FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE HONDURAS CON BASE EN ISO 27001 CASO DE ESTUDIO HOSPITAL MARIA ESPECIALIDADES PEDIÁTRICAS

SUSTENTADO POR:
EDDSON JERICK GUEVARA AGUILERA

PREVIA INVESTIDURA AL TÍTULO DE
MÁSTER EN DIRECCIÓN DE MERCADOTECNIA

TEGUCIGALPA, F. M., **HONDURAS, C.A.**

JULIO, 2017

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

MARLON ANTONIO BREVÉ REYES

SECRETARIO GENERAL

ROGER MARTINEZ MIRALDA

DECANO DE LA FACULTAD DE POSTGRADO

JOSE ARNOLDO SERMEÑO LIMA

LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE HONDURAS CON BASE EN ISO 27001 CASO DE ESTUDIO HOSPITAL MARIA ESPECIALIDADES PEDIÁTRICAS

MÁSTER EN DIRECCIÓN DE MERCADOTECNIA

ASESOR METODOLÓGICO

ELOISA RODRIGUEZ

ASESOR TEMÁTICO

LORENA GUADALUPE ARANA CANALES

MIEMBROS DE LA TERNA (O COMISIÓN EVALUADORA):

MINA CECILIA GARCIA

JORGE MARADIAGA

FACULTAD DE POSTGRADO

LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE HONDURAS CON BASE EN ISO 27001
CASO DE ESTUDIO HOSPITAL MARIA ESPECIALIDADES PEDIÁTRICAS

EDDSON JERICK GUEVARA AGUILERA

Resumen

La presente investigación tiene como objetivo determinar la garantía de la seguridad de los pacientes del Hospital María Especialidades Pediátricas. Para esto se analizó la situación actual del hospital en lo referente a seguridad de la información y con los datos obtenidos se realizó un análisis y evaluación de riegos, con una visión y criterios propios, aplicando la metodología dictada por la normativa ISO 27001. Finalmente se desarrolló la aplicabilidad de la metodología al caso de estudio y se propuso un manual de seguridad de la información que servirá de guía para la implementación de un sistema de gestión de seguridad de la información (SGSI) con el que se puedan controlar y prevenir futuros incidentes, garantizando de esta manera la confidencialidad, integridad y disponibilidad de la información.

Palabras clave: Análisis, Información, ISO, Riesgos, Seguridad, Sistema.

GRADUATE SCHOOL

THE SECURITY OF INFORMATION IN HONDURAN COMPANIES BASED ON ISO 27001
STUDY CASE: HOSPITAL MARIA ESPECIALIDADES PEDIÁTRICAS

EDDSON JERICK GUEVARA AGUILERA

Abstract

The present research aims to determine the guarantee of the information security of the patients of the Hospital María Especialidades Pediátricas. For this, the current situation of the hospital was analyzed in terms of InfoSec. With the data obtained, an analysis and evaluation of risks were made, with a vision and own criteria, applying the methodology dictated by ISO 27001. Finally, developed the applicability of the methodology to the case study and proposed an information security manual that will guide the implementation of an information security management system (ISMS) with which to control and prevent future incidents, thus guaranteeing the confidentiality, integrity and availability of the information.

Keywords: Analysis, Information, ISO, Risks, Security, System.

Dedicatoria

Primeramente, a Dios, dador de la sabiduría y el conocimiento y a quien debo todos los logros de mi vida.

A mi esposa quien ha sido un pilar fundamental y apoyo moral para la realización de este proyecto y por ayudarme en el cumplimiento de una meta trazada años atrás.

A mis padres por su apoyo incondicional en todos mis proyectos.

A mis hijos por su paciencia durante este periodo en el que estuve concentrado en este trabajo.

Agradecimientos

A la licenciada Lorena Arana, por su tiempo y disponibilidad para la revisión de esta investigación y por su apoyo para la realización de la misma.

Al Hospital María Especialidades Pediátricas por permitirme realizar la investigación dentro de sus instalaciones.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS Y GRÁFICOS

1 CAPÍTULO 1

INTRODUCCIÓN E INFORMACIÓN GENERAL

1.1 Introducción

En la actualidad, la seguridad de la información se constituye como una de las áreas más importantes de la informática ya qué además de proveer protección de los activos tecnológicos, se ha considerado como una herramienta que proporciona ventaja competitiva a una empresa en comparación con otras del mismo rubro. Precisamente por tener esta ventaja, las organizaciones se centran en generar valor dejando de lado el tema de la seguridad, lo que las pone en una situación comprometedora, propensas a fugas o robos de información, situación de la cual sus competidores podrían hacer uso y obtener una ventaja.

En las organizaciones estos escenarios se presentan de manera cotidiana, la información deja de ser confidencial y esto se vuelve un problema muy serio. Por ejemplo ¿Qué sucedería si un hospital pierde el servidor en el que se almacena la historia clínica de sus pacientes? O ¿Qué pasaría si su base de datos es secuestrada? Si la organización no cuenta con una estrategia definida la ocurrencia de uno o más de estos escenarios podría llevarla al colapso total.

Con el objetivo primordial de contribuir con el Hospital María Especialidades Pediátricas (HMEP), se realizó esta investigación que consiste en la aplicación de un estándar internacional especializado en seguridad de la información, a través del cual se identificaran e implementaran todos los controles de seguridad necesarios para la salvaguardia de la información considerada como confidencial.

1.2 Definición del Problema

La definición del problema se realiza a través de un enunciado del problema, la formulación del problema y las preguntas de investigación, las cuales se describen a continuación:

1.3 Enunciado del Problema

Actualmente, el Hospital María Especialidades Pediátricas no cuenta con un sistema de seguridad de la información que le permita atender y mitigar los incidentes, riesgos y amenazas a las que se ve expuesta su información, por lo que la confidencialidad, integridad y disponibilidad de esta, se ve comprometida ante posibles ataques informáticos.

Existen algunos controles establecidos por el departamento de Tecnologías de la Información y Comunicaciones, pero es necesaria la implementación de un sistema, lineamientos y buenas prácticas que garanticen la seguridad de la información de la organización.

1.4 Formulación del problema

¿Cómo identificar las vulnerabilidades, amenazas y riesgos que afectan la seguridad de la información del Hospital María Especialidades Pediátricas, con el fin implementar a futuro un sistema de seguridad que garantice la seguridad de la información de los pacientes?

1.5 Preguntas de Investigación

¿Cómo garantiza actualmente la seguridad de la información de sus pacientes el Hospital María especialidades Pediátricas?

¿Cuáles son los lineamientos actuales de la seguridad de la información dentro del hospital?

¿Cuáles son los riesgos y amenazas de no poseer una estructura o un sistema de seguridad de la información y como se pueden combatir?

1.6 Objetivos del proyecto

Los objetivos que se ambiciona lograr con el desarrollo de esta investigación son los siguientes:

1.6.1 Objetivo General

Determinar la garantía de la seguridad de la información de los clientes (pacientes) del Hospital María Especialidades Pediátricas.

1.6.2 Objetivos específicos

1. Implementar una política de seguridad de la información para el Hospital María.
2. Identificar las amenazas y las vulnerabilidades existentes en el Hospital, en cuanto a seguridad de la información se refiere y recomendar los controles necesarios.
3. Elaborar un manual de seguridad de la información basado en ISO27001, que se pueda implementar dentro de la organización y que considere una posible certificación en el futuro.

1.7 Justificación

En la actualidad, el Hospital María Especialidades Pediátricas es poseedor de una infraestructura tecnológica en proceso de crecimiento y robustecimiento. En esta infraestructura está basado el funcionamiento muchos procesos del área administrativa y de la gestión clínica. La mayoría de la información de estas áreas es almacenada en los sistemas de información, formatos físicos y otros medios, pero es visible la falencia en el tema de controles y lineamientos que garanticen en un 100% la salvaguardia de un activo tan importante como la información.

Por lo anteriormente expuesto, es conveniente que la organización considere el establecimiento e implementación de un sistema de seguridad de la información que le permita asegurar el flujo de información y garantizar la confidencialidad, disponibilidad e integridad de la misma.

Esta investigación propone la creación de un nuevo instrumento que ayudará a la organización a identificar los riesgos a los que se expone su información y la manera de tratarlos adecuadamente mediante el establecimiento de controles que permitan la adopción de buenas prácticas de seguridad que contribuyan con los objetivos institucionales. Adicionalmente la implementación de este sistema, permitirá tener una guía para la mitigación de riesgos y amenazas, que, de no ser tratadas de la manera correcta, pueden derivar en un problema legal o que afecte la imagen y reputación del hospital.

Esta investigación plantea una metodología para el establecimiento de un sistema de seguridad de la información, que si bien es cierto está orientada al análisis de un hospital, puede ser adoptada por otra instituciones o empresas que deseen aplicarlo, ya que la normativa empleada, tiene controles que pueden llamarse genéricos y pueden ser adecuados a las distintas organizaciones sin importar el rubro del negocio.

2 CAPÍTULO 2

MARCO TEÓRICO

2.1 Antecedentes:

Hace no muchos años atrás, antes de la invención de las primeras computadoras y sistemas de redes, toda la información importante de una organización o compañía debía ser almacenada en un formato físico, es decir, cuartos, almacenes o bodegas con una gran cantidad de archivadores eran los encargados de guardar todos los datos incluyendo la información financiera de una empresa.

Hoy en día como resultado de los avances tecnológicos de este siglo que las empresas tienen a su alance y adicionalmente la gran cantidad de información que se produce a diario, esta es digitalizada y guardada en dispositivos de almacenamiento como memorias USB, discos duros externos o dentro de un servidor que puede ocupar un espacio muy reducido en la empresa. Dados estos avances tecnológicos, actualmente las organizaciones conceden acceso a sus colaboradores, proveedores y socios estratégicos a sus sistemas de información, lo que, aunado a dichos avances, trae como consecuencia un problema al mundo informático de las empresas y este es, que la información digital, es más fácil ubicar y de transportar, lo que aumenta las probabilidades de robo y modificación. Por tal motivo es necesario conocer al detalle que recursos deben ser protegidos y controlados y es imperante que toda esta información sea manipulada de la mejor manera posible clasificándola como uno de los activos más valiosos dentro de la organización.

Debido al auge del internet y al crecimiento de los delitos informáticos en el mundo, algunas organizaciones en diferentes países se están preocupando cada vez más por el tema de la

seguridad de la información, adoptando el estándar ISO 27001 como mecanismo de gestión de seguridad de la información, tal como se puede observar en la siguiente figura:

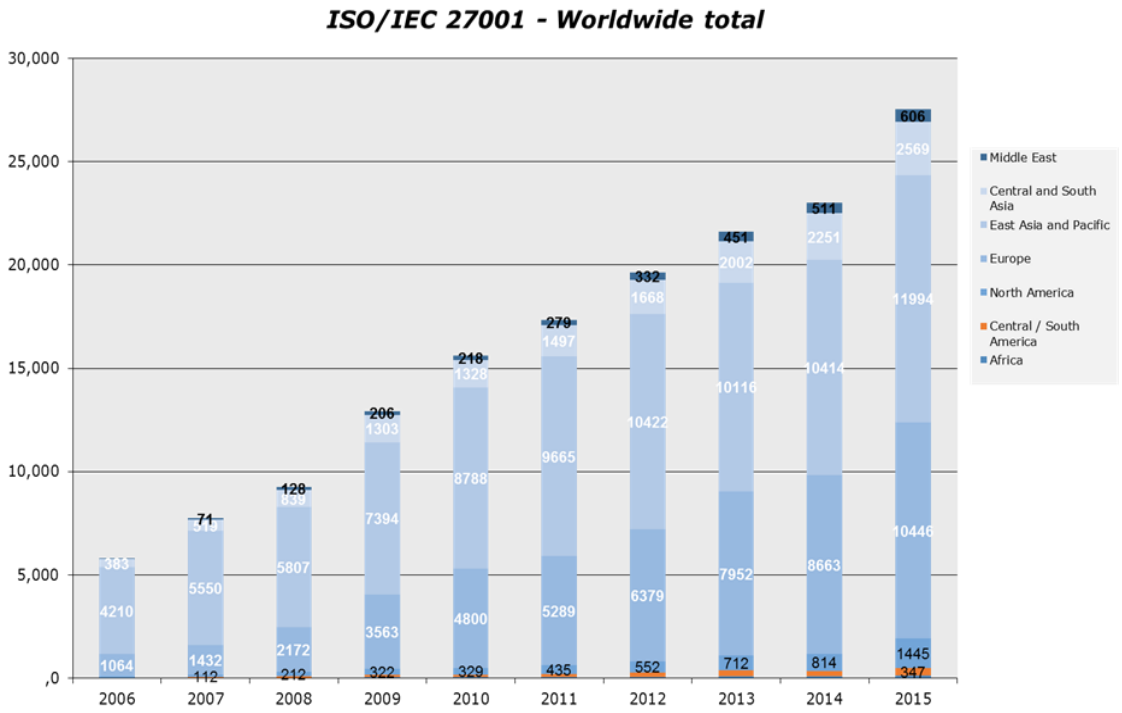


Figura 1: Certificados ISO/IEC 27001 a nivel mundial

Fuente: (Organización Internacional para la estandarización https://www.iso.org/search/x/query/27001)

En la actualidad la tendencia de las organizaciones alrededor del mundo es proteger su información de los delitos informáticos, ya que estos van en aumento, así lo establece Ernest & Young, (2015):

> Los informes técnicos, las estadísticas y las tecnologías futuras nos indican que las amenazas cibernéticas (ciberamenazas) seguirán multiplicándose.
> Con el advenimiento de la era digital (Big Data) y los cambios en los dispositivos tecnológicos (sistemas de información en la nube - cloudcomputing), se abre todo un nuevo campo de acción lleno de vulnerabilidades. (p. 4)

Hasta ahora la gran mayoría de las empresas utilizan los medios tradicionales de defensa como ser antivirus, cortafuegos (Firewalls), sistemas de detección de intrusos entre otro, pero debido al aumento del peligro de ataques, están optando por nuevos mecanismos de protección.

Según (Ernest & Young, 2015) ante las amenazas cibernéticas latentes, las empresas en el mundo comienzan a cimentar las bases para desarrollar estrategias de seguridad adoptando un nuevo enfoque en la seguridad de la información y adaptando sus medidas de seguridad a los cambios en sus estrategias de negocio y operaciones, cambiando su manera de pensar reactivamente ante las amenazas del futuro.

Algunas investigaciones relacionadas al tema, incluyen a américa latina como una región no exenta de los peligros informáticos y exponen la base legal aplicable en cada uno de los países, tal es el caso del estudio de Temperini (2014) sobre Delitos Informáticos en Latinoamérica, demuestra que no hay una armonía u homogeneidad de las normativas penales aplicables a los delitos informáticos. Adicionalmente el estudio concluye que, en la región, muchos de estos delitos aun no tienen sanción penal en algunos países (ver Tabla 1 y Tabla 2), lo que nos lleva a pensar que esta es una razón de gran peso para que las organizaciones se protejan de estas amenazas.

Tabla 1: Porcentaje de países que aún no tienen sanción por delito informático analizado.

Delito Informático	%
Acceso Ilícito	19%
Interceptación Ilícita	33%
Atentado contra la integridad de los datos	14%
Atentado contra la Integridad del sistema	33%
Abuso de los dispositivos	71%
Falsedad Informática	57%
Fraude o Estafa Informática	48%
Pornografía Infantil	19%

Fuente: (Tampieri (2014) Delitos Informáticos en Latinoamérica).

Tabla 2: Estadísticas que expresan el nivel de sanción penal de los delitos analizados, por país.

País	%
Argentina	88%
Bolivia	50%
Brasil	63%
Chile	63%
Colombia	75%
Costa Rica	88%
Cuba	0%
Ecuador	63%
El Salvador	63%
Guatemala	50%
Haití	0%
Honduras	50%
México	75%
Nicaragua	0%
Panamá	88%
Paraguay	88%
Perú	63%
Puerto Rico	100%
República Dominicana	100%
Uruguay	63%
Venezuela	100%

Fuente: (Tampieri (2014) Delitos Informáticos en Latinoamérica).

Como se observó en la tabla 2, Honduras forma parte de los países que tiene un nivel bajo de sanción penal para los delitos cibernéticos o informáticos, aunado a esto, muchas organizaciones en nuestro país no le dan la importancia que merece la seguridad informática y por ende la seguridad de su información, lo que lo expone a grandes riesgos como robo, perdida, fuga y modificación no autorizada de información, entre otros.

El artículo de Gutierrez (2016) afirma: “La situación de Honduras es congruente a lo que sucede en la región, donde las decisiones son dispares”. (párrafo 26)

“En términos de regulación, el país ha ido sumando esfuerzos para acoplarse a las exigencias del mercado, y mientras que ha logrado regular algunos aspectos, otros simplemente no”. (párrafo 4)

Por lo anteriormente expuesto, se considera de mucha importancia que las organizaciones en el país puedan adoptar modelos de gestión que les permitan garantizar la seguridad de la información que manejan.

Actualmente el país está dando pasos importantes en lo que a regulación de protección de datos se refiere, prueba de ello es que, en el año 2015, el Instituto de Acceso a la Información Pública (IAIP) presenta ante el Congreso Nacional de Honduras la propuesta de ley de Protección de Datos Personales, la cual busca la protección de los datos de los datos personales con el fin de regular su manejo garantizando la privacidad de las personas. (IAIP, 2015, p. 3)

Esta ley establece en su artículo 2 lo siguiente:

“Ámbito de Aplicación. Esta Ley será de aplicación a los datos personales registrados en bases de datos automatizadas o manuales, de organizaciones del sector público como del sector privado, y a toda modalidad de uso posterior de estos datos”. (IAIP, 2015, p. 8)

En la afirmación anterior se establece que la ley aplica para el sector público, lo que incluye los hospitales del país, siendo uno de ellos el ámbito de aplicabilidad de este trabajo de investigación.

La información hospitalaria o historia clínica de un paciente, es considerara como información confidencial, ya que implica que uno como paciente entrega al médico una porción de su vida privada, por lo tanto, esta demanda una protección sumamente cuidadosa debido a lo

sensible de la misma. Es por esto, que los hospitales deben dar la importancia merecida y adecuada a la protección y manejo de la información de sus pacientes.

