UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE SALUD, BASADO EN LAS NORMAS ISO 27799:2008, ISO/IEC 27005:2008 E ISO/IEC 27002:2013 APLICADA A LA CLÍNICA MÉDICA FÉRTIL

AUTORA: ALEXANDRA ARACELY ENRÍQUEZ COLLAGUAZO

DIRECTORA: MGS. SANDRA KARINA NARVÁEZ PUPIALES

IBARRA, 2018

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE IDENTIFICACIÓN DE LA OBRA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1002864443		
APELLIDOS Y NOMBRES:	ENRIQUEZ COLLAGUAZO ALEXANDRA ARACELY		
DIRECCIÓN:	RIO GUAYLLABAMBA 5-61 Y RIO AGUARICO		
EMAIL:	ale86aracely@gmal.com		
TELÉFONO FIJO:	06260721	**TELÉFONO MÓVIL:**	0994705686

DATOS DE LA OBRA	
TÍTULO:	MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE SALUD, BASADO EN LAS NORMAS ISO 27799:2008, ISO/IEC 27005:2008 E ISO/IEC 27002:2013 APLICADA A LA CLÍNICA MÉDICA FÉRTIL
AUTOR (ES):	ENRIQUEZ COLLAGUAZO ALEXANDRA ARACELY
FECHA: DD/MM/AAAA	01/08/2018

SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	[x] **PREGRADO** [ ] **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERA EN ELECTRONICA Y REDES DE COMUNICACIÓN
ASESOR /DIRECTOR:	MGS. SANDRA KARINA NARVÁEZ PUPIALES

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 01 días del mes de agosto de 2018

EL AUTOR:

……

Alexandra Aracely Enríquez Collaguazo

CERTIFICACIÓN

Certifico que el proyecto de Trabajo de Grado MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE SALUD, BASADO EN LAS NORMAS ISO 27799:2008, ISO/IEC 27005:2008 E ISO/IEC 27002:2013 APLICADAS A LA CLÍNICA MÉDICA FÉRTIL ha sido realizado en su totalidad por la señora Alexandra Aracely Enríquez Collaguazo portador de la cédula de identidad número: 100286444-3.

_____

Mgs. Sandra Karina Narváez Pupiales
DIRECTORA DE PROYECTO

DEDICATORIA

El presente trabajo va dedicado a Dios, por regalarme el don de la vida y salud, a mis padres que nunca dejaron de creer en mí, quienes han sido mi fortaleza y apoyo incondicional para seguir adelante, a mis hermanas, quienes me han dado ejemplo que todo es posible y a mi esposo, el pilar de mi vida.

Alexandra Enríquez

AGRADECIMIENTOS

A mis padres, Zoila y Fabián, quienes hicieron de mí una persona de bien y que siempre estuvieron brindándome su apoyo incondicional en cualquier circunstancia y a quienes debo todo lo que soy y lo que he logrado.

A mi esposo, Ricardo, persona incondicional que fue mi soporte en la culminación de este proyecto y quien día a día con su amor y paciencia me da la fuerza para luchar por mis metas.

A mis hermanas Paola y Gabriela y toda mi familia quienes han sido mi motivación y fortaleza contribuyendo a que siga adelante sin rendirme.

A todos mis profesores que supieron impartir sus conocimientos y valores en especial a mi directora de tesis Mgs. Sandra Narváez por su gran aporte en la culminación del presente proyecto y su don de gente.

A mis compañeros y amigos que de una u otra manera colaboraron en este proceso de culminación del proyecto.

Alexandra Enríquez

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El involucramiento de las tecnologías de la información en el sector salud ha propiciado un mejoramiento en los diagnósticos, tratamientos y tiempos de respuesta de los procesos médicos asistenciales para los pacientes; sin embargo, también ha ocasionado una gran cantidad de incidentes de pérdida de información derivados de deficiencias y desconocimiento de las políticas de seguridad de la información, a causa de errores o descuidos del personal en la manipulación de los datos de pacientes.

El presente proyecto de titulación tiene como finalidad diseñar un modelo de Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil basado en las normas ISO 27799:2008, ISO/IEC 27005:2013 E ISO/IEC 27002:2013, para lo cual se realiza una revisión bibliográfica de carácter analítico sobre el estado actual del sector salud en el país, así como también las leyes y regulaciones sobre confidencialidad de la información que posee el Ecuador. Posteriormente se describe las normativas, marco de referencia y buenas prácticas que tienen relación con la seguridad de la información aplicable al sector salud como son: ISO/IEC 27799, COBIT 5 e ITIL en su versión 3.

