Elaborar plan para la continuidad de la seguridad de la información de servicios tecnológicos ante cualquier incidente.
18.	**Cumplimiento**								

ISO 27001:2013		Control actual	Justificación de exclusión	Control a Implementar (Si/No)	Razones de selección				Plan de acción
Dominio	Objetivo de control				LR	CO	BR/BP	RRA	
18.1 Cumplimiento con Requerimientos Legales y Contractuales									
18.1.1	Identificación de legislación aplicable y requerimientos contractuales			Si	X				Cumplir con la Ley Orgánica de Salud.
18.1.2	Derechos de propiedad intelectual (IPR)			No					
18.1.3	Protección de registros			No					
18.1.4	Privacidad y protección de información personal identificable (PIR)			Si	X				Velar con el cumplimiento de normas como la Ley Orgánica de Salud.
18.1.5	Regulación de controles criptográficos			No					
18.2	**Revisiones de seguridad de la información**								
18.2.1	Revisión independiente de seguridad de la información			No					
18.2.2	Cumplimiento con políticas y estándares de seguridad			SI			X		Elaborar un SGSI de la empresa, que contenga las políticas y control de seguridad.
18.2.3	Revisión del cumplimiento técnico			No					

Fuente: Autor