El sector salud a nivel mundial, también ha sido golpeado por incidentes de seguridad de la información, así lo aseveran algunos estudios relacionados, por ejemplo:

El artículo de Sánchez-Henarejos et al. (2014) sobre Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria, afirma que: “En los últimos años el número de violaciones en la privacidad de los datos en las organizaciones sanitarias aumentó con la adopción de sistemas de historia clínica digital.” Adicionalmente, “Entre enero y junio de 2012 el número de episodios que comprometieron la confidencialidad del sistema de información en organizaciones sanitarias casi se duplicó.”

En el sector salud hondureño, adicional a la ley de protección de datos personales, a nivel de regulación solamente el Código de Ética del Colegio Médico de Honduras en su artículo 14 afirma lo siguiente:

> Se entiende por secreto médico al acto de salvaguardar la información que, por razón del ejercicio profesional, llegue al conocimiento del médico en la relación médico paciente y su contexto, ya sea porque le fue confiada, o porque la observó o la intuyó. Esta información no debe ser compartida salvo previo consentimiento del paciente, por daño al mismo o a terceros. (López Carballo, 2014, párrafo 6)

Las sanciones ante el incumplimiento de guardar el secreto médico son leves considerando la gravedad de la divulgación de la información confidencial de un paciente crónico, por ejemplo. Estas sanciones se establecen en el Reglamento de Sanciones del Colegio Médico de Honduras en el artículo 43 que reza lo siguiente:

> El secreto es un deber inherente a la profesión misma que exige el interés público, la seguridad de los enfermos, la honra a la familia, la responsabilidad del médico y la dignidad del arte, estableciendo una sanción en caso de violación del mismo de mil lempiras la primera vez y suspensión del ejercicio profesional hasta por tres meses en caso de reincidencia. (López Carballo, 2014, párrafo 8).

Esta es otra de las razones por las que se considera fundamental la aplicación de este tema de investigación en una institución de salud del país.

2.2 Bases teóricas

2.2.1 Seguridad de la Información:

Alexander (2014, p. 12) establece lo siguiente:

> Seguridad de la información es mucho más que establecer “firewalls, aplicar parches para corregir nuevas vulnerabilidades en el sistema de software, o guardar en la bóveda los “backups”. Seguridad de la información es determinar que requiere ser protegido y por qué, de que debe ser protegido y como protegerlo.

La seguridad de información se caracteriza por la preservación de:

a. Confidencialidad: La información está protegida de personas no autorizadas.
b. Integridad: La información esta como se pretende, sin modificaciones inapropiadas.
c. Disponibilidad: Los usuarios tienen acceso a la información y a los activos asociados cuando lo requieran.

2.2.2 Estándar ISO 27000

Alexander (2007, p 21) establece:

Dada la importancia que tiene un sistema de gestión de seguridad de la información para las empresas, en Ginebra, donde se encuentra la sede de ISO, se ha establecido, dentro de su estructura organizacional, el denominado Join Technical Commitee 1, al cual le reporta el subcomité 27 y luego el grupo de trabajo 1. El grupo de trabajo 1 está encargado de hacer las revisiones a las normas, las cuales, cada cinco años pasan por revisiones para decidir las posibles modificaciones. Este grupo de trabajo ha creado la familia ISO 27000, la cual se ha convertido en su agenda de trabajo para los próximos años. En la familia ISO 27000 se encuentran la norma

ISO/IEC 27001:2005, el código de prácticas ISO/IEC 17799:2005 y otros lineamientos que se irán desarrollando.

A continuación, se hace una breve descripción de los componentes de la familia ISO 27000:

1. ISO 27000 vocabulario y definiciones
2. ISO27001 Estándar Certificable ya oficializado.
3. ISO 27002 relevo del ISO/IEC 17799:2005.
4. ISO 27003 Guía para la implementación.
5. ISO 27004 Métricas e indicadores.
6. ISO 27005 Gestión de Riesgos.
7. ISO 27006 Requerimientos para entidades que proveen servicios de auditoría y certificación en sistemas de gestión de seguridad de información.

2.2.3 Sistema de Gestión de Seguridad de la Información (SGSI)

Alberts, Dorofree (citado en Alexander, 2007, p. 19) define un sistema de gestión de seguridad de la información de la siguiente manera: “Establecimiento de un sistema que determine qué requiere ser protegido, y porque, de qué debe ser protegido y como protegerlo”.

El modelo ISO 27001:2005 define a un SGSI como: Parte del sistema de gestión global basado en un enfoque del riesgo del negocio, para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar la seguridad de la información.

Merino Bada (2011)cita que “La norma/estándar UNE ISO/IEC 27001 del “Sistema de Gestión de la Seguridad de la Información” es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes,

vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información. El Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma UNE-ISO/IEC 27001, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua de Deming, que consiste en Planificar- Hacer-Verificar-Actuar, más conocido con el acrónimo en inglés PDCA (Plan- DO-Check-Act)

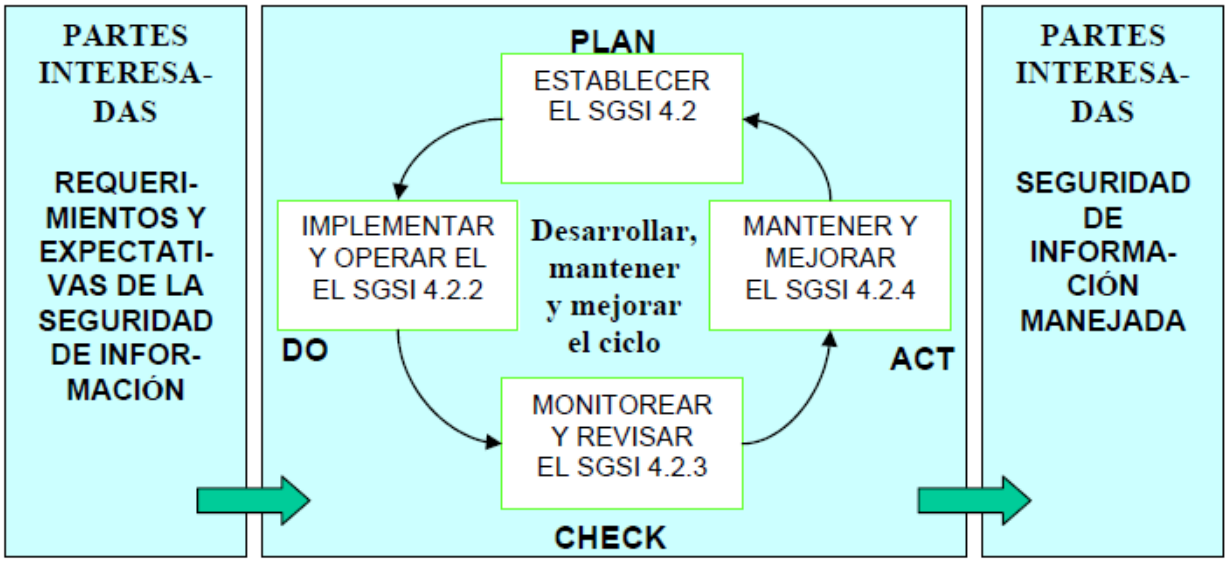


Figura 2: Modelo Sistema de Gestión de Seguridad de la información

Fuente: **(**Análisis y Evaluación del Riesgo de Información: Un caso en la banca. Aplicación del ISO27001:2005. www.centrum.pucp.edu.pe/excelencia).

2.2.4 Gestión de riesgos

La gestión de riesgos es una parte importante de la gestión de la seguridad y se define como el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzca

amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado (Aeritio J, 2008, p. 7).

Según Aeritio J (2008, pp. 54-55) en la práctica, existen dos metodologías básicas al momento de realizar un análisis de riesgos completo, una cualitativa y una cuantitativa siendo el primero el más utilizado debido a su sencillez.

Alexander (2007, pp. 42-43) afirma que "La gestión de los riesgos puede utilizar distintos enfoques gerenciales y métodos de cálculo que satisfagan las necesidades de la organización. La organización decidirá que método de cálculo del riesgo escoge".

"El ISO 27001 no exige un enfoque extremadamente detallado o técnico, en la medida en que todos los riesgos estén apropiadamente atendidos por la metodología utilizada".

A continuación, se ilustran los pasos a seguir para el manejo de la metodología para el análisis y evaluación del riesgo.

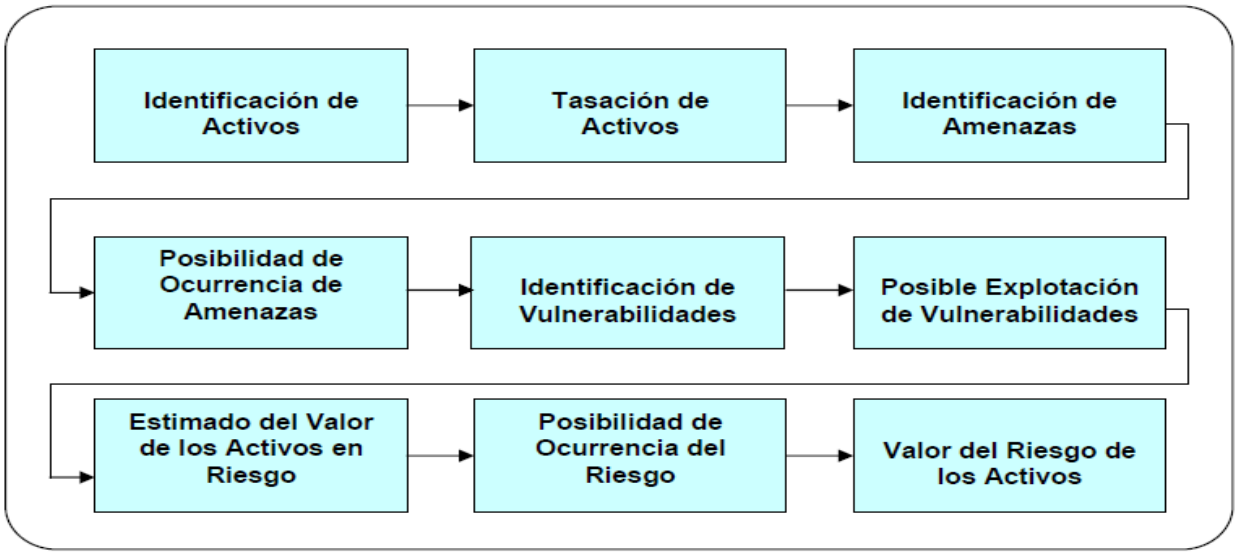


Figura 3: Metodología para el análisis y evaluación del riesgo

Fuente: (Análisis y Evaluación del Riesgo de Información: Un caso en la banca. Aplicación del ISO27001:2005. www.centrum.pucp.edu.pe/excelencia).

2.3 Términos Básicos:

2.3.1 Activo

Cualquier cosa que tenga valor para la organización y que requiere protección.

(ISO/IEC 13335-1:2004)

2.3.2 Disponibilidad

Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada.

(ISO/IEC 13335-1:2004)

2.3.3 Confidencialidad

Propiedad de que la información no está disponible o divulgada a individuos, entidades o procesos no autorizados. (ISO/IEC 13335-1:2004)

2.3.4 Integridad

Propiedad de salvaguardar la exactitud y la totalidad de los activos. (ISO/IEC 13335-1:2004)

2.3.5 Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información, adicionalmente pueden involucrarse otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad. (ISO/IEC TR18044:2004)

2.3.6 Seguridad Lógica

La seguridad lógica hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático. La seguridad lógica se complementa con la seguridad física. (ISO/IEC 17799:2005)

2.3.7 Seguridad Física

La seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informativo, para proteger el hardware de amenazas físicas. Esta también se complementa con la seguridad lógica. (ISO/IEC 17799:2005)

2.3.8 Políticas de gestión de seguridad de la información

Están constituidas por el conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que todos los activos y recursos, incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización. (ISO/IEC TR18044:2004)

2.3.9 Política de seguridad

Declaración de intenciones de alto nivel que cubre la necesidad de los sistemas informáticos y que proporcionan las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran. (ISO/IEC TR18044:2004)

2.3.10 Procedimiento de seguridad

Es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los procedimientos de seguridad permiten aplicar e implantar las políticas de seguridad que han sido aprobadas por la organización**.** (ISO/IEC Guide 73:2002)

2.3.11 Riesgos

Los riesgos son eventos o condiciones inciertas que, si se produce tiene un efecto positivo o negativo en los objetivos de un proyecto. Es la estimación el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. (ISO/IEC 13335-1:2004)

2.3.12 Amenaza

Conjunto de circunstancias negativas, potencial para causar un incidente no deseado, un riesgo que si se hace realidad tendrá un impacto negativo en un objetivo del proyecto, o posibilidad de cambios negativos. Cualquier circunstancia o evento que pueda explotar, intencionadamente o no, una vulnerabilidad especifica de un sistema de información. (ISO/IEC 13335-1:2004)

2.3.13 Vulnerabilidad

En una debilidad en el sistema de seguridad de la información, que puede hacer que una amenaza se materialice.

Una vulnerabilidad no causa daño, es simplemente una condición o conjunto de condiciones que pueden hacer que una amenaza afecte un activo. (ISO/IEC 13335-1:2004)

2.3.14 Incidente de seguridad de la información

Uno o una serie de eventos de seguridad de la información indeseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenacen la seguridad de la información. (ISO/IEC TR18044:2004)

2.3.15 Evento de seguridad de la información

Una ocurrencia de un estado del sistema, servicio o red que indica una posible violación a la política de seguridad o falla de salvaguarda, o de una situación previamente desconocida que puede ser pertinente a la seguridad. (ISO/IEC TR18044:2004)

3 CAPÍTULO 3

METODOLOGÍA

En este capítulo, se describe la metodología de investigación utilizada, la cual comprende el tipo de enfoque, el diseño de la investigación, el instrumento diseñado para la recolección de datos, las fuentes de información y las limitantes de la investigación.

Se diseñó un cuestionario con el objetivo de conocer la situación actual de la organización y se aplicó en el departamento de Tecnología (TIC) y a diferentes usuarios de los sistemas de información.

3.1 Metodología de desarrollo

Para desarrollar este proyecto de investigación, se decidió trabajar bajo la óptica del estándar ISO27001 ya que es una normativa de clase mundial con un alto nivel de reconocimiento en las organizaciones.

La metodología consiste en el establecimiento de sistema de seguridad de la información que sirva de guía a la organización Hospital María Especialidades Pediátricas, para que pueda realizar un correcto análisis de la seguridad de su información, permitiéndole conocer cómo se gestiona actualmente y proporcionándole las directrices necesarias para la gestión correspondiente.

En este apartado, se tratará de que la planeación del SGSI sea lo más genérica posible, para que pueda ser considerado por otras organizaciones. El detalle específico será presentado en el capítulo 4 Análisis de Resultados y en el manual de seguridad de la información que le será sugerido al hospital en estudio.

3.2 Enfoque de la Investigación

El enfoque de la investigación tiene un carácter cualitativo ya que se realiza el análisis no numérico, se explora el fenómeno de estudio desde la óptica de los individuos participantes en su ambiente natural, tomando en cuenta principalmente la situación actual de la organización.

3.3 Diseño y Alcance de la Investigación

La investigación considera la combinación de un diseño narrativo y de estudio de caso, en específico, el Hospital María Especialidades Pediátricas, con un alcance descriptivo, ya que se centra en recolectar información relevante del objeto de estudio para proporcionar la descripción de su estado actual y luego narrar las situaciones que interesan en el análisis de los datos.

3.4 Muestra

Para los fines de esta investigación se utiliza una muestra combinada de la siguiente manera: muestra de expertos ya que se realizaron entrevistas a individuos con cierto nivel de conocimiento del tema abordado como Jefes de IT, administradores de redes y técnicos en informática, adicionalmente se considera una muestra diversa, entrevistando a los usuarios de los sistemas de información de la organización para conocer su perspectiva en cuanto a seguridad de la información.

3.5 Instrumentos

El instrumento utilizado para obtener la información de la situación actual de la organización, es el cuestionario. Este cuestionario cuenta con preguntas abiertas y cerradas que nos permiten analizar la información de manera adecuada, aplicándolo mediante entrevista directa y personal a los individuos de la muestra seleccionada. Adicionalmente aprovechando mi situación de empleado del HMEP, como investigador se han realizado algunas observaciones de

los procedimientos del hospital que afectan a la seguridad de la información y que serán expuestas en el capítulo 4 en el análisis de resultados, convirtiéndome entonces en un investigador participativo.

3.6 Limitantes del estudio

Las limitantes más significativas detectadas durante la investigación son:

- Limitante de disponibilidad de las personas a entrevistar ya que sus actividades diarias dentro de la organización no les permite atender las entrevistas.
- Respuestas erróneas debido al desconocimiento de algunos individuos entrevistados.

3.7 Desarrollo de la Metodología

3.7.1 Establecimiento del Sistema de Gestión de Seguridad de la Información.

La implementación de un SGSI requiere el despliegue de recursos significativos, por lo que las organizaciones deben tener muy claras las razones para implementarlo. Estas razones deben estar documentadas considerando la relación costo beneficio que se obtendría de la implementación. (Alexander 2007, p.39)

3.7.2 Alcance.

La definición del alcancel del SGSI es la decisión más transcendental en el establecimiento del sistema y dependerá exclusivamente de la organización. El alcance puede abarcar a toda la empresa, solamente a parte de ella o sencillamente un proceso o un sistema de IT.

Una vez definido el alcance, se deben identificar los activos de información debido a que, con base en ellos, se creará la política de seguridad para iniciar la implementación.