Mediante el uso de las normas ISO/IEC 27001:2013, ISO/IEC 27005:2008, ISO/IEC 27002:2013 e ISO27799:2008 se diseña un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para la Clínica Médica Fértil, que contiene procesos y actividades dirigidas a salvaguardar la información de los pacientes y sus trabajadores ante cualquier amenaza que se presente, preservando la confidencialidad, integridad y disponibilidad de la información. De igual manera para completar el modelo propuesto se describe el proceso a seguir para obtener la certificación en la norma ISO/IEC 27001 y un análisis de los beneficios de implementar un SGSI en instituciones del sector salud.

En la validación del modelo propuesto del Sistema de Gestión de Seguridad de la Información (SGSI), se inicia analizando la situación actual de la Clínica Médica Fértil bajo el enfoque de las tecnologías de la información. Luego, conforme a la metodología del modelo se realiza un análisis de gestión de riesgos sobre los activos de información de la clínica, para identificar el tratamiento del riesgo a implementar y desarrollar las políticas de Seguridad de la información en base a las normas ISO/IEC 27002:2013 e ISO27799:2008.

ABSTRACT

The involvement of information technologies in the health sector has led to an improvement in the diagnosis, treatment and response times of medical care processes for patients; However, it has also caused a large number of incidents of information loss due to deficiencies and ignorance of information security policies, or due to staff errors or oversights in the handling of patient data.

The purpose of this titling project is to design an Information Security Management System model for the Médica Fértil Clinic based on the ISO / IEC 27001: 2013, ISO / IEC 27005: 2008, ISO / IEC 27002: 2013 standards. ISO27799: 2008, for which an analytical bibliographic review is made on the current state of the Health Sector in the country, as well as the laws and regulations on confidentiality of information held by Ecuador. Subsequently, the regulations, reference framework and good practices related to information security applicable to the health sector are described, such as: ISO / IEC 27799, COBIT 5 and ITIL in version 3.

Through the use of ISO / IEC 27001: 2013, ISO / IEC 27005: 2008, ISO / IEC 27002: 2013 and ISO27799: 2008 a model of Information Security Management System (ISMS) is designed for the Medical Clinic Fertile, which contains processes and activities aimed at safeguarding the information of patients and their workers against any threat that may arise, preserving the confidentiality, integrity and availability of the information. Similarly, to complete the proposed model, the process to be followed to obtain certification in ISO / IEC 27001 and an analysis of the benefits of implementing an ISMS in institutions of the health sector is described.

In the validation of the proposed model of the Information Security Management System (ISMS), it begins by analyzing the current situation of the Fertile Medical Clinic under the approach of information technologies. Then, according to the methodology of the model, a risk management analysis is carried out on the information assets of the clinic, to identify the risk treatment to implement and develop the Information Security policies based on the ISO / IEC 27002 standards. : 2013 and ISO27799: 2008.

CAPÍTULO 1: INTRODUCCIÓN

1.1 PROBLEMA

El uso de las Tecnologías de la Información dentro de las organizaciones del sector de salud ha ido aumentando rápidamente, permitiendo optimizar y mejorar la prestación de sus servicios, convirtiéndose en una herramienta valiosa dentro del proceso de atención médica. En la actualidad uno de los activos más importantes que poseen las organizaciones es la información; sin embargo, en muchas ocasiones no cuentan con políticas adecuadas para protegerla, generando vulnerabilidades que pueden ser aprovechadas por las amenazas existentes en el entorno y por ende afectar a la integridad, confidencialidad y disponibilidad de los activos de información.

La clínica Médica Fértil Clínica es una prestigiosa institución del Norte del país, ubicada en la ciudad de Ibarra, orientada a brindar servicios ambulatorios y hospitalarios con altos estándares de calidad, con los mejores médicos en todas las especialidades, además de contar con una excelente infraestructura física y siempre a la vanguardia con la tecnología. Además, se encuentran siempre innovando y creando nuevos servicios y espacios, por lo que próximamente ampliará sus servicios e instalaciones en otras ciudades de la zona 1 del Ecuador.