Para efectos de este estudio, para la definición del alcance se utilizará un método conocido como Metodología de las elipses, ya que se considera un excelente y sencillo mecanismo para la identificación de activos de información dado un alcance. (ver figura 4)

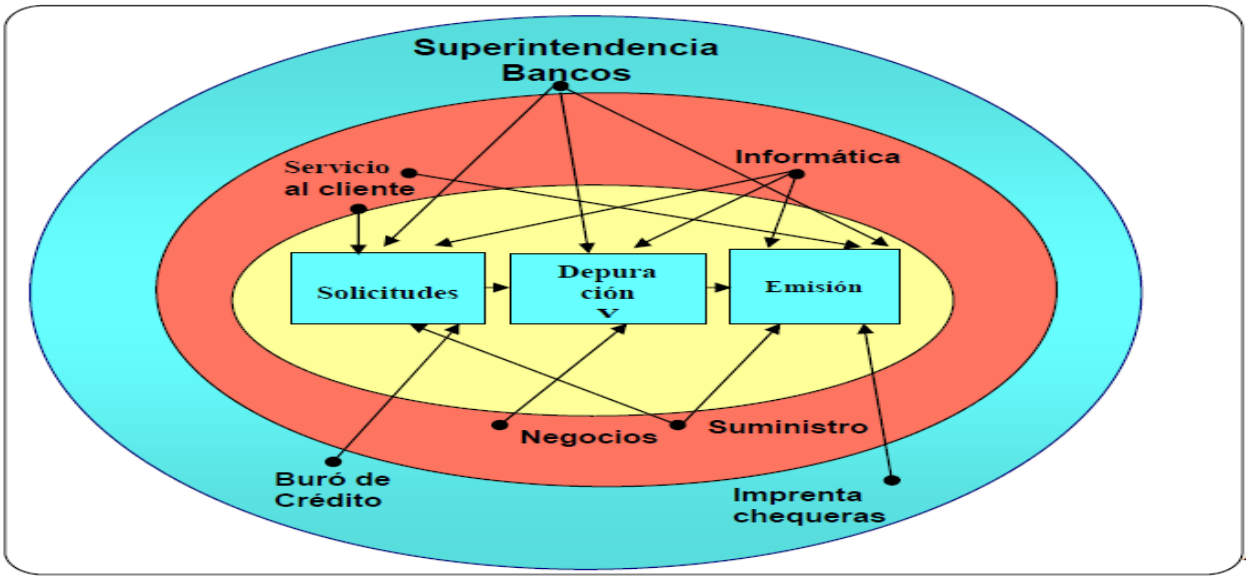


Figura 4: Metodología de las elipses, Ejemplo

Fuente: (Análisis y Evaluación del Riesgo de Información: Un caso en la banca. Aplicación del ISO27001:2005. www.centrum.pucp.edu.pe/excelencia).

3.7.3 Política de Seguridad de la Información.

Al haber determinado el alcance e identificados los activos de información del SGSI, la empresa debe definir una clara policía de seguridad con el objetivo de apoyar el establecimiento de la seguridad de información.

3.7.4 Enfoque para la Gestión del Riesgo.

Existen diferentes metodologías para la gestión de riesgos. La organización debe decidir que método utilizar asegurándose que el elegido es el más adecuado para atender los requerimientos organizacionales, regulatorios y legales.

La normativa ISO 27001 no demanda el uso de un método extremadamente detallado, siempre y cuando los riegos estén debidamente atendidos por la metodología utilizada.

Para efectos de esta investigación, se utilizará la metodología ilustrada en la figura 3 del apartado 2.2.4 Gestión del Riesgo del capítulo 2.

3.7.5 Proceso de evaluación del riesgo.

El proceso de cálculo de riesgo de seguridad de la información incluye el análisis y la evaluación del riesgo.

El análisis del riesgo incluye:

- Identificación de los activos de información.
- Identificación de requerimientos legales y comerciales para los activos identificados.
- Tasación de los activos identificados.
- Identificación de Amenazas y vulnerabilidades para cada uno de los activos de información.
- Calculo de la posibilidad de ocurrencia de las amenazas y vulnerabilidades.

La evaluación del riesgo incluye:

- Calculo del riesgo.
- Identificación del significado de los riesgos. Esta operación se realiza definiendo criterios y evaluando los riesgos contra una escala predeterminada.

3.7.6 Análisis del Riego.

"El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades" (Alexander, 2007, p. 53).

3.7.6.1 Identificación de los Activos de Información.

La identificación de los activos de información de la empresa, que se incluyen dentro del alcance de SGSI, es el tema clave para la correcta implementación de un sistema de gestión de seguridad de información.

Los activos de información pueden abarcar un espectro muy amplio, por lo cual es necesario comprender bien que es un activo de información y conocer su clasificación con el objetivo de poder realizar un análisis y una evaluación de riesgos de manera apropiada.
"Un activo de información es algo a lo que la organización directamente asigna un valor y, por lo tanto, la organización debe proteger" (Alexander, 2007a, p. 44).

3.7.6.2 Identificación de los requerimientos legales y comerciales.

Al momento de realizar el proceso de identificación de los activos, también se debe analizar si existen algunos requerimientos comerciales y/o legales que tengan alguna relación con los activos y verificar si estos requerimientos incluyen otros activos de información.

3.7.6.3 Tasación de Activos.

Para llevar a cabo la tasación de activos, se debe plantear la siguiente pregunta:
¿Cómo una falla o pérdida de un activo puede afectar la confidencialidad, la integridad y la disponibilidad de la información?

Cada uno de los activos identificados en el paso previo, debe tasarse utilizando una escala de Likert, del 1 al 5, donde el valor 1 significa “muy poco” y el valor 5 significa “muy alto”.

En la siguiente tabla se muestra un ejemplo de tasación de activos:

Tabla 3: Tasación de Activos de Información

Activo de información	Confidencialidad	Integridad	Disponibilidad	Total (Promedio)
Bases de datos pacientes	5	5	5	5
Laptops	4	4	4	4
Técnico Informática	4	2	4	3

Fuente: (Elaboración propia)

Adicionalmente y como requerimiento de la normativa ISO 27001, se deben identificar los propietarios o responsables de cada uno de los activos de información. En la siguiente tabla, se muestra un ejemplo:

Tabla 4: Activos de información y propietarios.

Activo de Información	Propietarios
Bases de datos pacientes	Departamento de Sistemas
Laptops	Departamento de Sistemas
Técnico de Informática	Departamento de Sistemas

Fuente: Elaboración Propia

Los propietarios de los activos de información serán responsables de especificar la clasificación de la seguridad, los derechos de accesos a estos activos y los controles correspondientes.

3.7.6.4 Identificación de amenazas y vulnerabilidades.

Los activos de información de una organización están expuestos a las amenazas, las cuales pueden ocasionar daños a los mismos y por ende a la organización.

Las amenazas se clasifican como se muestra en la siguiente tabla:

Tabla 5:Clasificación de las Amenazas.

Amenazas naturales	Inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales.
Amenazas a instalaciones	Fuego, explosión, caída de energía, daño de agua, pérdida de acceso, fallas mecánicas.
Amenazas humanas	Huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave.
Amenazas tecnológicas	Virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en líneas telefónicas.
Amenazas operacionales	Crisis financieras, pérdida de suplidores, fallas en equipos, aspectos regulatorio, mala publicidad.
Amenazas sociales	Motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo.

Fuente**:** (Alexander, 2007, p. 48)

Las amenazas pueden tener su origen de acontecimientos ocasionados intencionalmente o por simples accidentes y para que se produzca un daño a uno o varios de los activos de información, debe ser detonante de una o varias vulnerabilidades.

Acto seguido de la identificación de las amenazas, se debe evaluar la posibilidad de que estas ocurran. Esta evaluación se realiza utilizando una escala de Likert del 1 al 5, donde el valor 1 significa “Muy poco” y el valor 5 significa “Muy Alto”.

Las vulnerabilidades, se clasifican en:

1. Seguridad de los Recursos humanos.
2. Control de acceso.
3. Seguridad física y ambiental.
4. Gestión de operaciones y comunicación.
5. Mantenimiento, desarrollo, y adquisición de sistemas de información.

Una vez determinadas las vulnerabilidades, la normativa exige la estimación de la posibilidad de que estas sean explotadas por las amenazas, este procedimiento se realiza utilizando una escala de Likert del 1 al 5, donde el valor 1 significa “Baja” y el valor 5 significa “Extrema”.

3.7.6.5 Cálculo de Amenazas y vulnerabilidades.

En esta fase, se calcula la posibilidad de que las amenazas y las vulnerabilidades puedan juntarse y producir un riesgo para los activos de información. Este cálculo se ve reflejado en el capítulo de aplicabilidad.

3.7.6.6 Análisis y evaluación del Riesgo.

En esta fase, se pretende identificar y calcular los riesgos con base en los activos de información identificados previamente y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos son calculados relacionando los valores de los activos que determinan el impacto de una perdida por confidencialidad, disponibilidad e integridad de la información y del cálculo que las amenazas y las vulnerabilidades puedan juntarse y producir un riesgo.

Un ejemplo de este método se muestra en la siguiente tabla:

Tabla 6:Metodología para calcular el riesgo

Activo	Amenaza	Impacto de la amenaza	Probabilidad de Ocurrencia	Medición del Riesgo	Priorización
Bases de datos pacientes	Secuestro	5	2	10	2
Laptops	Virus	4	5	20	1
Técnico Informática	Fuga de Información	3	3	9	3

Fuente**:** (Elaboración propia).

En primera instancia, se evalúa el impacto de la amenaza utilizando una escala de Likert del 1 al 5, donde 1 significa “Menor” y 5 significa “Grave”. Seguidamente, se calcula la probabilidad de ocurrencia de la amenaza considerada, utilizando la misma escala para el paso anterior. En seguida, se procede a calcular el riesgo multiplicando los valores del impacto de la

amenaza por la probabilidad de ocurrencia de la amenaza. Finalmente, con base en el valor de riesgo, las amenazas se priorizan en orden para determinar cuáles son los riesgos más significativos

Para evaluar el riesgo, es necesario definir cuáles son las amenazas cuyos riesgos son los más relevantes. Para este proceso se utilizará una escala de Likert que permita medir los niveles de riesgo. Los criterios generalmente utilizados son los siguientes:

1. Impacto económico del riesgo.
2. Tiempo de recuperación de la empresa.
3. Posibilidad de ocurrencia del riesgo.
4. Posibilidad de interrumpir las actividades de la empresa.

3.7.6.7 Tratamiento del Riesgo y el proceso de toma de decisión gerencial.

Una vez que se ha completado el análisis de los riesgos, se debe determinar qué acciones se van a tomar con respecto a los activos expuestos a riesgos. Esta fase se vuelve un proceso de toma de decisiones en cuanto a cómo se deben tratar los riesgos identificados. Estas decisiones están fuertemente influenciadas por os objetivos estratégicos de la organización, pero se pueden encadenar a dos factores:

1. El posible impacto si el riesgo sucede.
2. Con que frecuencia puede suceder.

3.7.6.8 Estrategias para tratamiento de riesgos.

Reducción del riesgo.

Si se toma la decisión de reducir el riesgo, se deben seleccionar con precisión los controles que permitan cumplir con esta decisión.

Aceptar el Riesgo.

Si no se encuentran los controles apropiados o la implementación de dichos controles involucra un costo mayor al que puede producir un riesgo, se toma la decisión de aceptar el riesgo y convivir con las consecuencias que esto pueda generar.

Transferir el Riesgo.

Esta decisión debe tomarse cuando resulta muy difícil a la organización controlar o reducir el riesgo a un nivel aceptable. La transferencia involucra a una tercera parte, que será la encargada de controlar los riesgos transferidos. Esto con el objetivo de generar ahorros en la gestión de ese tipo de riesgo.

Evitar el Riesgo.

Evitar el riesgo es cualquier acción orientada a modificar las actividades para así evitar la presencia del riesgo. Por ejemplo:

Mover los activos de un área de riesgo.

No procesar información sensible.

3.7.7 Riesgo Residual

El riesgo residual es el riesgo es el remanente que queda después de implementar las decisiones de tratamiento. Este riesgo es muy difícil de calcular, pero debe al menos efectuarse una evaluación que indique que se tiene una protección suficiente. Esto puede lograrse a través de la implementación de más controles o a través de diferentes opciones de tratamiento a las ya mencionadas.

Si el riesgo residual resultante fuese imposible de reducir a un nivel de aceptación o si representan un costo exageradamente elevado, deberá de aplicarse la estrategia de aceptación. En este punto es importante que la alta gerencia apruebe estos riesgos y revisar en determinados períodos los niveles de riesgo residual y riesgo aceptable.

4 CAPÍTULO 4

RESULTADOS Y ANÁLISIS DE DATOS

4.1 Análisis de resultados

Previo a la elaboración del manual de seguridad de la información es necesario, realizar un análisis previo de la situación actual del hospital en lo referente a seguridad de la información. Para efectuar este análisis se elaboró un cuestionario (ver Anexo 1) orientándolo a la recolección de datos que aportarán valor para el logro de los objetivos planteados y que brinde un panorama general de cómo se maneja el tema de seguridad dentro de la organización.

El departamento de Tecnologías de Información y Comunicaciones es un área esencial dentro del hospital, ya que de ella depende el correcto funcionamiento de las tecnologías de información que se manejan dentro de la organización, motivo por el que se ha tomado como alcance del análisis, este departamento.

Adicionalmente, para la elaboración del análisis se consideraron aspectos como la seguridad lógica, seguridad física, seguridad de las aplicaciones, gestión de incidentes de seguridad, control de accesos, que son cláusulas de control contenidas en la normativa ISO 27001.

A continuación, se muestran los hallazgos agrupados por cláusulas de control:

4.1.1 Políticas de Seguridad

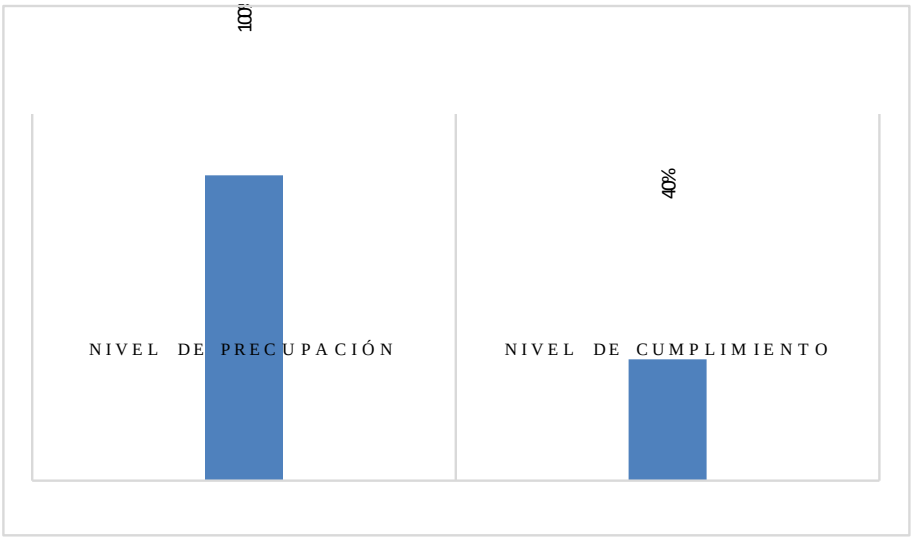
- El Hospital María cuenta con una Política Digital establecida en el documento interno Lineamientos para la gestión de tecnologías de la información y comunicaciones, que incluye a nivel macro el tema de seguridad de la información, sin embargo, no tiene definida una política específica de seguridad de la información tal como lo exige la normativa de aplicabilidad de esta

investigación en la cláusula 5 y control 5.1.1 Conjunto de políticas para la seguridad de la información que establece lo siguiente:

"Un documento de política de seguridad de la información debería aprobarse por la dirección, ser publicado y comunicado a todos los empleados y partes externas pertinentes" (Fondonorma, 2007, p. 13).

Se pudo constatar mediante las entrevistas realizadas que a nivel gerencial la preocupación por los temas de seguridad de la información tiene un nivel alto, pero debido a diversos factores como, por ejemplo, temas presupuestarios, falta de personal entre otros, el nivel de cumplimiento es más bajo que el que se debería tener. Este se pude observar más claramente en la siguiente gráfica:

Gráfico 1: Nivel de Preocupación vs nivel de cumplimiento de política de seguridad.



Fuente: (Elaboración propia)

- La información de los Pacientes es considerada como un activo de información muy importante ya que el ente regulador exige la presentación de indicadores e información relacionada a las atenciones realizadas, información que tiene origen en el expediente de los pacientes. Toda esta información es provista a través de los sistemas de información que maneja actualmente el HMEP por lo que dese ya, se puede considerar a estos sistemas como un activo de información crítico.

- La seguridad de la información de los pacientes es garantizada a través de la implementación de planes de acción de contingencia y de proyectos de adquisición y puesta en marcha de sistemas robustos que brindan la capacidad de respuesta que el hospital necesita.

- Se observó que el HMEP no cuenta con metodologías documentadas para la seguridad de la información, sin embargo, se conocen las metodologías aplicables y se ejecutan controles relacionados. Como consecuencia de la falta de documentación, no se pueden obtener indicadores medibles de la seguridad de la información.

En la siguiente tabla, se muestran los niveles de cumplimiento relacionados a la cláusula de control número 5, de la normativa en aplicación, que trata lo referente a las políticas de seguridad.

Tabla 7:Situación actual sobre políticas de seguridad

Clausula de control	Nivel de cumplimiento Actual (%)
5. POLÍTICAS DE SEGURIDAD	**40**
5.1 Directrices de la Dirección en seguridad de la información.	40
5.1.1 Conjunto de políticas para la seguridad de la información.	40
5.1.2 Revisión de las políticas para la seguridad de la información.	40

Fuente: (Elaboración propia)

4.1.2 Organización para la seguridad de información

- Los roles de seguridad de la información son administrados por el departamento de TIC.
- Se considera que las responsabilidades de seguridad están implícitas dentro de las funciones de los empleados.

En la siguiente tabla, se muestran los niveles de cumplimiento relacionados a la cláusula de control número 6.

Tabla 8: Situación actual sobre Organización para la seguridad de la información

Clausula de control	Nivel de cumplimiento Actual (%)
6. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN	**44**
6.1 Organización interna.	**57**
6.1.1 Asignación de responsabilidades para la seguridad de la información.	30
6.1.2 Segregación de tareas.	80
6.1.3 Contacto con las autoridades.	80
6.1.4 Contacto con grupos de interés especial.	50
6.1.5 Seguridad de la información en la gestión de proyectos.	45
6.2 Dispositivos para movilidad y teletrabajo.	**30**
6.2.1 Política de uso de dispositivos para movilidad.	30
6.2.2 Teletrabajo.	N/A

Fuente: (Elaboración propia)

4.1.3 Seguridad de los recursos Humanos

- Se pudo confirmar que los usuarios de los sistemas de información no son capacitados en cuanto a temas de seguridad de información.
- Durante las observaciones y por experiencia propia, se pudo confirmar que, dentro de los procesos de contratación del departamento de Talento Humano del hospital, uno de los requisitos solicitados a los aspirantes es la información relacionada con sus antecedentes, que es una de controles solicitados por la norma (control 7.1.1 Revisión).

- Adicionalmente se verifico que el hospital cuenta con un proceso disciplinario aplicable a los colaboradores de la organización, sin embargo, este no contiene clara y específicamente el proceso formal a seguir cuando se cometa un incumplimiento de seguridad.