Por la falta de conocimiento de las normativas de seguridad de la información se crea una vulnerabilidad y riesgos dentro de la seguridad de los datos que se maneja la Clínica Médica Fértil y debido al alto grado de importancia de los archivos que contiene la institución, puede producir un significativo impacto en el aspecto clínico de los pacientes y en los servicios que presta la organización, conllevando a sanciones económicas y legales, ya que la imagen y los niveles de competitividad de la clínica pueden verse comprometidos.

La unidad de tecnología de la información y comunicaciones de la clínica Médica Fértil, no dispone de un modelo de Gestión de Seguridad de la Información que oriente a las personas responsables o técnicos afines sobre las mejores

prácticas o mecanismos tecnológicos para salvaguardar la información contra amenazas y ataques tanto internos como externos.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Proponer un Modelo de Gestión de Seguridad de la Información para la Clínica Médica Fértil; que permita garantizar la integridad, disponibilidad y confidencialidad de la información, mediante el uso de la norma ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013.

1.2.2 OBJETIVOS ESPECÍFICOS

- Realizar una revisión bibliográfica de las normativas sobre confidencialidad de la información para el sector salud del Ecuador y de la metodología de las normas ISO 27799:2008, ISO/IEC 27002:2015 e ISO/IEC 27005:2013; que permita establecer lineamientos adecuados para el desarrollo del modelo de Sistema de Gestión de Seguridad de la Información aplicable al sector de salud.

- Realizar el levantamiento de información de la situación actual de la Clínica Médica Fértil, para la identificación de escenarios de riesgos lógicos, físicos y de índole ambiental que comprometan la seguridad de la información mediante la metodología de la norma ISO/IEC 27005:2008.

- Plantear un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para la Clínica Médica Fértil; seleccionando los controles de seguridad de información más importantes que garanticen la confidencialidad, integridad y disponibilidad de la información.

- Realizar un análisis costo beneficio para una futura implementación de los controles y políticas generadas a través del modelo de Gestión de Seguridad de la Información (SGSI) en organizaciones del sector salud en el Ecuador.

- Describir los pasos a seguir para una certificación ISO 27001 en organizaciones relacionadas al sector salud, que complemente la funcionalidad y aplicabilidad del modelo de Sistema de Gestión de Seguridad de la Información (SGSI) propuesto.

- Validar el modelo de Sistema de Gestión de Seguridad de la Información (SGSI) hasta el planteamiento de políticas para el caso de estudio en la Clínica Médica Fértil que permita garantizar la integridad, disponibilidad y confidencialidad de la información.

1.3 ALCANCE

El presente proyecto de titulación consiste en proponer un modelo de Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil que permita garantizar la integridad, disponibilidad y confidencialidad de la información, basado en las normas: ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013.

Se realiza una revisión bibliográfica de las normativas sobre confidencialidad de la información para el sector salud del Ecuador; posteriormente se analiza la metodología de las normas ISO 27799:2008, ISO/IEC 27002:2013 e ISO/IEC 27005:2008 que permita establecer lineamientos adecuados para el desarrollo del modelo de Sistema de Gestión de Seguridad de la Información.

Posteriormente, se elabora un diagnóstico de la situación actual de la Clínica Médica Fértil en lo que respecta a la seguridad de la información, basado en la metodología de la norma ISO/IEC 27005:2008; se identificarán y valorarán los activos de información; así como también se evaluarán las amenazas, vulnerabilidades, riesgos e impactos que pueden sufrir dichos activos de información, permitiendo obtener un análisis de los posibles controles y políticas de seguridad de la información a ser establecidos para la clínica.

Luego, se planteará un modelo de Sistema de Gestión de Seguridad de la Información usando la norma ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013 para la Clínica Médica Fértil. De igual manera, se describirá los lineamientos para una futura implementación de las políticas y controles de seguridad de la información obtenidos previo a un análisis de costo – beneficio; además se detallarán los procesos y lineamientos a seguir para una futura certificación ISO 27001.

Y finalmente, se validará el modelo de Sistema de Gestión de Seguridad de la Información propuesto en el caso de estudio y se diseñará las políticas de seguridad de la información mediante el uso de la Norma ISO 27799:2008 e ISO/IEC 27002:2013 que brinde confidencialidad, integridad y disponibilidad a la información de la clínica.