En la siguiente tabla, se muestran los niveles de cumplimiento actual, relacionados a la cláusula de control número 7 seguridad de los recursos humanos.

Tabla 9: Situación actual sobre Seguridad de los recursos humanos.

Clausula de control	Nivel de cumplimiento Actual (%)
7. SEGURIDAD DE LOS RECURSOS HUMANOS	**43**
7.1 Antes de la contratación.	**75**
7.1.1 Revisión	100
7.1.2 Términos y condiciones de contratación.	50
7.2 Durante el empleo.	**23**
7.2.1 Responsabilidades gerenciales	30
7.2.2 Concienciación, educación y toma de conciencia para la seguridad de la información.	0
7.2.3 Proceso disciplinario.	40
7.3 Terminación o cambio de puesto de trabajo.	**30**
7.3.1 Terminación o cambio de puesto de trabajo.	30

Fuente: (Elaboración propia)

4.1.4 Gestión de activos

- Se pudo confirmar que el HMEP no cuenta con la documentación necesaria referente a la importancia, clasificación prioritaria y criticidad de los activos de información. Así lo confirma la Jefe de TIC del HMEP: “Eso se saca de una matriz de riesgos, y en este caso, nosotros no tenemos una matriz de riesgos asociados a todos los activos”. (Licenciada Lorena Arana, comunicación personal, 23 de agosto 2017).

- Las autoridades del HMEP se considera que los activos de información están en un nivel de protección muy alto tomando como referencia una escala de Likert el 1 al 5, donde el valor 1 significa “bajo” y el valor 5 significa “muy alto”. Sin embargo, durante el proceso de

recolección de datos, se pudo comprobar que algunos de los activos no cuentan con una protección adecuada , ya que por ejemplo no se cuenta con controles de encriptación de información, a pesar de que se maneja un control de accesos vía contraseñas, por ejemplo, si ocurre un robo de una maquina portátil en la que se maneja información confidencial una persona ajena a la institución entendida en la materia de informática podría fácilmente vulnerar la contraseña y obtener accesos a la información sensible del hospital.

En la siguiente tabla, se muestran los niveles de cumplimiento actual relacionados a la cláusula de control número 8.

Tabla 10: Situación actual sobre Gestión de activos.

Clausula de control	Nivel de cumplimiento Actual (%)
8. GESTIÓN DE ACTIVOS.	**41**
8.1 Responsabilidad sobre los activos.	**85**
8.1.1 Inventario de activos.	80
8.1.2 Propiedad de los activos.	80
8.1.3 Uso aceptable de los activos.	80
8.1.4 Devolución de activos.	100
8.2 Clasificación de la información.	**0**
8.2.1 Directrices de clasificación.	0
8.2.2 Etiquetado y manipulado de la información.	0
8.2.3 Manipulación de activos.	0
8.3 Manejo de medios	**37**
8.3.1 Gestión de medios removibles.	30
8.3.2 Disposición de medios	40
8.3.3 Trasferencia física de medios	40

Fuente: (Elaboración propia)

4.1.5 Control de Accesos

- Se constató que actualmente tienen acceso a la información de los pacientes las siguientes áreas y su personal:

- Personal de Gestión de Pacientes. Este es el departamento que tiene el primer contacto con el paciente al momento de abrir un expediente físico y electrónico.
- Personal Clínico (Médicos y enfermeras)
- Departamento de Calidad y Auditoria Clínica.
- Departamento de control Interno.
- Departamento de Control de Gestión.

Se observó que son varias áreas y un gran número de personas las que tienen acceso a la información de los pacientes, que como ya se planteó en el marco teórico de esta investigación, es información altamente confidencial y sensitiva tanto para el hospital como para el paciente mismo. A pesar de esto, el Hospital María Especialidades no cuenta con un acuerdo de confidencialidad que garantice que las áreas de contacto con esta información respeten la confidencialidad, lo que se traduce en una amenaza latente para la seguridad de la información. Sin embargo, las autoridades del HMEP son conscientes de la importancia de estos acuerdos, así lo manifiesta la Jefe del departamento de Tecnologías de Información y Comunicaciones del hospital:

"No existe un acuerdo de confidencialidad, pero deberíamos de tenerlo, para que las áreas de contacto con el expediente estén obligadas a respetar la confidencialidad de la información". (Licenciada Lorena Arana, comunicación personal, 23 de agosto 2017).

- Se corroboró que el HMEP cuenta con perfiles de accesos de los usuarios tanto a nivel de acceso a recursos como a nivel de software.
- El departamento de TIC ha definido ciertas restricciones a los usuarios de los recursos de TI como los sistemas de información en donde se guarda la información.

- El HMEP tiene procedimientos establecidos para otorgar y revocar privilegios, pero actualmente no se cumplen a cabalidad.

"Ese es un problema de seguridad porque, no tenemos un mecanismo eficiente para validar que los empleados son dados de baja, no nos damos cuenta en ese momento por que no se nos notifica" (Licenciada Lorena Arana, comunicación personal, 23 de agosto 2017).

Este hallazgo también aplica a la cláusula de Seguridad de Recursos Humanos (cláusula de control 7).

En la siguiente tabla, se muestran los niveles de cumplimiento actual relacionados a la cláusula de control número 9, Control de Accesos.

Tabla 11: Situación actual sobre Control de accesos.

Clausula de control	Nivel de cumplimiento Actual (%)
9. CONTROL DE ACCESOS.	**76**
9.1 Requisitos de negocio para el control de accesos.	**85**
9.1.1 Política de control de accesos.	75
9.1.2 Control de acceso a las redes y servicios asociados.	95
9.2 Gestión de acceso de usuario.	**50**
9.2.1 Registro de usuarios y desregistro.	50
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	50
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	70
9.2.4 Gestión de información confidencial de autenticación de usuarios.	50
9.2.5 Revisión de los derechos de acceso de los usuarios.	30
9.2.6 Retirada o adaptación de los derechos de acceso	50
9.3 Responsabilidades del usuario.	**100**
9.3.1 Uso de información confidencial para la autenticación.	100
9.4 Control de acceso a aplicaciones y sistemas.	**70**
9.4.1 Restricción del acceso a la información.	50
9.4.2 Procedimientos seguros de inicio de sesión.	75
9.4.3 Gestión de contraseñas de usuario.	75
9.4.4 Uso de herramientas de administración de sistemas.	75
9.4.5 Control de acceso al código fuente de los programas.	75

Fuente**:** (Elaboración propia)

4.1.6 Criptografía

- Durante las entrevistas realizadas, se pudo confirmar que no se cuenta con políticas documentadas ni en ejecución de uso de controles criptográficos, adicionalmente como se mencionó en los hallazgos de la cláusula de Gestión de activos, no se cuenta con controles de encriptación de información.

En la siguiente tabla, se muestran los niveles de cumplimiento actual relacionados a la cláusula de control número 10, Criptografía.

Tabla 12: Situación actual sobre Criptografía.

Clausula de control	Nivel de cumplimiento Actual (%)
10. CRIPTOGRAFÍA	**0**
10.1 Controles criptográficos.	0
10.1.1 Política de uso de los controles criptográficos.	0
10.1.2 Gestión de claves.	0

Fuente: (Elaboración propia)

4.1.7 Seguridad Física y Ambiental

- En las observaciones realizadas durante la investigación, se pudo verificar que el hospital cuenta, con controles de seguridad física, desde guardias apostados en los diferentes puntos de accesos al hospital, hasta controles biométricos para áreas restringidas. De igual manera se verificó que el Data Center es un área segura en el departamento de IT, que cuenta con las restricciones de acceso únicamente para personal autorizado.

En la tabla a continuación mostrada, se observa el nivel de cumplimiento actual del hospital en lo referente a seguridad física y ambiental.

Tabla 13: Situación actual sobre Seguridad física y ambiental.

Clausula de control	Nivel de cumplimiento Actual (%)
11. SEGURIDAD FÍSICA Y AMBIENTAL.	**72**
11.1 Áreas seguras.	**90**
11.1.1 Perímetro de seguridad física.	95
11.1.2 Controles físicos de entrada.	75
11.1.3 Seguridad de oficinas, cuartos y ambientes	95
11.1.4 Protección contra las amenazas externas y ambientales.	90
11.1.5 El trabajo en áreas seguras.	95
11.1.6 Áreas de acceso público, carga y descarga.	90
11.2 Seguridad de los equipos.	**54**
11.2.1 Ubicación y protección de equipos.	75
11.2.2 Apoyo de servicios públicos.	70
11.2.3 Seguridad del cableado.	80
11.2.4 Mantenimiento de los equipos.	75
11.2.5 Salida de activos fuera de las dependencias de la empresa.	50
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	30
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	65
11.2.8 Equipo informático de usuario desatendido.	40
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	0

Fuente: (Elaboración propia)

4.1.8 Seguridad en Operaciones

- Durante la entrevista se corroboró que los procedimientos de backups se realizan diarios y de manera diferencial cada cierto número de horas.

- El hospital no cuenta con gestión de versiones de las aplicaciones, solamente se tienen notificaciones de parte de los proveedores, pero aún no se ha madurado el proceso.

"No tenemos la gestión de versiones. Tenemos las notificaciones del proveedor en el caso del sistema ERP, que nos remiten que contienen las versiones, pero todavía no tenemos muy maduro ese proceso" (Licenciada Lorena Arana, comunicación personal, 23 de agosto 2017).

En la siguiente tabla, se muestran los niveles de cumplimiento actual relacionados a la cláusula de control número 12, Seguridad en Operaciones**.**

- La instalación de programas o productos se restringe a través de accesos ya que ningún usuario tiene privilegios de instalación a excepción del administrador de sistemas, por lo tanto, toda licencia y sistemas operativos son tramitadas a través del departamento de TI. Bajo este esquema, no se realizan monitoreos de programas o aplicaciones instaladas sin autorización.

Tabla 14: Situación actual sobre Seguridad en operaciones.

Clausula de control	Nivel de cumplimiento Actual (%)
12. SEGURIDAD EN LA OPERACIONES	**79**
12.1 Responsabilidades y procedimientos de operación.	**64**
12.1.1 Documentación de procedimientos de operación.	50
12.1.2 Gestión de cambios.	20
12.1.3 Gestión de capacidades.	90
12.1.4 Separación de entornos de desarrollo, prueba y producción.	95
12.2 Protección contra código malicioso.	**95**
12.2.1 Controles contra el código malicioso.	95
12.3 Copias de seguridad.	**50**
12.3.1 Copias de seguridad de la información.	50
12.4 Registro de actividad y supervisión.	**84**
12.4.1 Registro y gestión de eventos de actividad.	80
12.4.2 Protección de los registros de información.	80
12.4.3 Registros de actividad del administrador y operador del sistema.	80
12.4.4 Sincronización de relojes.	95
12.5 Control del software operativo	**95**
12.5.1 Instalación del software en sistemas en producción.	95
12.6 Gestión de la vulnerabilidad técnica.	**73**
12.6.1 Gestión de las vulnerabilidades técnicas.	50
12.6.2 Restricciones en la instalación de software.	95
12.7 Consideraciones de las auditorías de los sistemas de información.	**95**
12.7.1 Controles de auditoría de los sistemas de información.	95

Fuente: (Elaboración propia)

4.1.9 Seguridad en las comunicaciones

- Se pudo confirmar que en cuanto al uso de la información y de los activos asociados a esta, el hospital tiene procedimientos establecidos para ciertos niveles de servicios, pero se detectó que no se maneja un control para ciertas aplicaciones, como por ejemplo la activación del

correo institucional en los dispositivos móviles. La aplicación de correo es configurada a solicitud de los usuarios, pero no se conoce a nivel de detalle que personal cuenta con ese privilegio.

- Se confirmó que el hospital cuenta con políticas de control y accesos a los servidores de la red, siendo estas controladas por el administrador de infraestructura del departamento de TI.

En la siguiente tabla, se muestran los niveles de cumplimiento actual relacionados a la cláusula de control número 13, Seguridad en las comunicaciones.

Tabla 15: Situación actual sobre Seguridad en comunicaciones.

Clausula de control	Nivel de cumplimiento Actual (%)
13. SEGURIDAD EN LAS COMUNICACIONES	**47**
13.1 Gestión de la seguridad en las redes.	**68**
13.1.1 Controles de red.	75
13.1.2 Servicios de seguridad de redes	50
13.1.3 Segregación de redes.	80
13.2 Intercambio de información con partes externas.	**25**
13.2.1 Políticas y procedimientos de intercambio de información.	30
13.2.2 Acuerdos de intercambio.	30
13.2.3 Mensajería electrónica.	40
13.2.4 Acuerdos de confidencialidad y secreto.	0

Fuente: (Elaboración propia)

4.1.10 Gestión de incidentes de seguridad de información

- Durante las entrevistas, se pudo obtener información sobre ataques informáticos confirmando que, el HMEP ya fue atacado en una ocasión, siendo víctima de secuestro de una base de datos (Ransomware), debido a que un proveedor tuvo acceso a un servidor considerado

no crítico para realizar un mantenimiento. En una memoria USB se portaba un virus que infecto el equipo generando el ransomware.

A raíz de este acontecimiento, se fortaleció el control de accesos gestionándolo única y exclusivamente a través de la persona que tiene asignado el rol de seguridad dentro de la organización. Como se pudo observar en el marco teórico, en el artículo de Sánchez Henarejos et al. (2014) el sector salud en los últimos años, se ha vuelto vulnerable a los ataques cibernéticos, por lo que se vuelve una necesidad la implementación de un sistema de seguridad, que prevenga ataques y ayude a mitigar los ya ocurridos.

En la siguiente tabla, se muestran los niveles de cumplimiento actual relacionados a la gestión de incidentes de seguridad de información.

Tabla 16: Situación actual sobre Gestión de incidentes de seguridad de información.

Clausula de control	Nivel de cumplimiento Actual (%)
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**42**
16.1 Gestión de incidentes de seguridad de la información y mejoras.	**42**
16.1.1 Responsabilidades y procedimientos.	30
16.1.2 Notificación de los eventos de seguridad de la información.	30
16.1.3 Notificación de puntos débiles de la seguridad.	30
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	50
16.1.5 Respuesta a los incidentes de seguridad.	30
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	75
16.1.7 Recopilación de evidencias.	50

Fuente: (Elaboración propia)

4.1.11 Gestión de Continuidad del Negocio

- Se pudo confirmar, que el hospital cuenta a nivel de políticas con un plan de contingencia ante las caídas de los servidores y que se encuentra en una etapa de maduración ya que se está tratando de ampliar a través de cambios en la infraestructura tecnológica, por

ejemplo, con la migración de servidores a equipos más robustos y seguros y considerando la continuidad de las operaciones. Así lo confirma la jefa del departamento de TI:

> "Existe un plan de contingencia que todavía en este momento se está tratando de ampliar ya que nosotros a nivel técnico, estamos haciendo cambios a nivel de infraestructura, migración de servidores, pero si tenemos a nivel de políticas el plan de contingencias y ahorita estoy trabajando para ampliarlo para el tema de continuidad" (Licenciada Lorena Arana, comunicación personal, 23 de agosto 2017).

A pesar de tener estas políticas de continuidad, existe algunas falencias en el resto de controles relacionados, que debe ser atendidos para lograr el nivel de cumplimiento esperado, por ejemplo, el tema de redundancias, ya que actualmente no se cuenta con ellas.

En la tabla siguiente, se muestra el nivel de cumplimiento actual del hospital en cuanto a los controles relacionados a la continuidad del negocio.

Tabla 17: Situación actual sobre continuidad del negocio.

Clausula de control	Nivel de cumplimiento Actual (%)
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	**50**
17.1 Continuidad de la seguridad de la información.	**50**
17.1.1 Planificación de la continuidad de la seguridad de la información.	50
17.1.2 Implantación de la continuidad de la seguridad de la información.	50
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	50
17.2 Redundancias.	**50**
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	50

Fuente: (Elaboración propia)

A continuación, se muestra el análisis completo de todas las cláusulas de control y controles establecidos en la normativa ISO 27001. Este análisis se caracteriza por ser del tipo cuantitativo al igual que las tablas presentadas en la sección anterior, pero al interpretarlo nos

permitirá tener una mejor visión de la información dada por las observaciones y entrevistas realizadas.

Los datos de nivel de cumplimiento, se establecieron con base tanto en las entrevistas, y observaciones, como en los criterios y experiencias del investigador.

Tabla 18: Situación actual de la seguridad de la información Hospital María.

Clausula de control	Nivel de cumplimiento Actual (%)
5. POLÍTICAS DE SEGURIDAD	**40**
5.1 Directrices de la Dirección en seguridad de la información.	40
5.1.1 Conjunto de políticas para la seguridad de la información.	40
5.1.2 Revisión de las políticas para la seguridad de la información.	40
6. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN	**44**
6.1 Organización interna.	**57**
6.1.1 Asignación de responsabilidades para la seguridad de la información.	30
6.1.2 Segregación de tareas.	80
6.1.3 Contacto con las autoridades.	80
6.1.4 Contacto con grupos de interés especial.	50
6.1.5 Seguridad de la información en la gestión de proyectos.	45
6.2 Dispositivos para movilidad y teletrabajo.	**30**
6.2.1 Política de uso de dispositivos para movilidad.	30
6.2.2 Teletrabajo.	N/A
7. SEGURIDAD DE LOS RECURSOS HUMANOS	**43**
7.1 Antes de la contratación.	**75**
7.1.1 Revisión	100
7.1.2 Términos y condiciones de contratación.	50
7.2 Durante el empleo.	**23**
7.2.1 Responsabilidades gerenciales	30
7.2.2 Concienciación, educación y toma de conciencia para la seguridad de la información.	0
7.2.3 Proceso disciplinario.	40
7.3 Terminación o cambio de puesto de trabajo.	**30**
7.3.1 Terminación o cambio de puesto de trabajo.	30
8. GESTIÓN DE ACTIVOS.	**41**
8.1 Responsabilidad sobre los activos.	**85**
8.1.1 Inventario de activos.	80
8.1.2 Propiedad de los activos.	80
8.1.3 Uso aceptable de los activos.	80
8.1.4 Devolución de activos.	100
8.2 Clasificación de la información.	**0**
8.2.1 Directrices de clasificación.	0
8.2.2 Etiquetado y manipulado de la información.	0
8.2.3 Manipulación de activos.	0

Clausula de control	Nivel de cumplimiento Actual (%)
8.3 Manejo de medios	**37**
8.3.1 Gestión de medios removibles.	30
8.3.2 Disposición de medios	40
8.3.3 Trasferencia física de medios	40
9. CONTROL DE ACCESOS.	**76**
9.1 Requisitos de negocio para el control de accesos.	**85**
9.1.1 Política de control de accesos.	75
9.1.2 Control de acceso a las redes y servicios asociados.	95
9.2 Gestión de acceso de usuario.	**50**
9.2.1 Registro de usuarios y desregistro.	50
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	50
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	70
9.2.4 Gestión de información confidencial de autenticación de usuarios.	50
9.2.5 Revisión de los derechos de acceso de los usuarios.	30
9.2.6 Retirada o adaptación de los derechos de acceso	50
9.3 Responsabilidades del usuario.	**100**
9.3.1 Uso de información confidencial para la autenticación.	100
9.4 Control de acceso a aplicaciones y sistemas.	**70**
9.4.1 Restricción del acceso a la información.	50
9.4.2 Procedimientos seguros de inicio de sesión.	75
9.4.3 Gestión de contraseñas de usuario.	75
9.4.4 Uso de herramientas de administración de sistemas.	75
9.4.5 Control de acceso al código fuente de los programas.	75
10. CRIPTOGRAFÍA	**0**
10.1 Controles criptográficos.	0
10.1.1 Política de uso de los controles criptográficos.	0
10.1.2 Gestión de claves.	0
11. SEGURIDAD FÍSICA Y AMBIENTAL.	**72**
11.1 Áreas seguras.	**90**
11.1.1 Perímetro de seguridad física.	95
11.1.2 Controles físicos de entrada.	75
11.1.3 Seguridad de oficinas, cuartos y ambientes	95
11.1.4 Protección contra las amenazas externas y ambientales.	90
11.1.5 El trabajo en áreas seguras.	95
11.1.6 Áreas de acceso público, carga y descarga.	90
11.2 Seguridad de los equipos.	**54**
11.2.1 Ubicación y protección de equipos.	75
11.2.2 Apoyo de servicios públicos.	70
11.2.3 Seguridad del cableado.	80
11.2.4 Mantenimiento de los equipos.	75
11.2.5 Salida de activos fuera de las dependencias de la empresa.	50
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	30
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	65
11.2.8 Equipo informático de usuario desatendido.	40
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	0

Clausula de control	Nivel de cumplimiento Actual (%)
12. SEGURIDAD EN LA OPERACIONES	**79**
12.1 Responsabilidades y procedimientos de operación.	**64**
12.1.1 Documentación de procedimientos de operación.	50
12.1.2 Gestión de cambios.	20
12.1.3 Gestión de capacidades.	90
12.1.4 Separación de entornos de desarrollo, prueba y producción.	95
12.2 Protección contra código malicioso.	**95**
12.2.1 Controles contra el código malicioso.	95
12.3 Copias de seguridad.	**50**
12.3.1 Copias de seguridad de la información.	50
12.4 Registro de actividad y supervisión.	**84**
12.4.1 Registro y gestión de eventos de actividad.	80
12.4.2 Protección de los registros de información.	80
12.4.3 Registros de actividad del administrador y operador del sistema.	80
12.4.4 Sincronización de relojes.	95
12.5 Control del software operativo	**95**
12.5.1 Instalación del software en sistemas en producción.	95
12.6 Gestión de la vulnerabilidad técnica.	**73**
12.6.1 Gestión de las vulnerabilidades técnicas.	50
12.6.2 Restricciones en la instalación de software.	95
12.7 Consideraciones de las auditorías de los sistemas de información.	**95**
12.7.1 Controles de auditoría de los sistemas de información.	95
13. SEGURIDAD EN LAS COMUNICACIONES	**47**
13.1 Gestión de la seguridad en las redes.	**68**
13.1.1 Controles de red.	75
13.1.2 Servicios de seguridad de redes	50
13.1.3 Segregación de redes.	80
13.2 Intercambio de información con partes externas.	**25**
13.2.1 Políticas y procedimientos de intercambio de información.	30
13.2.2 Acuerdos de intercambio.	30
13.2.3 Mensajería electrónica.	40
13.2.4 Acuerdos de confidencialidad y secreto.	0
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	**79**
14.1 Requisitos de seguridad de los sistemas de información.	**77**
14.1.1 Requerimientos de análisis y especificación de la seguridad de información	70
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	80
14.1.3 Protección de servicios de aplicaciones en transacciones	80
14.2 Seguridad en los procesos de desarrollo y soporte.	**71**
14.2.1 Política de desarrollo seguro de software.	N/A
14.2.2 Procedimientos de control de cambios en los sistemas.	50
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	65
14.2.4 Restricciones a los cambios en los paquetes de software.	80
14.2.5 Uso de principios de ingeniería en protección de sistemas.	50
14.2.6 Seguridad en entornos de desarrollo.	N/A
14.2.7 Externalización del desarrollo de software.	95

Clausula de control	Nivel de cumplimiento Actual (%)
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	60
14.2.9 Pruebas de aceptación.	95
14.3 Datos de prueba.	**90**
14.3.1 Protección de los datos utilizados en pruebas.	90
15. RELACIONES CON SUMINISTRADORES.	**46**
15.1 Seguridad de la información en las relaciones con suministradores.	**42**
15.1.1 Política de seguridad de la información para suministradores.	0
15.1.2 atención a la seguuridad en los acuerdos con proveedores.	50
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	75
15.2 Gestión de la prestación del servicio por suministradores.	**50**
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	70
15.2.2 Gestión de cambios en los servicios prestados por terceros.	30
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**42**
16.1 Gestión de incidentes de seguridad de la información y mejoras.	**42**
16.1.1 Responsabilidades y procedimientos.	30
16.1.2 Notificación de los eventos de seguridad de la información.	30
16.1.3 Notificación de puntos débiles de la seguridad.	30
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	50
16.1.5 Respuesta a los incidentes de seguridad.	30
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	75
16.1.7 Recopilación de evidencias.	50
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	**50**
17.1 Continuidad de la seguridad de la información.	**50**
17.1.1 Planificación de la continuidad de la seguridad de la información.	50
17.1.2 Implantación de la continuidad de la seguridad de la información.	50
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	50
17.2 Redundancias.	**50**
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	50
18. CUMPLIMIENTO.	**60**
18.1 Cumplimiento de los requisitos legales y contractuales.	**70**
18.1.1 Identificación de la legislación aplicable.	70
18.1.2 Derechos de propiedad intelectual (DPI).	70
18.1.3 Protección de los registros de la organización.	70
18.1.4 Protección de datos y privacidad de la información personal.	70
18.1.5 Regulación de los controles criptográficos.	N/A
18.2 Revisiones de la seguridad de la información.	**50**
18.2.1 Revisión independiente de la seguridad de la información.	50
18.2.2 Cumplimiento de las políticas y normas de seguridad.	50
18.2.3 Revisión del cumplimiento.	50

Fuente: **(**Elaboración propia)

En la siguiente tabla, se muestra el resumen del nivel de cumplimiento actual del HMEP por cada una de las cláusulas de control establecidas en la normativa.

Tabla 19: Condensado situación actual de la seguridad de la información.

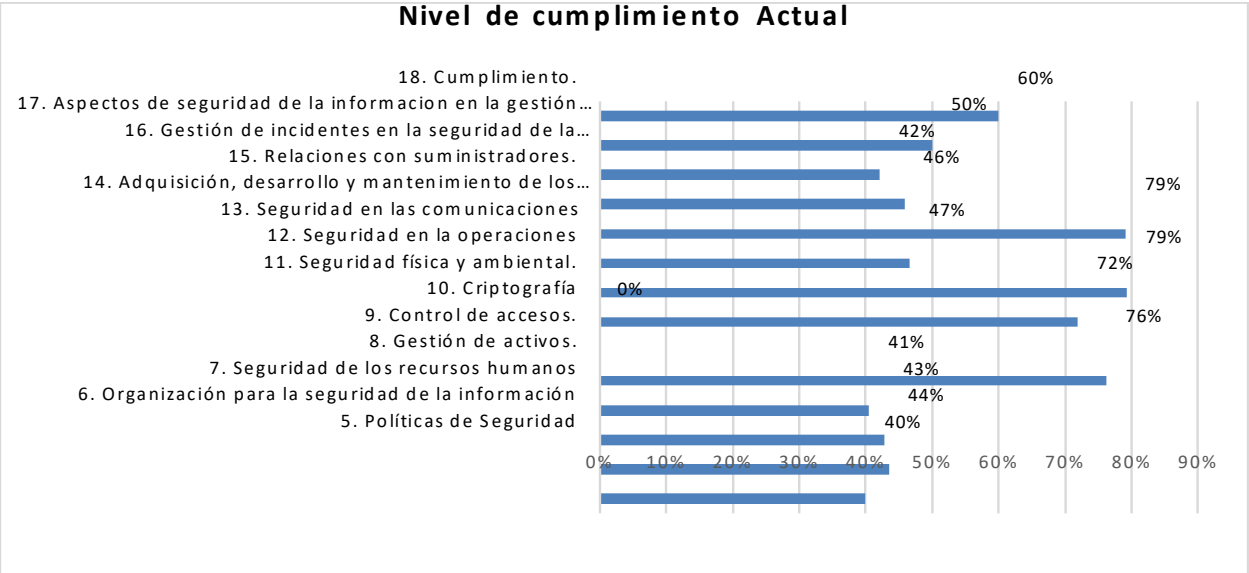
Clausula de Control	Descripción	Nivel de cumplimiento Actual (%)
5	Políticas de Seguridad	40
6	Organización para la seguridad de la información	44
7	Seguridad de los recursos humanos	43
8	Gestión de activos.	41
9	Control de accesos.	76
10	Criptografía	0
11	Seguridad física y ambiental.	72
12	Seguridad en la operaciones	79
13	Seguridad en las comunicaciones	47
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	79
15	Relaciones con suministradores.	46
16	Gestión de incidentes en la seguridad de la información.	42
17	Aspectos de seguridad de la informacion en la gestión de la continuidad del negocio.	50
18	Cumplimiento.	60

Fuente**:** (Elaboración propia)

Como se puede observar en la tabla anterior, en la mayoría de las cláusulas de control se obtiene una calificación inferior a un 80% que para efectos de esta investigación se considera debe ser el nivel mínimo de cumplimiento que se debería tener para garantizar la seguridad la información del Hospital María especialidades pediátricas y que se esperaría alcanzar si se decide implementar el modelo planteado en esta investigación.

En la siguiente gráfica, se puede apreciar de mejor manera lo expuesto en la tabla 19

Gráfico 2: Nivel actual de cumplimiento de la seguridad de la información.



Fuente**:** (Elaboración Propia)

A continuación, se muestra una gráfica comparativa de la situación actual y el nivel de cumplimiento deseado, que sería el resultado si se decidiera implementar el sistema.

Gráfico 3: Evolución sobre las cláusulas de seguridad.

Fuente**:** (Elaboración Propia)

5 CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. El Hospital María Especialidades Pediátricas está realizando grandes esfuerzos por garantizar la seguridad de la información de sus pacientes, tal como demuestra en lo hallazgos plasmados en el capítulo anterior, a través de la implementación de algunos controles y procedimientos generales, así como con la adquisición de nuevos sistemas de información más robustos y seguros. Pero debido a la falta de una política específica y orientada exclusivamente a la seguridad de la información, la salvaguarda de esta no puede garantizarse en un 100%.
2. Una vez analizada la situación actual de la organización, se puede determinar que los lineamientos existentes de seguridad como control de accesos físicos y lógicos, seguridad física y ambiental, firewalls y antivirus entre otros controles aplicados, funcionan manera correcta hasta cierto punto deben ser reforzadas en términos de implementación de otros controles, para lograr su adecuando funcionamiento y cumplimiento.
3. Con base en lo planteado en el análisis de los resultados, se ha demostrado que el hospital es vulnerable a múltiples amenazas como, robo, fuga o pérdida de información, y principalmente a ataques de hackers, por lo que es necesaria la implementación de un sistema de detección de espías, para evitar que estos puedan tener acceso a información confidencial de la organización.

4. En lo referente al análisis y evaluación de riesgos y amenazas, se concluye que son manejables y pueden ser mitigados a través de la implementación de controles aplicables a este alcance. Sin embargo, si la dirección decide implementar este sistema, es necesario un análisis más exhaustivo para la definición del alcance global de la organización.
5. Con el desarrollo de la investigación y el estudio de la normativa ISO 27001, se puede valorar como el rápido crecimiento de la tecnología ha llevado a las organizaciones en el mundo a verse expuestas y vulnerables a riesgos antes no pensados, en uno de sus activos más importantes como es la información y el Hospital María no está exento de estos peligros. Por tal motivo, se ha dado la necesidad de crear conciencia de la importancia vital que tiene la información dentro de la organización y por ende a implementar los modelos, sistemas y reglas que provean el correcto manejo de esta y que reduzcan y/o eviten los riesgos a los que se ve expuesta, ya que, de no contar con una estrategia definida como la planteada en el manual de seguridad diseñado, la ocurrencia de uno o más de estos escenarios podría llevarlo al colapso total.

5.2 Recomendaciones

1. Del análisis de datos, se ha detectado la falta de algunos documentos importantes que pueden ayudar con la implementación y cumplimiento del SGSI, por lo que se recomienda documentar e implementar los siguientes procesos:
    - Proceso de Control de Documentos.
    - Proceso de Control del Registro.

- Proceso de Capacitación del Personal.
- Proceso de Manejo de Auditorías Internas.
- Proceso de Manejo de Acción Correctiva.
- Proceso de Manejo de Acción Preventiva.
- Proceso de Reporte de Eventos e Incidentes de Seguridad.

2. Debido a las vulnerabilidades y amenazas que representan los hackers hoy en día y a los antecedentes detectados en el análisis de datos, se recomienda implementar un programa de pruebas de penetración y realizarlo con cierta frecuencia para poder detectar en tiempo los intentos de intrusión que se puedan presentar.
3. Dado que se consideran factores críticos de éxito que se deben considerar a la hora de implementar un sistema de esta naturaleza, se recomiendan los siguientes:
    - Establecimiento de políticas y objetivos de seguridad como los propuestos en este trabajo de investigación y acordes a los objetivos de la organización.
    - Crear conciencia de la importancia vital que tiene la información dentro de la organización y evaluar de manera continua al personal de tal manera que se garantice el correcto uso de los recursos tecnológicos y de la información considerada como confidencial.
4. Reforzar las medidas de seguridad en los equipos de la alta dirección administrativa y clínica, para que, ante una eventual pérdida o daño de uno de estos activos, no se vea comprometida la seguridad y confidencialidad de la

información. Esto podría lograrse a través de borrados remotos de información o mediante técnicas de encriptación.

5. Utilizar el actual sistema de gestión de tickets, creando un apartado específico, para que, a través de este, se puedan reportar y registrar los eventos de seguridad de información que puedan presentarse en la operación cotidiana del hospital. Esta recomendación se hace considerando que la documentación generada por esta herramienta será de vital importancia para las respuestas ágiles y eficientes a los eventos e incidentes. Esto significa que en la medida que se documenten las políticas y los procedimientos antes, durante y después de la ocurrencia de los incidentes, estos se podrán manejar y resolver de la manera más adecuada.
6. En vista de que actualmente el hospital está en proceso de implementación de un nuevo sistema de información de gestión administrativa y clínica, que considera los aspectos de seguridad de la información, se sugiere la automatización de algunos procedimientos como, por ejemplo, las visitas médicas a las salas de hospitalización. Para este tema en particular, se recomienda el uso de iPads o en su defecto computadoras portátiles para que los médicos puedan visualizar la información de los pacientes e indicar el plan médico correspondiente, logrando digitalizar la información, evitando posibles pérdidas de expedientes físicos.
7. Se recomienda al hospital mantenerse a la vanguardia de la tecnología mediante la adquisición servidores más robustos para el manejo y cuidado de la información de la institución, considerando las posibles ampliaciones a futuro en su cartera de servicios, lo que también evitará inversiones adicionales en servidores.

En este apartado, también se recomienda el uso de la virtualización, ya que esta tecnología puede aportar diversos beneficios porque permite una utilización más eficiente de los recursos de Tecnologías de Información y Comunicación.

8. Uno de los activos de información más valiosos con los que cuenta el hospital, es su Data Center, por lo que debe protegerse de la manera más adecuada. Actualmente el sitio solamente cuenta con un dispositivo de aire acondicionado, por lo que se recomienda la instalación de un segundo dispositivo, que actúe como respaldo del primero cuando este no pueda operar correctamente. Adicionalmente se sugiere la instalación de un sensor dentro de este sitio, con el objetivo de controlar la humedad relativa a la que deben operar los equipos. Todo esto con el fin primordial de salvaguardar la información contenida en estas unidades.
9. Se recomienda al Hospital María la adquisición de un sistema de redundancia de redes para poder mantener una alta disponibilidad de los servicios en caso de una falla o caída del sistema. Esto podría lograrse a través de la gestión del ente regulador (Secretaria de Salud) ante la Comisión Nacional de Telecomunicaciones (Conatel). Con esta redundancia, se lograría que el sistema detecte el fallo del mismo y que, además, reaccione de manera rápida y eficiente en la búsqueda de una solución a la caída.

6 CAPÍTULO 6

APLICABILIDAD

A continuación, se establece el manual de seguridad de la información que es uno de los objetivos específicos de este trabajo y que servirá de guía para la implementación de un SGSI para el Hospital María Especialidades Pediátricas, atendiendo la metodología planteada en el capítulo 3.

6.1 Alcance

Tal como se estableció al inicio de este capítulo, el alcance del SGSI contempla el departamento de Tecnologías de la Información y Comunicaciones del Hospital María Especialidades Pediátricas.

6.2 Política de seguridad

El HMEP califica como activo primordial y estratégico la información por lo que se debe proteger con los métodos que un activo de gran valor merece.

Tal como se estableció en la sección 3.7.3 de la metodología, la Política de Seguridad de la información debe ser establecida por la alta gerencia del hospital. En vista que no se cuenta con una política establecida, se sugiere la siguiente:

La seguridad de la información es de gran importancia por lo que se deben mantener los principios fundamentales de confidencialidad, integridad y disponibilidad de la información por todos y cada uno de los empleados del Hospital María, volviéndose un hábito dentro de la cultura organizacional el manejo de la seguridad de la información.