1.4 JUSTIFICACIÓN

El sector salud se ha visto beneficiado con el uso de las Tecnologías de la Información y la Comunicación (TIC), en donde la información del sector salud junto a los procesos y los sistemas que hacen uso de ella, son activos importantes para los hospitales. La información como recurso invaluable debe ser protegida en su totalidad y tomando en cuenta el creciente aumento de amenazas informáticas que buscan sustraer de las organizaciones su información, con el fin de llevar a cabo fraudes, efectuar ataques de denegación de servicio o afectar a la imagen de la institución.

De acuerdo al informe salud y ciberseguridad (health care and cyber security) indica que “En los últimos dos años el 81% de los hospitales y aseguradoras de salud sufrieron una brecha en sus datos” (Bell & Ebert , 2015). En donde “Todos estos incidentes provocaron una pérdida en los datos, mostrando que los incidentes registrados no se tratan solo de un malware o un virus, sino que además se trata

de una exfiltración por parte del personal que pertenece a la organización (Bell & Ebert , 2015).

> Según (Areitio, 2008). "La seguridad Informática no solo debe encargarse de los posibles fallos desaprensivos, sino que también debe tener en cuenta los errores que se pudieran generar por el mal funcionamiento del hardware, así como prevenir acciones involuntarias que puedan afectar la seguridad de la información que se encuentre contenida en los sistemas. La seguridad informática también ha pasado de utilizarse para preservar los datos clasificados del gobierno en cuestiones militares, a tener una aplicación de dimensiones inimaginables y crecientes que incluyen transacciones financieras, acuerdos contractuales, información personal, archivos médicos, negocios por Internet y más".

La información, junto a los procesos y los sistemas que hacen uso de ella, son activos importantes para los hospitales y clínicas; en donde la confidencialidad, integridad y disponibilidad de dicha información les permitirá prestar con eficiencia su cartera de servicios médicos, permitiéndoles desarrollar efectivamente su misión y visión social.

En la actualidad existen marcos de referencia, normas y buenas prácticas para solventar este problema; entre ellos se encuentran las normas ISO 27000, COBIT 5, ITIL V3, entre otros. COBIT 5 e ITIL V3 permiten el Gobierno de las Tecnologías de la Información (TI) y la Gestión de Servicios de TI respectivamente. A diferencia de las normas ISO 27000 que son normas internacionales específicas para seguridad de la información y que permiten a cualquier organización reducir riesgos y maximizar el valor de las tecnologías de la información, además de acceder a una certificación que demuestra que se tienen bajo control la seguridad de la Información a través de los sistemas más adecuados de detección y eliminación de las amenazas y vulnerabilidades.

Por lo cual el presente proyecto de titulación consiste en proponer un modelo de Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil;

que permita garantizar la integridad, disponibilidad y confidencialidad de la información, mediante el uso de la Norma ISO 27799:2008, ISO/IEC 27005:2013 e ISO/IEC 27002:2013.

CAPÍTULO 2: MARCO TEÓRICO

2.1 EL SISTEMA NACIONAL DE SALUD EN EL ECUADOR

En el Ecuador según la Constitución de la República del año 2008, en su calidad de norma suprema del Gobierno establece que la salud es un derecho garantizado por el Ecuador para que toda persona alcance el nivel más alto posible de salud física y mental y los mecanismos para su realización y de igual manera define los lineamientos principales sobre los cuales se construye el Sistema Nacional de Salud (SNS). Considerando lo anterior el artículo 32 de la Constitución de la Republica, en la sección séptima sobre la salud como un derecho garantizado por el Estado, dice:

> Art. 32.- La salud es un derecho que garantiza el Estado, cuya realización se vincula al ejercicio de otros derechos, entre ellos el derecho al agua, la alimentación, la educación, la cultura física, el trabajo, la seguridad social, los ambientes sanos y otros que sustentan el buen vivir (Constitución de la República del Ecuador, 2008, pág. 17).

La Constitución de la República del Ecuador, también hace referencia al establecimiento del Sistema Nacional de Salud (SNS), señalando sus principios, integrantes, obligaciones y definiendo una autoridad sanitaria nacional, según indican los artículos 358, 359, 360, 361 y 362 de la sección segunda sobre la salud:

> Art. 358.- El Sistema Nacional de Salud tendrá por finalidad el desarrollo, protección y recuperación de las capacidades y potencialidades para una vida saludable e integral, tanto individual como colectiva, y reconocerá la diversidad social y cultural. El sistema se guiará por los principios generales del sistema nacional de inclusión y equidad social, y por los de bioética, suficiencia e interculturalidad, con enfoque de género y generacional. (Constitución de la República del Ecuador, 2008, pág. 112).