El Hospital María mantendrá un Sistema de Gestión de seguridad de la información con la finalidad primordial de reducir los riesgos a los que se vea expuesta la información y fortalecer

la cultura de análisis y evaluación de riesgos, desde la óptica de la confidencialidad, integridad y disponibilidad de la información.

Para que esta política de seguridad pueda ser medible en el tiempo, se propone adoptar los siguientes objetivos de seguridad:

1. Capacitar a los empleados en buenas prácticas de seguridad de la información
2. Registrar, controlar y minimizar los incidentes de seguridad.
3. Minimizar la ocurrencia de acontecimientos de seguridad que se conviertan en incidentes.

6.3 Partes interesadas Sistema de Gestión de Seguridad de la Información

Dado que el modelo está concebido para que opere con base en insumos provenientes de las partes interesadas, si a la alta dirección del hospital decidiera implementar esta metodología, se definen las mismas para el SGSI del Hospital María Especialidades Pediátricas como:

Empleados: deberán ser retroalimentados a través de constante comunicación de la implementación y los cambios al SGSI, para poder promover una cultura organizacional de seguridad de Información.

Pacientes: Los pacientes del hospital deberán ser retroalimentados de manera constante por medio de eventos organizados para este fin y campañas que les brinden información sobre la capacidad del HMEP para salvaguardar la seguridad de su información.

Proveedores/Contratistas: Deberán ser informados de las políticas de seguridad del hospital y luego se les debe exigir el cumplimiento de un plan de capacitación y retroalimentación previamente definido para ellos.

Junta Directiva: La retroalimentación debe ser anual mediante una presentación.

6.4 Relación entre Política de Seguridad, Objetivos de Seguridad, Indicadores y Criterios de Evaluación del Riesgo

La relación de entre la Política de Seguridad, los Objetivos de Seguridad, los Indicadores y los Criterios de Evaluación del Riesgo se puede apreciar en la siguiente tabla:

Tabla 20: Relación entre la Política, los Objetivos de Seguridad, los Indicadores y los Criterios de Evaluación del Riesgo.

Política de Seguridad de la Información	Objetivos de Seguridad	Indicadores de Medición	Criterios de Evaluación del Riesgo
La seguridad de la información es de gran importancia por lo que se deben mantener los principios fundamentales de confidencialidad, integridad y disponibilidad de la información por todos y cada uno de los empleados del Hospital María, volviéndose un hábito dentro de la cultura organizacional el manejo de la seguridad de la información. El Hospital María mantendrá un Sistema de Gestión de seguridad de la información con la finalidad primordial de reducir los riesgos a los que se vea expuesta la información y fortalecer la cultura de análisis y evaluación de riesgos, desde la óptica de la confidencialidad, integridad y disponibilidad de la información	1. Capacitar a los empleados en buenas prácticas de seguridad de la información	Que al menos el 70% de los empleados asista al menos a 8 horas de capacitación anual sobre el SGSI.	• Impacto económico del riesgo • Tiempo de Recuperación de la Empresa • Posibilidad de Ocurrencia • Posibilidad de Interrumpir actividades de la empresa • Imagen/ Reputación
	2. Registrar, controlar y minimizar los incidentes de seguridad.	Disponibilidad de la red de un 99%, Registro de incidentes en el Gis (Help Desk)	
	3. Minimizar la ocurrencia de acontecimientos de seguridad que se conviertan en incidentes.	Numero de eventos que se convirtieron en incidentes/número de eventos.	

Fuente: (Elaboración Propia)

6.5 Enfoque para la evaluación del riesgo

Para la implementación de esta metodología, el hospital debe conformar un comité gerencial multidisciplinario para que evalúen los factores que podrían tener un impacto en la operativa de la organización.

Para efectos de esta investigación, se utilizará la metodología expuesta en la sección 2.2.4 del capítulo 2 y que también se menciona en la sección 3.7.4 del capítulo 3.

y que incluye:

1. Establecimiento del alcance mediante la metodología de las elipses
2. Identificación y Tasación de activos
3. Identificación de amenazas
4. Posibilidad de ocurrencia de las amenazas
5. Identificación de vulnerabilidades
6. Posible explotación de vulnerabilidades
7. Estimados del valor de los activos en riesgo
8. Posibilidad de ocurrencia del riesgo
9. Valor del riesgo de los activos

6.5.1 Paso 1: Metodología de las elipses.

Esta metodología permite identificar con precisión las interfaces y dependencias del SGSI con otras partes de la organización y actores externos.

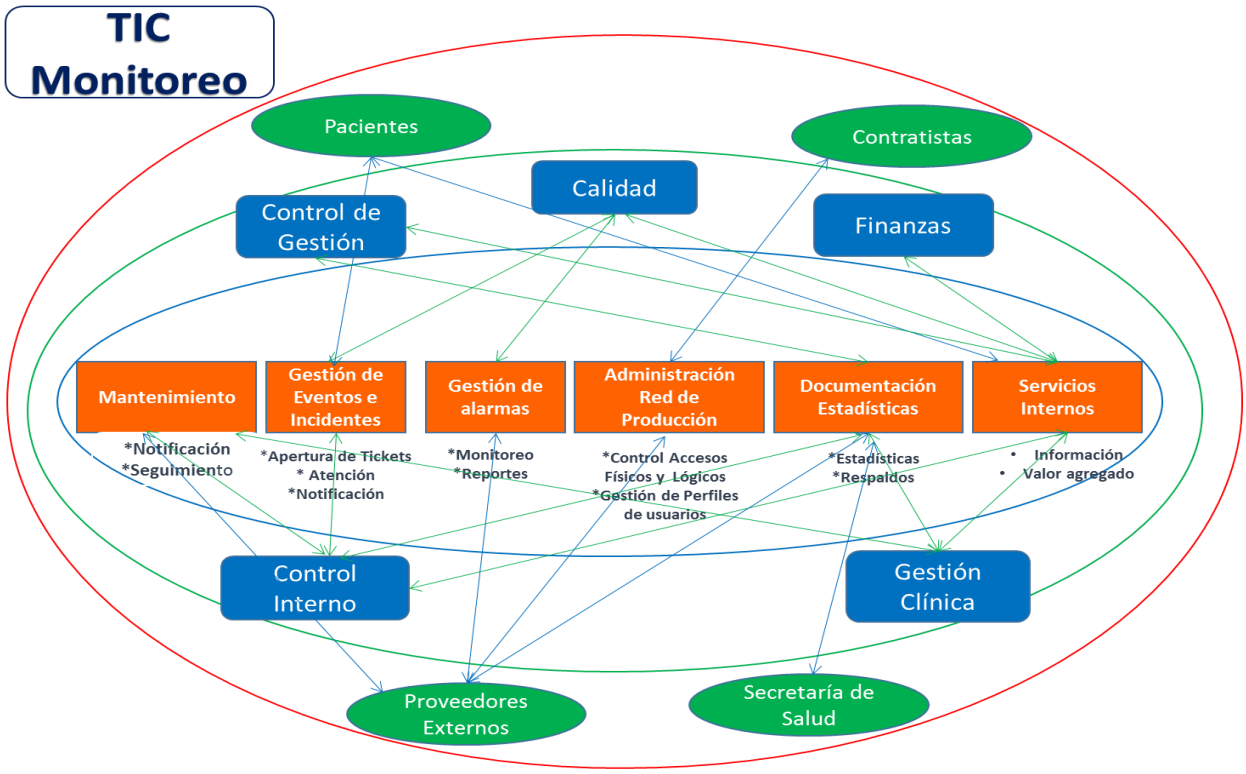
El primer paso consiste en determinar en la elipse concéntrica los distintos procesos y subprocesos que conforman el alcance del SGSI. (En este caso, el Departamento de Tecnologías de Información y Comunicaciones, ejemplificando el proceso de monitoreo).

El segundo paso consistió en identificar en la elipse intermedia las distintas interacciones que los procesos de la elipse concéntrica tienen con otros procesos de la organización.

En la elipse externa, identificamos aquellos actores extrínsecos a la empresa que tienen cierto tipo de interacción con los procesos y subprocesos identificados en la elipse concéntrica.

Finalmente, las flechas indican el tipo de interacción, y la direccionalidad que tiene el flujo de información, tal como se muestra en la siguiente figura:

Figura 5: Alcance del Sistema de seguridad de la Información



Fuente: (Elaboración Propia)

6.5.2 Paso 2: Identificación y Tasación de Activos.

Un Activo es cualquier cosa que tenga valor para la organización. Según el ISO 27002 código de Practica para la Gestión de Seguridad de información, un activo de información es "algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".

Existen varias categorías de activos de información, las cuales son clasificadas por el ISO 27002:2005, de la siguiente manera:

- Activos de información
- Documentos de papel
- Activos de Software
- Activos físicos
- Personal
- Imagen de la compañía y reputación
- Servicios

Estos activos, relacionados a los procesos identificados en el alcance del SGSI deben ser identificados y a su vez tasados considerando su impacto en la empresa por su deterioro o por sus fallas en:

- Confidencialidad
- Integridad
- Disponibilidad

Se tasan utilizando una escala de Likert de 5 puntos, como se muestra en la siguiente tabla:

Tabla 21: Valoración de Activos.

Valor	Descripción	Puntaje
Muy poco	Ante una falla o pérdida la afectación de la confidencialidad, integridad o disponibilidad prácticamente no se ve afectada.	1
Poco	Ante una falla o pérdida la afectación de la confidencialidad, integridad o disponibilidad de la información sufre un impacto menor.	2
Regular	Ante una falla o pérdida la afectación de la confidencialidad, integridad o disponibilidad de la información es impactada a una escala media y se necesita tomar acción del propietario.	3
Alto	Ante una falla o pérdida la afectación de la confidencialidad, integridad o disponibilidad de la información es altamente impactada se requeriría utilización significativa de recursos para poder recobrar la estabilidad del SGSI	4
Muy Alto	Ante una falla o pérdida la afectación de la confidencialidad, integridad o disponibilidad de la información compromete todo el sistema se requiere inmediata intervención de Gerencia General y utilización significativa de recursos para recobrar la estabilidad del SGSI.	5

Fuente: (Elaboración Propia)

La pregunta efectuada es: "¿Cómo una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?"

En el Anexo 2 (Tasación de Activos) se tiene el resultado final de la tasación efectuada al alcance del sistema en la organización.

Una vez efectuado el proceso de tasación, se considerarán como activos de impacto para la organización, solamente aquellos que tuvieron una puntuación comprendida en un rango comprendido entre 3 y 5.

6.5.3 Paso 3: Análisis del Riesgo.

En esta etapa se efectúa el análisis del riesgo llegando a identificar estimados de riesgo por cada activo de información.

6.5.3.1 Identificación de Amenazas y Vulnerabilidades.

Una amenaza es una indicación de un evento desagradable con el potencial de causar daño.

El próximo paso nos condujo a identificar las distintas amenazas que pueden afectar a un activo y luego se evaluó su posibilidad de ocurrencia.

Para esto usamos la escala Likert de 5 puntos

Tabla 22: Posibilidad de Ocurrencia de la Amenaza

Probabilidad	Descripción	Puntaje
Baja	Muy rara vez	1
Mediana	Hasta dos veces al Año	2
Alta	Hasta una vez al mes	3
Muy alta	Más de una vez al mes	4
Extrema	Varias veces a la semana o al día	5

Fuente: (Elaboración Propia)

Se consideran amenazas de impacto aquellas que obtuvieron un puntaje entre 3 y 5 de la tabla antes mencionada. Aquellas amenazas que obtuvieron un puntaje comprendido entre 1 y 2 no se consideraron.

Seguidamente se identifican las vulnerabilidades de cada activo de información en relación a las amenazas previamente identificadas.

Una vulnerabilidad por sí sola no causará un daño, estas, más bien son condiciones o medios que pueden hacer que una amenaza afecte un activo. Por esta razón las vulnerabilidades deben ser identificadas y las posibilidades de que sean explotadas por la amenaza se evalúan usando una escala Likert como se muestra a continuación:

Tabla 23: Posibilidades de que las Vulnerabilidades sean Explotadas por las Amenazas.

Probabilidad	Descripción	Puntaje
Baja	Muy rara vez	1
Mediana	Hasta dos veces al Año	2
Alta	Hasta una vez al mes	3
Muy alta	Más de una vez al mes	4
Extrema	Varias veces a la semana o al día	5

Fuente: (Elaboración Propia)

Aquellas vulnerabilidades que obtuvieron un valor comprendido entre 3 y 5 se consideraron de importancia para la organización. El resto de las vulnerabilidades no se toman en cuenta por considerarse irrelevantes.

El impacto del riesgo si ocurriera, en este caso, se evalúa considerando el impacto económico que tendría en la organización la perdida de la integridad, confidencialidad e integridad de un activo de información importante o crucial. El puntaje se asigna mediante una escala de Likert, como se observa en la siguiente tabla:

Tabla 24: Impacto del Riesgo.

Nivel de Impacto	Porcentaje basado en la facturación mensual	Puntaje
Menor	0-2%	1
Significativo	3-9%	2
Dañino	10-14%	3
Serio	15-29%	4
Grave	30% o mas	5

Fuente: (Elaboración Propia)

El último paso consiste en estimar el riesgo (Estimado del Riesgo Total), multiplicando los valores obtenidos del Impacto del Riesgo por la Posibilidad de Ocurrencia de las Amenazas. (Ver Anexo 3 Análisis de Riesgo)

6.5.4 Paso 4: Evaluación del Riesgo.

El proceso de evaluación del riesgo consiste en determinar aquellos riesgos considerados más significativos para la organización. Los criterios empleados para determinar aquellos riesgos más importantes son los siguientes:

Tabla 25: Criterios de evaluación del riesgo.

Impacto del Riesgo	Nivel de daño que el riesgo pudiese generar en los activos de información
Tiempo de recuperación de la organización	El tiempo que la empresa se tomaría en recuperarse de los daños causados por el impacto del riesgo
Posibilidad de ocurrencia	La probabilidad de que el riesgo se presente
Probabilidad de interrumpir las actividades de la empresa	El grado en el cual el riesgo pudiese paralizar actividades en la empresa
Imagen y Reputación	El grado de daño que el riesgo pudiese ocasionar en la marca de la empresa

Fuente: (Elaboración Propia)

El impacto del riesgo se estima según la escala de Likert mostrada en la tabla 22.

El tiempo de recuperación de la organización se evalúa según la escala de Likert de 5 puntos, como se muestra en la tabla siguiente:

Tabla 26: Tiempo de recuperación de la Organización

Tiempo de Recuperación	Descripción	Puntaje
Menor	No se requiere esfuerzo extra para reparar, recuperar o reemplazar el o los activos dañados	1
Significativo	Se requiere esfuerzo extra para reparar, recuperar o reemplazar el o los activos dañados	2
Dañino	Se requiere una utilización significativa de recursos para reparar, recuperar o reemplazar el o los activos dañados	3
Serio	Extendida paralización y pérdida de conectividad. Se comprometen grandes cantidades de datos y servicios	4
Extremo	Permanente paralización. Compromete todo el sistema.	5

Fuente: (Elaboración Propia)

La posibilidad de ocurrencia del riesgo se calcula según la misma escala de Likert mostrada en la tabla 20.

La posibilidad de interrumpir las actividades de la empresa se evalúa según la escala de Likert mostrada en la siguiente tabla:

Tabla 27: Posibilidad de Interrumpir las actividades de la organización

Probabilidad	Puntaje
Baja	1
Mediana	2
Alta	3
Muy alta	4
Extrema	5

Fuente: (Elaboración Propia)

El criterio de imagen y reputación se estima aplicando la escala de Likert representada en la siguiente tabla:

Tabla 28: Posibilidad de Afectar la Imagen y/o Reputación de la organización

Probabilidad	Puntaje
Ninguna	1
Baja	2
Mediana	3
Alta	4
Extrema	5

Fuente: (Elaboración Propia)

Seguidamente, el Riesgo Total se debe calcular realizando la suma de los resultados de los criterios mencionados anteriormente.

La metodología completa utilizada en la "Evaluación del Riesgo", se muestra en el anexo 4 (Evaluación del Riesgo).

Como resultado de la evaluación, se identifican los criterios para la aceptación de los riesgos y los niveles de riesgo aceptables. Para dicho efecto se utiliza la información plasmada en la siguiente tabla:

Tabla 29: Criterios para la Aceptación de los Riesgos y Niveles de Riesgo Aceptables

Rango de Riesgos	Niveles de Riesgo
5-7	Aceptable
8-10	Bajo
11-14	Medio
15-18	Alto
19-21	Muy Alto

Fuente: (Elaboración Propia)

6.5.5 Paso 5: Opciones de Tratamiento.

Una vez identificados los riesgos que tienen los activos de información, y teniendo los criterios para la aceptación de los riesgos y los niveles de riesgo aceptables identificados, se deben tomar las decisiones relacionadas a las distintas opciones disponibles para el tratamiento del riesgo que son: Reducir, Aceptar, Evitar y Transferir.

6.5.5.1 Controles.

Los controles que Apoyan el SGSI pueden ser apreciados en la Declaración de Aplicabilidad, plasmada en el Anexo 7 de este Manual de Seguridad.

6.5.6 Paso 6: Tratamiento del Riesgo

El Plan de Tratamiento del Riesgo es un proyecto en el que se planifican las actividades a realizar para poder implantar las decisiones relacionadas con los objetivos de control y controles previamente seleccionados. Cada actividad de implementación debe ser identificada con claridad y desagregada en una gama de sub-actividades requeridas para poder distribuir las responsabilidades a personas, estimar los requerimientos de recursos y asignar fechas críticas para el proyecto. (En el Anexo 5 se muestra un ejemplo de un Plan de Tratamiento del Riesgo del riesgo para los activos de información que no resultaron aceptados en la evaluación del riesgo)

6.5.7 Riesgo residual

El riesgo residual, es aquel remanente después de haber implementado las opciones de tratamiento del riesgo. (Ver Anexo 6, Riesgo Residual)

6.6 Reporte de Evaluación del Riesgo

Este documento se debe elaborar a partir de los anexos 2, 3, 4, 5 y 6 referentes a análisis y Evaluación del Riego.

6.7 Monitoreo de eficacia

Todos los controles identificados y aplicados en el Plan de Tratamiento del Riesgo, deben tener un indicador para poder medir en el tiempo su eficacia. De esta manera la organización obtiene una métrica que le permite conocer de manera precisa el nivel o grado de funcionamiento de los controles implementados.