> Art. 359.- El Sistema Nacional de Salud comprenderá las instituciones, programas, políticas, recursos, acciones y actores en salud; abarcará todas las dimensiones del derecho a la salud; garantizará la promoción, prevención, recuperación y rehabilitación en todos los niveles; y propiciará la participación ciudadana y el control social (Constitución de la República del Ecuador, 2008, pág. 112).
>
> Art. 360.- El sistema garantizará, a través de las instituciones que lo conforman, la promoción de la salud, prevención y (...).
> La red pública integral de salud que será parte del Sistema Nacional de Salud y estará conformada por el conjunto articulado de establecimientos estatales, de la seguridad social y con otros proveedores que pertenecen al Estado, con vínculos jurídicos, operativos y de complementariedad (Constitución de la República del Ecuador, 2008, pág. 112).
>
> Art. 361.- El Estado ejercerá la rectoría del sistema a través de la autoridad sanitaria nacional, será responsable de formular la política nacional de salud, y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector (Constitución de la República del Ecuador, 2008, pág. 112).

El Sistema Nacional de Salud a través de la Ley Orgánica del Sistema Nacional de Salud (LOSNS) “establece los principios y normas generales para la organización y funcionamiento del SNS que regirá en todo el territorio nacional” (Ministerio de Salud Pública, 2012, pág. 1), éste sistema tiene como objetivo mejorar el nivel de salud y vida de la población ecuatoriana y hacer efectivo el ejercicio del derecho a la salud. En la Tabla 1 se detallan las cinco funciones fundamentales que ejerce el Sistema Nacional de Salud:

Tabla 1. Funciones del Sistema Nacional de Salud.

Funciones del Sistema Nacional de Salud		
Rectoría	El Estado garantizará la rectoría del sistema a través de la Autoridad Sanitaria Nacional, será responsable de formular la política nacional de salud, y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector.	Constitución de la República del Ecuador Art. 361
Coordinación	Es la función del sistema que coordina el relacionamiento entre las demás funciones y entre los integrantes del Sistema. Su ejercicio es competencia del Ministerio Salud Pública, en todos sus niveles, como autoridad sanitaria nacional, apoyado por los Consejos de Salud.	Ley Orgánica del Sistema Nacional de Salud Art. 10
Provisión de servicios	La provisión de servicios de salud es plural y con participación coordinada de las instituciones prestadoras. El Sistema establecerá los mecanismos para que las instituciones garanticen su operación en redes y aseguren la calidad, continuidad y complementariedad de la atención.	Ley Orgánica del Sistema Nacional de Salud Art.11
Aseguramiento	Es la garantía de acceso universal y equitativo de la población al Plan Integral de Salud en cumplimiento al derecho ciudadano a la protección social en salud. Se promoverá la ampliación de cobertura de salud de todas las entidades prestadoras de servicios y del Seguro General Obligatorio y Seguro Social Campesino, pertenecientes al IESS, de otros seguros públicos, como el Issfa e Isspol.	Ley Orgánica del Sistema Nacional de Salud Art.12
Financiamiento	El financiamiento es la garantía de disponibilidad y sostenibilidad de los recursos financieros necesarios para la cobertura universal en salud de la población. El Consejo Nacional de Salud establecerá mecanismos que permitan la asignación equitativa y solidaria de los recursos financieros entre grupos sociales, provincias y cantones del país, así como su uso eficiente.	Ley Orgánica del Sistema Nacional de Salud Art. 13

Fuente: Adaptado de (Flores Ma. & Castillo A., 2012, pág. 6).

El Sistema Nacional de Salud del Ecuador está compuesto por instituciones del sector público, privado y mixto, que actúan en el sector de la salud, o en campos

directamente relacionados con ella. En la Tabla 2 se listan las diecisiete entidades que forman parte del Sistema Nacional de Salud.

Tabla 2. Entidades que forman parte del Sistema Nacional de Salud

Entidades que forman parte del Sistema Nacional de Salud	
1	Ministerio de Salud Pública y sus entidades adscritas.
2	Ministerios que participan en el campo de la salud.
3	El Instituto Ecuatoriano de Seguridad Social, IESS; Instituto de Seguridad Social de las Fuerzas Armadas, Issfa; e Instituto de Seguridad Social de la Policía Nacional, Isspol.
4	Organizaciones de salud de la Fuerza Pública: Fuerzas Armadas y Policía Nacional.
5	Las Facultades y Escuelas de Ciencias Médicas y de la Salud de las Universidades y Escuelas Politécnicas.
6	Junta de Beneficencia de Guayaquil.
7	Sociedad de Lucha Contra el Cáncer, Solca.
8	Cruz Roja Ecuatoriana.
9	Organismos seccionales: Consejos Provinciales, Concejos Municipales y Juntas Parroquiales.
10	Entidades de salud privadas con fines de lucro: prestadoras de servicios, de medicina prepagada y aseguradoras.
11	Entidades de salud privadas sin fines de lucro: organizaciones no gubernamentales (ONG), servicios pastorales y fiscomisionales.
12	Servicios comunitarios de salud y agentes de la medicina tradicional y alternativa.
13	Organizaciones que trabajan en salud ambiental.
14	Centros de desarrollo de ciencia y tecnología en salud.
15	Organizaciones comunitarias que actúen en promoción y defensa de la salud.
16	Organizaciones gremiales de profesionales y trabajadores de la salud.
17	Otros organismos de carácter público, del régimen dependiente o autónomo y de carácter privado que actúen en el campo de la salud.

Fuente: Adaptado de (Flores Ma. & Castillo A., 2012, pág. 7)

Mediante el ejercicio de las instituciones que pertenecen al Sistema Nacional de Salud, se busca cumplir con cinco objetivos principales, como menciona la Ley Orgánica del Sistema Nacional de Salud en su artículo 3:

- Garantizar el acceso equitativo y universal a servicios de atención integral de salud, a través del funcionamiento de una red de servicios de gestión desconcentrada y descentralizada.

- Proteger integralmente a las personas de los riesgos y daños a la salud; al medio ambiente de su deterioro o alteración.
- Generar entornos, estilos y condiciones de vida saludables.
- Promover la coordinación, la complementación y el desarrollo de las instituciones del sector.
- Incorporar la participación ciudadana en la planificación y veeduría en todos los niveles y ámbitos de acción del Sistema Nacional de Salud. (Ministerio de Salud Pública, 2012, pág. 2).

Se debe considerar que las entidades de salud privada con fines de lucro que prestan servicios de medicina prepagada y aseguradoras, pertenecen al Sistema Nacional de Salud y de igual manera deben regirse a las disposiciones del Ministerio de Salud pública (MSP) como su ente rector.

2.2 LEYES Y REGLAMENTOS SOBRE CONFIDENCIALIDAD DE LA INFORMACIÓN PARA EL SECTOR SALUD DEL ECUADOR

En el Ecuador a través de la Constitución del año 2008, se garantiza la confidencialidad de la información de los pacientes, que se generen a través de la utilización de los diferentes tipos de servicios de salud, según delinea el artículo 362 de la sección segunda sobre la salud.

> Art. 362.- La atención de salud como servicio público se prestará a través de las entidades estatales, privadas, autónomas, comunitarias y aquellas que ejerzan las medicinas ancestrales alternativas y complementarias. Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes (Constitución de la República del Ecuador, 2008, pág. 113).

Para las instituciones de salud que reciben o administran fondos públicos la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), sobre confidencialidad de la información en el artículo 6 indica que:

> Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República (Congreso Nacional, 2004, pág. 3).

Así mismo, la Ley orgánica de Salud en su artículo 7 de los Derechos y deberes de las personas y del Estado en relación con la salud, sobre confidencialidad de la información en historias clínicas detalla que:

> Art. 7.- Toda persona, sin discriminación por motivo alguno, tiene en relación a la salud, los siguientes derechos (...) f) Tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida (Congreso Nacional, 2006, pág. 5).

Se debe considerar también la ley de derechos y amparo del paciente, la cual promueve el derecho a la confidencialidad para los pacientes que utilicen los servicios de las entidades adscritas al SNS, como lo indica en su artículo 4:

> Art. 4.- Derecho a la confidencialidad: Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial (Ministerio de Salud Pública, 2006, pág. 1).