6.8 Reevaluación de riesgo

La reevaluación del riesgo en el sistema de gestión de seguridad de la información debe realizarse de manera anual, con el objetivo de mantener actualizados los activos de información, controles y opciones de tratamiento para el mantenimiento correcto de la seguridad de la información.

7 LISTA DE REFERENCIAS

Aeritio J, J. (2008). Seguridad de la información. Redes, informática y sistemas de información (1.ª ed.). España: Paraninfo.

Alexander, A. G. (2007a). Diseño de un sistema de gestión de seguridad de información. Colombia: Alfa y Omega.

Alexander, A. G. (2007b). Diseño de un Sistema de Gestión de Seguridad de Información (1.ª ed.). Colombia: Alfa y Omega.

Alexander, A. G. (2014). Análisis e Interpretación de un Sistema de Gestión de Seguridad de Información ISO27001:2013.

Ernest & Young. (2015). Encuesta Global de Seguridad de Información 2015. Recuperado a partir de https://www.ey.com/PE/EYPeruLibrary

Fondonorma, F. (2007). Tecnología de la información. Técnicas de seguridad. Código de prácticas para la gestión de la seguridad de la información. Recuperado a partir de http://www.fondonorma.org.ve/

Gutierrez, R. (2016). ¿Cómo legisla Honduras la protección de sus datos? Recuperado a partir de https://revistaitnow.com/legisla-honduras-la-proteccion-datos/

IAIP. Ley de Protección de datos personales (2015). Recuperado a partir de http://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf

López Carballo, D. (2014). El secreto médico en Honduras y la protección de la privacidad de las personas. Recuperado a partir de http://dlcarballo.com/2014/06/05/el-secreto-medico-en-honduras-y-la-proteccion-de-la-privacidad-de-las-personas/

Merino Bada, C. (2011). Implantación de un sistema de gestión de seguridad de la información según ISO 27001 (1.ª ed.). España: Fundación Confemetal.

Sánchez-Henarejos, A. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria.

Temperini, M. (2014). Delitos Informáticos en Latinoamérica. Recuperado a partir de http://43jaiio.sadio.org.ar/proceedings/SID/13.pdf

8 ANEXOS

Anexo 1
Cuestionario

Con el fin de poder analizar la situación actual del Hospital María Especialidades Pediátricas en cuanto a seguridad de la información se refiere, se aplica el siguiente cuestionario para su posterior análisis y presentación de resultados. Por favor contestar de forma clara, precisa y con la mayor sinceridad posible.

1. ¿Se tiene definida y documentada una política de seguridad de información dentro del Hospital? Por favor explique su respuesta

2. ¿Cuál es la importancia de la información de los pacientes?

3. ¿Cómo se garantiza la seguridad de la información de los pacientes?

4. ¿Quiénes o quien tienen acceso a la información de los pacientes?

5. ¿Se cuenta con un plan de contingencia ante una caída de los servidores?
   Por favor explique su respuesta.

6. ¿El hospital cuenta con metodologías y/o procesos para la seguridad de la información?
   Por favor explique su respuesta.

7. ¿De qué manera se puede asegurar y medir la idoneidad, eficiencia y eficacia de las políticas de seguridad?

8. ¿Se cuenta con algún acuerdo de confidencialidad?
   Por favor explique su respuesta.

9. ¿Cuáles son las políticas que se tienen para la divulgación de la información?

10. ¿Existe perfiles de acceso de usuario?
    Por favor explique su respuesta.

11. ¿El hospital tiene definidos roles y responsabilidades en seguridad de información?
    Por favor explique su respuesta.

12. ¿Se tiene definidas las restricciones de acceso?
    Por favor explique su respuesta.
13. ¿Se tienen establecidos procedimientos para el uso eficiente de la información y de los activos asociados? Ejemplo uso de correo electrónico o de Teléfonos celulares.
    Por favor explique su respuesta.

14. ¿Cuenta el hospital con un plan de contingencia en caso de pérdida de información?
    Por favor explique su respuesta.

15. ¿Se tiene documentada la importancia de los activos de información?
    Por favor explique su respuesta.

16. ¿Cuál es el nivel de protección de los activos de información de mayor importancia?

17. ¿Se establecen controles criptográficos para proteger la información?
    Por favor explique su respuesta.

18. ¿Se pueden retirar los equipos o programas fuera de la oficina?
    Por favor explique su respuesta.

19. ¿El hospital cuenta una política de acceso a los servidores de la red?
    Por favor explique su respuesta.

20. ¿Se tiene establecidos procedimientos para otorgar privilegios, así como para revocarlos?
    Por favor explique su respuesta.

21. ¿Con que frecuencia se realizan los Back-up de la información crítica?
    Por favor explique su respuesta.

22. ¿EL hospital ha sido atacado por hackers en alguna ocasión?
    Por favor explique su respuesta.

23. ¿Se tienen procedimientos establecidos para que los usuarios de los sistemas tengan conocimientos de los posibles ataques?
    Por favor explique su respuesta.

24. ¿Se realiza una gestión de versiones de las aplicaciones?
    Por favor explique su respuesta.

25. ¿Se realizan monitoreos para verificar que no instale software no autorizado y productos sin licencia? Por favor explique su respuesta.

26. ¿se ha establecido alguna política de protección y privacidad de la data?
    Por favor explique su respuesta?

Anexo 2

Tasación de activos de información

Hospital María Especialidades Pediatricas				
Tasación de Activos				
Activos	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Total**
Técnicos de Informática	1	3	3	2
Formato de solicitud de materiales	1	3	3	2
Red de Producción	5	5	5	5
Administrador de Redes	5	3	3	4
Correo Electronico	4	4	3	4
Contratos Proveedores	3	2	2	2
Servicio de Facturación	2	2	3	2
Gestor de Tickets (GIS)	5	3	3	4
ERP	5	3	4	4
Servicio de Telefonía	2	2	3	2
Base de datos de Pacientes	5	4	4	4
Base de datos de proveedores y contratistas	3	3	3	3
Jefe de IT	5	4	3	4
Fibra optica	1	5	5	4
Celular de empleados TIC	1	2	3	2
Laptops equipo Gerencial y Staff Clínico	5	5	4	5
Desktop Operaciones Tecnicas	3	2	2	2
Proveedores	3	4	4	4
Contratistas	2	2	3	2
Pacientes	1	1	1	1
Reportes de proveedores	2	2	2	2
Reportes de contratistas	1	4	2	2

Anexo 3
Análisis del Riesgo

Hospital María Especialidades Pediatricas						
Analisis de Riesgos						
Activos	**Amenazas**	**Posibilidad de ocurrencia de amenaza**	**Vulnerabilidades**	**Posibilidades de ser de las vulnerabilidades explotadas por las amenazas**	**Impacto economico del riesgo**	**Total (Estimado del Riesgo total)**
Red de Producción	Virus	3	Mal uso de recursos	3	3	9
	Sabotaje	3	Insatisfacción de contratistas y proveedores	3		
			ó de exempleados	3		
	Ataques de Hackers	3	Falla en seguimiento a control de accesos físicos y lógicos	3		
Administrador de Redes	Robo de información	3	Baja efectividad de controles implantados	2	1	3
	Error humano	1	Falta de revisión y verificación en la labor que desempeña, por falta de conocimiento o compromiso	1		
	Divulgación de información confidencial	3	Baja efectividad de controles implantados	1		
Correo Electrónico	Disponibilidad	3	Mal uso de recursos	2	2	6
			Daño de Hadware/software	3		
	Virus	3	Mal uso de recursos	3		
Gestor de Tickets (GIS)	Ataque de Virus	3	Falla en la política de actualización de antivirus y/o firewall de protección del servidor	2	2	6
ERP	Disponibilidad	3	Caída de servicio	2	2	6
			Falta de notificaciones sobre mantenimientos y caídas por parte del administrador.	2		
	Pérdida de Información	2	Ataque de hackers	2		

Hospital María Especialidades Pediatricas						
Analisis de Riesgos						
Activos	**Amenazas**	**Posibilidad de ocurrencia de amenaza**	**Vulnerabilidades**	**Posibilidades de ser de las vulnerabilidades explotadas por las amenazas**	**Impacto economico del riesgo**	**Total (Estimado del Riesgo total)**
Base de datos de Pacientes	Fallas de integridad de la información	3	Configuraciones erróneas de los sistemas de Información	2	2	6
	Indisponibilidad de la información	2	Que no se encuentre en un lugar accesible a las areas que le requieran.			
Base de datos de proveedores y contratistas	Información desactualizada	2	Fallas de conectividad	2	1	3
	Falta de disponibilidad	3	Que no se encuentre en un lugar accesible a las áreas que le requieran.	3		
Jefe de IT	Robo de información	3	Baja efectividad de controles implantados	2	1	3
	Error humano	3	Falta de revisión y verificación en la labor que desempeña, por falta de conocimiento o compromiso,	2		
	Divulgación de información confidencial	3	Baja efectividad de controles implantados	2		
Fibra óptica	Sabotaje Físico	3	Exposición de cables aéreos	5	4	16
	Error humano	2	Falta de revisión y ó en la labor que desempeña, por falta de conocimiento o compromiso, falta de capacitación.	2		
	Incendio	2	Exposición de cables aereos	2		
	Robo	4	Exposición de cables aereos	4		
	Ataque de Animales	4	Exposición de cables aereos	5		

Hospital María Especialidades Pediatricas						
Analisis de Riesgos						
Activos	**Amenazas**	**Posibilidad de ocurrencia de amenaza**	**Vulnerabilidades**	**Posibilidades de ser de las vulnerabilidades explotadas por las amenazas**	**Impacto economico del riesgo**	**Total (Estimado del Riesgo total)**
Laptops equipo Gerencial y Staff Clínico	Ataque de virus	3	Mal uso de recursos	2	1	3
	Robo y pérdida	3	Pérdida de información	3		
	Daño de Hadware/software	2	Mal uso de recursos	2		
Proveedores	Mal servicio de proveedores	2	Falta de un acuerdo de prestación de servicios	1	1	2
	Fuga de información	2	Baja efectividad de controles implementados	1		
	Error humano	2	Falta de Supervisión	1		

Anexo 4
Evaluación del Riesgo

Hospital María Especialidades Pediátricas								
Evaluacion del Riesgo								
		Criterios para Evaluación						
Activos	**Amenazas**	**Impacto económico del riesgo**	**Tiempo de Recuperación de la empresa**	**Posibilidad de Ocurrencia**	**Posibilidad de interumpir actividades de la empresa**	**Imagen-Reputación**	**Total Riesgo**	**Nivel de Riesgo Aceptable**
Red de Producción	Virus	3	3	3	3	3	**15**	Medio
	Sabotaje							
	Ataques de Hackers							
Administrador de Redes	Robo de información	1	2	2	1	1	**7**	Aceptado
	Divulgación de información confidencial							
Correo Electrónico	Disponibilidad	2	2	3	1	1	**9**	Bajo
	Virus							
Gestor de Tickets (GIS)	Ataque de Virus	2	1	3	1	1	**8**	Aceptado
ERP	Disponibilidad	2	2	3	3	3	**13**	Medio
	Pérdida de Información							
Base de datos de Pacientes	Fallas de integridad de la información	2	1	3	3	4	**13**	Medio
Base de datos de proveedores y contratistas	Falta de disponibilidad	1	2	3	1	1	**8**	Aceptado
Jefe de IT	Robo de información	1	2	3	1	1	**8**	Aceptado
	Error humano							
	Divulgación de información confidencial							
Fibra óptica	Sabotaje Físico	4	4	3	4	4	**19**	Alto
	Error humano							
	Incendio							
	Robo							
	Ataque de Animales							
Laptops equipo Gerencial y Staff Clínico	Ataque de virus	1	1	3	1	1	**7**	Aceptado
	Robo y pérdida							
	Daño de Hadware/software							

Anexo 5
Plan de Tratamiento del Riesgo

Hospital María Especialidades Pediátricas							
PLAN DE TRATAMIENTO DEL RIESGO							
Activos de Información	**Propietario**	**Objetivos de Control**	**Controles**	**Responsables**	**Acciones esperadas del Responsable**	**Fecha de Entrega**	**Indicador de Efectividad del Control**
Red de Producción	Departamento de TIC Administrador de redes	A.12.2Control contra código malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.	Administrados de Redes	Implementación y revisión de Política Antivirus	2018	Verificacion del cumplimiento de la politica de manejo de Antivirus
		A.13.1 Gestión de seguridad de redes	Servicios d seguridad de redes Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.	Administrados de Redes	Revisión Política de control de accesos	2018	Verificacion del cumplimiento de la politica de Administracion y Acceso a la Red de Producción
		A.7.2 Durante el empleo	Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.	Jefe de TIC	Elaborar Plan de Toma de Conciencia (Jornada Toma de Conciencia).	2018	Implementación y cumplimiento del Plan de Toma de Conciencia
		A.9.1 Requerimiento del negocio para el control de acceso	Política de control de acceso Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.	Administrador de Redes	Revisión Política de control de accesos	2018	Verificación del cumplimiento de la política de control de accesos
		A.9.2 Gestión de acceso a usuarios	Un proceso formal de registro y desregistro de usuarios debe implementarse. La asignación y uso de derechos de privilegios de accesos debe ser restringida y controlada. Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	Administrador de Redes	Revisión Política de control de accesos	2018	Verificación del cumplimiento de la política de control de accesos
		A.9.4 Control de Acceso a aplicaciones y sistemas	Procedimiento para comienzo de sesión segura Cuando sea requerido por la política de control de accesos, los accesos a sistemas y aplicaciones deben ser controlados por un procedimiento de comienzo de sesión segura	Administrador de Redes	Revisión Política de control de accesos	2018	Verificación del cumplimiento de la política de control de accesos
Administrador de Redes	**Riesgo Aceptado**						

Hospital María Especialidades Pediátricas

PLAN DE TRATAMIENTO DEL RIESGO

Activos de Información	Propietario	Objetivos de Control	Controles	Responsables	Acciones esperadas del Responsable	Fecha de Entrega	Indicador de Efectividad del Control
Correo Electronico	Adminsitrador de Red de Producción	A.13.2 Transferencia de información	Mensaje electrónico La información involucrada en mensajes electrónicos debe protegerse adecuadamente	Administrador de Redes	Implementación y revisión de una política para manejo y uso de Correo electrónico	2018	Verificar el cumplimiento de la Política para Manejo y uso del Correo Electrónico
		A.12.2Control contra código malicioso	Controles contra software malicioso Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.	Administrador de Redes	Revision Política Antivirus	2018	Verificar cumpliento de política antivirus
Gestor de Tickets (GIS)	Adminsitrador de Red de Producción	A.12.2Control contra código malicioso	Controles contra software malicioso Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.	Administrador de Redes	Revisión de Política de manejo de Antivirus	2018	Verificación del cumplimiento de la política de manejo de Antivirus
ERP	Jefe de TIC	A.12.4 Registro y Monitoreo	Registro deeventos Registros de eventos de las actividades de los usuarios, excepciones, errores, y los eventos de seguridad de información deben ser producidos, mantenidos y regularmente revisados.	Jefe de TIC/Administrador de redes	Implemnetación de un proceso para deteccion de fallas. Utilización del gestro de tickets para el registro de eventos.	2018	Verificar el cumplimiento del proceso de Deteccion de Fallas identificando los casos en los que ocurren fallas que no son registradas y no se toma la acción apropiada.
		A.12.3 Respaldo	Copias de respaldo en la información Copias de respaldo de la información, software e imágenes de sistemas, deben ser tomadas y probadas, regularmente en concordancia con una políticca de respaldos acordada.	Administrador de Redes	Proceso de Respaldos	2018	Verificar cumplimiento de proceso de Respaldos
		A.9.1 Requerimiento del negocio para el control de acceso	Política de control de acceso Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.	Administrador de Redes	Revisión Política Administracion y Acceso Red Producción	2018	Verificar cumplimiento de la Política de Administración y Acceso a los sistemas de información
		A.9.2 Gestión de acceso a usuarios	Un proceso formal de registro y desregistro de usuarios debe implementarse. La asignación y uso de derechos de privilegios de accesos debe ser restringida y controlada. Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	Administrador de Redes	Revisión Proceso Altas y Bajas	2018	Verificar cumplimiento de proceso de Altas y Bajas

Hospital María Especialidades Pediátricas

PLAN DE TRATAMIENTO DEL RIESGO

Activos de Información	Propietario	Objetivos de Control	Controles	Responsables	Acciones esperadas del Responsable	Fecha de Entrega	Indicador de Efectividad del Control
Base de datos de Pacientes	Jefe de TIC	A.12.3 Respaldo	Copias de respaldo en la información Copias de respaldo de la información, software e imágenes de sistemas, deben ser tomadas y probadas, regularmente en concordancia con una políticca de respaldos acordada.	Administrador de Redes	Proceso de Respaldos	2018	Verificar cumplimiento de proceso de Respaldos
		A.9.1 Requerimiento del negocio para el control de acceso	Política de control de acceso Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.	Administrador de Redes	Revisión Política Administracion y Acceso Red Producción	2018	Verificar cumplimiento de la Política de Administración y Acceso a los sistemas de información
		A.9.2 Gestión de acceso a usuarios	Un proceso formal de registro y desregistro de usuarios debe implementarse. La asignación y uso de derechos de privilegios de accesos debe ser restringida y controlada. Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	Administrador de Redes	Revisión Proceso Altas y Bajas	2018	Verificar cumplimiento de proceso de Altas y Bajas
Base de datos de proveedores y contratistas	**RIESGO ACEPTADO**						
Jefe de IT	**RIESGO ACEPTADO**						

Hospital María Especialidades Pediátricas

PLAN DE TRATAMIENTO DEL RIESGO

Activos de Información	Propietario	Objetivos de Control	Controles	Responsables	Acciones esperadas del Responsable	Fecha de Entrega	Indicador de Efectividad del Control
Fibra óptica	Departamento de TIC	A.11.1 Áreas seguras	Controles de entrada físicos Las áreas seguras deben protegerse a través de apropiados controles de entrada para asegurar que solo se le permite el ingreso a las personas autorizadas.	Jefe de TIC	Implementación de un Proceso de Bitacora de Acceso para áreas seguras	2018	Verificar el cumplimiento del registro en la Bitacora de Accesos.
			Protección contra amenazas externas y ambientales Protección física contra desastres naturales, ataques maliciosos o accidentes debe ser diseñada y aplicada.	Jefe de TIC	Implementación de Politica de Mantenimiento de Operaciones Tecnicas y aplicación del plan de continuidad	2018	Verificar cumplimiento de la politica de mantenimiento de operaciones técnicas
		A.11.2 Equipo	Seguridad en el cableado el cableado de energía y de telecomunicaciones transportando datos o servicios de apoyo de información, debe protegerse de intercepción, interferencia o daño	Jefe de TIC	Revision Proceso para el Mantenimiento de Equipos	2018	Verificar cumplimiento del proceso de mantenimiento de equipos
		A.9.1 Requerimiento del negocio para el control de acceso	Política de control de acceso Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.	Administrador de Redes	Revisión Política de control de accesos	2018	Verificar el cumplimiento del registro en la Bitacora de Accesos.
Laptops equipo Gerencial y Staff Clínico	**RIESGO ACEPTADO**						