Finalmente, en el año 2015 mediante Acuerdo Ministerial 5216 se expide el Reglamento de Información Confidencial en el SNS que tiene como objetivo “establecer las condiciones operativas de la aplicación de los principios de manejo y gestión de la información confidencial de los pacientes y sus disposiciones serán

de cumplimiento obligatorio dentro del Sistema Nacional de Salud" (Ministerio de Salud Pública, 2015, pág. 2).

El reglamento a través de sus artículos 2, 3, 4, 5, 6 establece principios como Confidencialidad, Integridad, Disponibilidad, Seguridad en el manejo de la información y Secreto Médico.

> Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información (Ministerio de Salud Pública, 2015, pág. 3).
>
> Art. 3.- Integridad de la información. - Es la cualidad o propiedad de la información que asegura que no ha sido mutilada, alterada o modificada, por lo tanto mantiene sus características y valores asignados o recogidos en la fuente. Esta cualidad debe mantenerse en cualquier formato de soporte en el que se registre la información, independientemente de los procesos de migración entre ellos (Ministerio de Salud Pública, 2015, pág. 3).
>
> Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional (Ministerio de Salud Pública, 2015, pág. 3).
>
> Art. 5.- Seguridad en el manejo de la información. - Es el conjunto sistematizado de medidas preventivas y reactivas que buscan resguardar y proteger la información para mantener su condición de confidencial, así como su integridad y disponibilidad. Inicia desde el momento mismo de la generación de la información y trasciende hasta el evento de la muerte de la persona (...) (Ministerio de Salud Pública, 2015, pág. 3).
>
> Art. 6.- Secreto Médico. - Es la categoría que se asigna a toda información que es revelada por un/a usuario/a al profesional de la salud que le brinda la atención de salud. Se configura como un compromiso que adquiere el médico ante el/la usuario/a y la sociedad, de guardar silencio sobre toda

información que llegue a conocer sobre el/la usuario/a en el curso de su actuación profesional (Ministerio de Salud Pública, 2015, pág. 3).

En lo que respecta específicamente a Seguridad en la Custodia de las Historias Clínicas, el Acuerdo Ministerial 5216 en su cuarto capítulo Seguridad en la Custodia de las Historias Clínicas acuerda:

> Art. 14.- La historia clínica sólo podrá ser manejada por personal de la cadena sanitaria. Como tal se entenderá a los siguientes profesionales: médicos, psicólogos, odontólogos, trabajadoras sociales, obstetrices, enfermeras, además de auxiliares de enfermería y personal de estadística (Ministerio de Salud Pública, 2015, pág. 4).
>
> Art. 15.- El acceso a documentos archivados electrónicamente será restringido a personas autorizadas por el responsable del servicio o del establecimiento, mediante claves de acceso personales (Ministerio de Salud Pública, 2015, pág. 4).
>
> Art. 16.- La custodia física de la historia clínica es responsabilidad de la institución en la que repose. El personal de la cadena sanitaria, mientras se brinda la prestación, es responsable de la custodia y del buen uso que se dé a la misma, generando las condiciones adecuadas para el efecto (Ministerio de Salud Pública, 2015, pág. 4).
>
> Art. 17.- El archivo de historias clínicas es un área restringida, con acceso limitado solo a personal de salud autorizado, donde se guardan de manera ordenada, accesible y centralizada todas las historias clínicas que se manejan en el establecimiento. Se denomina activo cuando cuenta con historias activas, esto es con registros de hasta cinco años atrás y se denomina pasivo cuando almacena aquellas que tienen más de cinco años sin registros, tomando en cuenta la última atención al paciente (Ministerio de Salud Pública, 2015, pág. 4).
>
> Art. 18.- Los datos y la información consignados en la historia clínica y los resultados de pruebas de laboratorio e imagenología registrados sobre cualquier medio de soporte ya sea físico, electrónico, magnético o digital, son de uso restringido y se manejarán bajo la responsabilidad del personal

> operativo y administrativo del establecimiento de salud, en condiciones de seguridad y confidencialidad que impidan que personas ajenas puedan tener acceso a ellos (Ministerio de Salud Pública, 2015, pág. 4).
>
> Art. 19.- Todas las dependencias que manejen información que contenga datos relevantes sobre la salud de los/las usuarios/as deberán contar con sistemas adecuados de seguridad y custodia (Ministerio de Salud Pública, 2015, pág. 4).
>
> Art. 20.- Los documentos físicos que contengan información confidencial de los/las usuarios/as y que no requieran ser archivados, deberán ser destruidos evitando su reutilización, de conformidad a lo dispuesto en el Capítulo II del Manual del Manejo, Archivo de las Historias Clínicas (Ministerio de Salud Pública, 2015, pág. 4).