Anexo 6
Riesgo Residual

Hospital María Especialidades Pediátricas							
Evaluacion del Riesgo							
RIESGO RESIDUAL							
Activos	**Amenazas**	**Impacto económico del riesgo**	**Tiempo de Recuperación de la empresa**	**Posibilidad de Ocurrencia**	**Posibilidad de interumpir actividades de la empresa**	**Imagen/ Reputación**	**Total Riesgo Residual**
Red de Producción	Virus	1	2	2	2	2	**9**
	Sabotaje						
	Ataques de Hackers						
Administrador de Redes	Robo de información	**Riesgo Aceptado**					
	Divulgación de información confidencial						
Correo Electrónico	Disponibilidad	1	1	2	1	1	**6**
	Virus						
Gestor de Tickets (GIS)	Ataque de Virus	**Riesgo Aceptdo**					
ERP	Disponibilidad	1	1	2	1	1	**6**
	Pérdida de Información						
Base de datos de Pacientes	Fallas de integridad de la información	1	1	1	1	1	**5**
Base de datos de proveedores y contratistas	Falta de disponibilidad	**Riesgo Aceptado**					
Jefe de IT	Robo de información	**Riesgo Aceptado**					
	Error humano						
	Divulgación de información confidencial						
Fibra óptica	Sabotaje Físico	3	3	2	3	3	**14**
	Error humano						
	Incendio						
	Robo						
	Ataque de Animales						
Laptops equipo Gerencial y Staff Clínico	Ataque de virus	**Riesgo Aceptado**					
	Robo y pérdida						
	Daño de Hadware/software						

Anexo 7
Declaración de Aplicabilidad

ANEXO 6: DECLARACIÓN DE APLICABILIDAD HOSPITAL MARÍA ESPECIALIDADES PEDIÁTRICAS						
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
A5.1	Directrices de la Dirección en seguridad de la información					
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos						
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Si	No	Si	angular donde se fundamentará la seguridad de la información de la organización, aprobado por la Gerencia General y comunicado a la empresa para orientar a la empresa a la Seguridad de la información.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	Si	No	No	Proveer continuidad a la Política de Seguridad de la Información y realizar la actualización periódica de las buenas prácticas y políticas en mejoras de la seguridad de la información
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
A6.1	Organización interna					
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.						
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Si	No	Si	Establecimiento de los responsables para coordinar los roles dentro del SGSI.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	Si	No	No	Distribución de las responsabilidades y funciones dentro del SGSI para evitar conflictos de intereses por la seguridad de la información
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	Si	No	Si	Para enmarcar al hospital dentro de las leyes actuales de acuerdo a los cambios que se puedan presentar y que afecten la seguridad de la información.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Si	No	No	Obtener actualizaciones en lo relacionado a mejores prácticas de la seguridad de la información con grupos de interés especial.
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Si	No	No	Implementar controles en la gestión de proyectos que pudieran afectar la seguridad de la información
A6.2	**Dispositivos móviles y teletrabajo**		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles						
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Si	No	No	Establecer y documentar las responsabilidades en cuanto al uso de dispositivos móviles en los que se procesa información del hospital.
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	No	No	No	Este cotrol no aplica ya que el hospital actualmente no realiza teletrabajo.

A7	SEGURIDAD DE LOS RECURSOS HUMANOS		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
A7.1	Antes de la contratación					
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.						
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Si	No	Si	Desarrollar un sistema que permita llevar a cabo chequeos de verificación de todos los candidatos a empleados
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Si	No	Si	Establecer contratos de servicio que estipulen las responsabilidades del cargo y los reglamentos por los que se regirán los empleados.
A7.2	Durante el empleo		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.						
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Si	No	No	Involucramiento de la alta dirección para asegurar que los empleados, contratistas y terceros apliquen la seguridad de información en concordancia con las
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Si	No	No	capacitar a los empleados, contratistas y terceros sobre la seguridad de información, políticas y procedimientos relacionados con el SGSI que se implemente en el hospital.
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Si	Si	No	Regular y exigir en base al Código de Trabajo de Honduras, el cumplimiento de las políticas y procedimientos orientados a la seguridad de la información, aplicando sanciones al incumplimiento de los mismos.
A7.3	Terminación y cambio de puesto de trabajo		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo						
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Si	No	No	Determinar las responsabilidades legales que conllevan la desvinculación del hospital, asi como el tratamiento de la información durante un tiempo definido.
A8	**GESTION DE ACTIVOS**		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
A8.1	Responsabilidad por los activos					
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.						
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Si	No	Si	Tener un control sobre los inventarios de activos de información
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	Si	No	Si	Establecer la responsabilidad en relación a los activos de información
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Si	No	No	Para el manejo adecuado de los activos de información.

A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Si	No	Si	Garantizar la recuperaciónd e los activos de información petenecientes a la organización.
A8.2	Clasificación de la información		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.						
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Si	No	Si	Establecer lineamientos a seguir para determinar la importancia de la información de acuerdo al impacto que pueda tener la divulgación de la misma.
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Si	No	No	Estabelcer la reglamentación para la correcta identificación de la información producida manejada dentro del hospital.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Si	No	No	Establecer la responsabilidad en relación a los activos de información
A8.3	Manejo de medios		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios						
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Si	No	Si	Verificar que los medios en los cuales se envía o recibe información sean confiables para la función y no pueda existir robo o fuga de dicha información.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Si	No	No	Garantizar que los medios de procesamiento de información sean correctamente desechados empleando los procedimientos adecuados para eliminación de información.
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Si	No	No	Garantizar la seguridad de la información contenida en medios de almacenamiento que pueden ser sacados fuera del hospital.
A9	**CONTROL DE ACCESOS**					
A9.1	Requisitos del negocio para el control de acceso		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.						
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Si	No	Si	Establecer una política de control de accesos tanto a los equipo de procesamiento (Servidores), como a las computadoras y la información confidencial.
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Si	No	Si	Verificar que los usuarios tengan accesos y/o utilicen los servicios y/o sistemas autorizados.
A9.2	Gestión de acceso de usuarios		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.						
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Si	No	Si	De acuerdo a las actividades de cada usuario es de suma importancia llevar un control de los accesos permitidos a cada usuario así como dar de baja a los mismos cuando sea el caso.

A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Si	Si	Si	Establecer la política de control de accesos
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Si	Si	Si	Llevar control de las asignaciones de privilegios de cada usuario, ya que las mismas se realizaran de acuerdo a las actividades que realicen cada usuario.
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Si	No	No	Establecimiento del proceso de autenticación secreta
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Si	No	No	Revisar los provilegios en períodos establecidos con el fin de dar de baja a los accesos o privilegios que por algún motivo el usuario ya no requiera.
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Si	No	No	Estabelcer el procedimiento correcto para la cancelación de accesos por baja de empleados.
A9.3	Responsabilidades del usuario		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.						
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Si	No	No	Establecimiento del proceso de autenticación secreta
A9.4	Control de acceso a aplicaciones y sistemas		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.						
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Si	No	Si	Controlar los derechos (lectura, escritura etc.) de la información de acuerdo a los requerimientos de cada usuario
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Si	Si	Si	Garantizar la seguridad de los medios de procesamiento de información como de ella misma.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Si	No	Si	Establecer un proceso de asignación de contraseñas con el fin de proteger toda la información confidencial y llevar un control de las mismas
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Si	No	Si	Garantizar la inviolabilidad de la información mediante programas o aplicaciones ajenas a la institución
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	Si	No	Si	Garantizar la seguridad de la información ante modificaciones realizados mediante cambios en bases de datos.

A10	CRIPTOGRAFÍA		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
A10.1	Controles criptográficos					
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información						
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Si	No	No	Proteger la información sensible almcenada en las computadoras portatiles del equipo gerencial administrativo y médico.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Si	No	No	Controlar adecuandamente el ciclo de vida de los controles criptográficos y sus contraseñas
A11	SEGURIDAD FÍSICA Y AMBIENTAL		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
A11.1	Áreas seguras					
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.						
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	Si	No	Si	Identificar los perímetros de seguridad física y establecer los controles de acceso a las áreas que contienen información sensible y equipos.
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Si	No	Si	Llevar registro del personal interno o externo que accede a las instalaciones corroborando que todos éstos estén debidamente identificados, otorgando los privilegios de acuerdo al rol de sus funciones.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	Si	No	Si	Controlar para que no ingresen personas sin autorización.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Si	No	Si	Proteger los activos de información contra cualquier amenaza externa y de amenazas ambientales.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Si	No	Si	Mantener áreas de trabajo seguras mediante la aplicaciónd e controles de seguridad.
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Si	No	Si	Controles de acceso restrictivo para terceros.
A11.2	Seguridad de los equipos		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.						
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Si	No	Si	Ubicación de los equipos en áreas seguras paa reducir los riesgos de amenazas y peligros ambientales
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Si	No	Si	Protección de los equipos ante fallas eléctricas u/y otras interrupciones.
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Si	No	Si	Protección del cableado de energía y telecomunicaciones de cualquier intercepción o daño.

A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Si	No	Si	Establecer y documentar un programa de mantenimiento adecuado para los equipos.
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Si	No	No	Evitar que equipos, información o software no salgan de la empresa sin previa autorización
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Si	No	No	Proteger adecuadamente la seguridad de los equipos fuera de las instalaciones, considerando los diferentes riesgos.
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.	Si	No	No	Verificar que la información contenida en los equipos al momento de ser desechados o reutilizados quede eliminada por completo para evitar fuga de información.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Si	No	No	Concientizar a los colaboradores sobre la importancia del manejo de la información y su seguridad, lo que inluye estar pendientes de la seguridad de sus equipos mediante el uso de bloqueos y contraseñas.
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Si	No	Si	Establecimeinto de una política de control y seguridad de información que se maneja de manera física y digital.
A12	**SEGURIDAD EN LAS OPERACIONES**		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
A12.1	Responsabilidades y procedimientos de operación					
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.						
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Si	No	Si	Documentar y mantener los principales procedimientos de operación
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Si	No	Si	Establecer controles para los cambios en los medios y sistemas de información
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Si	Si	Si	Establecimiento de proyecciones y garantía del uso adecuado de los recursos para asegurar el desempeño del sistema requerido.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Si	No	Si	Establecer ambientes de prueba en los sistemas de información para control de actividades y nuevas implementaciones requeridas
A12.2	Protección contra código malicioso		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.						
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Si	No	Si	Proteger la integridad de la información de ataques externos.

A12.3	Copias de seguridad		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
Objetivo: Proteger contra la perdida de datos						
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Si	No	Si	Asegurar que se realizan y mantienen copias de respaldo de la información.
A12.4	Registro de actividad y supervisión		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Registrar eventos y generar evidencia						
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Si	No	No	Registrar todas las fallas con el fin de analizar e investigar las causas para tomar las medidas respectivas y así evitar la recurrencia.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Si	No	Si	Evitar el acceso no autorizado
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Si	No	Si	Para asegurar que el usuario está realizando solamente las actividades que se han autorizado explícitamente, se deben mantener registrada la actividad del administrador de redes.
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Si	No	Si	Capacidad de eoperación en tiempo real.
A12.5	Control deL software operativo		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Asegurarse de la integridad de los sistemas operacionales						
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Si	No	Si	Controlar que mediante instalaciones de programas pueda ser vulnerada de seguridad de la información.
A12.6	Gestión de la vulnerabilidad técnica		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas						
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Si	No	Si	Identificar las vulnerabilidades del sistema de información, evaluarlas y tomar las medidas correspondientes.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Si	No	Si	Evitar la instalación de programas no autorizados en las computadoras de la organización, que puedan afectar la seguridad de la información.
A12.7	Consideraciones de las auditorias de sistemas de información		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos						
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Si	No	No	Para futuras investigaciones y seguimiento del control de accesos se necesita mantener registradas las actividades, excepciones y eventos de seguridad de los usuarios.

A13	SEGURIDAD EN LAS COMUNICACIONES		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
A13.1	Gestión de la seguridad en las redes					
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.						
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Si	No	Si	Proteger la red interna de ataques externos, perdida o robo de información.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Si	No	Si	Verificar que la red tenga y proveea la seguridad requerida para la seguridad de la información de la organización.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Si	No	Si	Controlar la asignación de privilegiós de acuerdo a las necesidades y a la información que maneja cada una de las redes disponibles.
A13.2	Intercambio de información con partes externas		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.						
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Si	No	No	Proteger el intercambio de información a través de la utilización de toda clase de recursos de comunicación.
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Si	No	No	Establecer los lineamientos de intercambio de información con el ente regulador, proveedores y cualquier otra parte externa con la que se deba
A13.2.3	Mensajería Electronica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Si	No	Si	Establecer métodos para proteger la información transportada por mensajería electrónica
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Si	No	No	Evitar y controlar con fundamento legalmente la fuga de información así como estringir la divulgación de la misma de acuerdo a los cargos desempeñados
A14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
A14.1	Requisitos de seguridad de los sistemas de información					
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los						
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Si	No	Si	Proteger la seguridad de la información bajo requisitos de seguridad para la adquisisción de sistemas de información o cambios en los actuales.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Si	No	Si	Garantizar que la información que pasa a traves de redes públicas sena protegida de a manera mas adecuada.
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Si	No	Si	Garantizar la integridad de la información.

A14.2	Seguridad en los procesos de Desarrollo y Soporte		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.						
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	No	No	No	Este control no aplica, ya que la organización no realiza desarrollos "In House"
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	Si	No	Si	Controlar la seguridad de la información durante los cambios aplicados a los sistemas.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Si	No	Si	Controlar la seguridad de la información durante los cambios aplicados a los sistemas.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Si	No	Si	Controlar la seguridad de la información durante los cambios aplicados a los sistemas.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Si	No	Si	Controlar la seguridad de la información durante los cambios aplicados a los sistemas.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No	No	No	Este control no aplica, ya que la organización no realiza desarrollos "In House"
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Si	No	Si	Asegurar la seguridad de la información en todos los sistemas de información que se adquieran de proveedores
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Si	No	Si	Asegurar la seguridad de la información en todos los sistemas de información que se adquieran de proveedores
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Si	No	No	Garnatizar que los sistemas adquiridos cumplen con los requerimientos del sistema de seguridad de información.
A14.3	Datos de prueba		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
Objetivo: Asegurar la protección de los datos usados para pruebas.						
A.14.3.1	Protección de datos de prueba	Control:Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Si	No	Si	Granatizar la protección de la información que es utilizada en los ambientes de prueba previa implementación de aplicaciones o sistemas de información

A15	RELACIONES CON SUMINISTRADORES		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
A15.1	Seguridad de la información en las relaciones con los suministradores.					
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.						
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Si	No	Si	Establecer los lineamientos por los cuales los proveedores deben garantizar la seguridad de a información del hospital.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Si	No	Si	
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Si	No	Si	
A15.2	Gestión de la prestación de servicios por suministradores		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores						
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Si	No	Si	Garantizar el cumplimiento de las mormas establecidas a travesde auditorias para garantizar la seguridad de la información.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la rrevaluación de los riesgos.	Si	No	Si	Garantizar que no resulte afectada la seguridad de la información debido a cambios realizados por los proveedores o por la organización sin un concenso previo.
A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
A16.1	Gestión de incidentes de seguridad de la información y mejoras					
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y						
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Si	No	Si	Establecer los procedimientos de gestión que aseguren la eficaz y rápida respuesta a los incidentes de seguridad.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Si	No	No	Identificar los eventos de seguridad que afecten la información con el fin de tomar las medidas correctivas oportunas.
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Si	No	No	Identificar las debilidades del sistema de seguridad de información.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Si	No	No	Clasificar los eventos de seguridad para determinar si se consderan como incidentes y tartarlos como tal.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Si	No	No	Documentar el procedimiento a seguir para el tratamiento de los inciedentes de seguridad bajo los lineamientos establecidos.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	Si	No	No	Cuantificar los incidentes para poder identificar los volúmenes y tipos.

A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Si	No	No	Identificar y documentar las evidencias que han causado un incidente de seguridad con el fin de tomar las medidas tanto correctivas pertinentes.
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
A17.1	Continuidad de la Seguridad de la información					
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.						
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Si	No	Si	Desarrollar un proceso para la continuidad del negocio, considerando los requisitos de seguridad de la información
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Si	No	Si	Implementar planes que de mantenimiento de los procesos críticos con el fin de asegurar la disponibilidad de la información.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Si	No	Si	Evaluar los planes de continuidad del negocio con el objetivo de mantenerlos actualizados y verificar su correcto funcionamiento
A17.2	Redundancias		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.						
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Si	No	Si	Garantizar la disponibilidad de la información y sistemas de procesamiento ante un evento que pueda afectar.
A18	**CUMPLIMIENTO**		**APLICABILIDAD**	**CONTROLES LEGALES**	**CONTROLES ACTUALES**	**JUTIFICACIÓN**
A18.1	Cumplimiento de requisitos legales y contractuales					
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier						
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Si	No	Si	Identificar y documentar todos los requerimientos legales y contractuales de la empresa según los requisitos del sistema de seguridad de la información.
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Si	No	Si	Establecer procedimientos para asegurar el cumplimiento de todos los requisitos legales y contractuales sobre el uso de material que este protegido por
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Si	No	Si	Proteger toda la información pertinente, contra perdida, destrucción o falsificación, en un área segura
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	Si	No	No	Este control se cumple por elección interna no por exigencia de la legislación del país.
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No	No	No	Este control no aplica ya que no existe una regulación en el país que trate el tema de critográfia.

A18.2	Revisiones de seguridad de la información		APLICABILIDAD	CONTROLES LEGALES	CONTROLES ACTUALES	JUTIFICACIÓN
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.						
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Si	No	No	Realizar auditorías planificando los requerimientos a evaluar, con el fin de verificar que se están cumpliendo todos los requisitos de sistema de información.
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	Si	No	No	
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Si	No	No	