Para las instituciones públicas la Secretaría Nacional de la Administración Pública (SNAP) tiene como misión “Mejorar la eficiencia de las instituciones del Estado Central a través de políticas y procesos que optimicen la calidad, la transparencia y la calidez del Servicio Público” (Secretaría Nacional de la Administración Pública, En línea). Y que mediante el Acuerdo Ministerial 166 se emite el Esquema Gubernamental de Seguridad de la Información (EGSI), donde la “SNAP dispone a las entidades de la Administración Pública Central, Institucional, y que dependen de la Función Ejecutiva, el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información (SGI)” (Secretaría Nacional de la Administración Pública, 2013). Las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 vigentes en la fecha de elaboración del presente trabajo son: NTE INEN – ISO/IEC 27001 es una traducción idéntica de la norma internacional ISO/IEC 27001:2013, NTE INEN – ISO/IEC 27005 es una traducción idéntica de la norma internacional ISO/IEC 27005:2008, NTE INEN – ISO/IEC 27002 es una traducción idéntica de la norma internacional ISO/IEC 27002:2013 y NTE INEN – ISO 27799 es una traducción idéntica de la norma internacional ISO 27799:2008.

De igual manera, en el Código Orgánico Integral Penal (COIP), como el conjunto sistematizado y organizado de normas jurídicas de carácter punitivo, se

establece delitos y penas conforme al sistema penal ecuatoriano, al comprobarse una infracción relacionada con la protección de la información considerada reservada.

> Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.
>
> Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, 2014, pág. 79).
>
> Art. 230.- Interceptación ilegal de datos. Será sancionada con pena privativa de libertad de tres a cinco años:
>
> 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
>
> 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
>
> 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (Código Orgánico Integral Penal, 2014, pág. 80).

Art. 231.- Transferencia electrónica de activo patrimonial. La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona (Código Orgánico Integral Penal, 2014, pág. 80).

Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad (Código Orgánico Integral Penal, 2014, pág. 81).

Art. 233.- Delitos contra la información pública reservada legalmente. La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad (Código Orgánico Integral Penal, 2014).

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Código Orgánico Integral Penal, 2014).

2.3 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información es un proceso continuo que consiste en:

Garantizar que los riesgos de la seguridad de la información sean identificados valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y

adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías (ISO 27000.ES, 2005).

Independiente de su naturaleza o segmento de mercado, las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a los activos críticos de la información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Actualmente la información junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. "La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos" (ISO 27000.ES, 2005).

La implementación de un Sistema de Gestión de Seguridad de la Información mediante la utilización de buenas prácticas o normas como la familia ISO/IEC 27000 permite "conservar la confidencialidad, integridad y disponibilidad de la información al aplicar un proceso de gestión de riesgo y le entrega confianza a las partes interesadas cuyos riesgos son gestionados de manera adecuada" (ISO/IEC, 2013, pág. 1). En la Figura 1 se muestra la relación entre los diferentes actores que permiten obtener confidencialidad, integridad y disponibilidad en la información.

Figura 1.Objetivos de la seguridad informática

Fuente: Adaptado de (Calderón, 2017)

2.4 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

Las normas de seguridad de la información son documentos aprobados por organismos reconocidos como la ISO (Organización Internacional de Normalización), a través de los cuales se establecen actividades para cumplir condiciones mínimas que debe poseer un producto o servicio.

La implementación de las normas, es la actividad que tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes repetidos, con el fin de obtener un nivel de ordenamiento óptimo, en un contexto dado, que puede ser tecnológico, político o económico.

Las normas de seguridad más relevantes y que son normadas por el Instituto Ecuatoriano de Normalización (INEN) son la biblioteca de infraestructura de tecnología de la información (ITIL) en su versión 3, la norma ISO/IEC 27000 y el marco de referencia Objetivos de Control para Información y Tecnologías Relacionadas (COBIT) en su versión 5.

2.5 NORMA ISO/IEC 27000

La Normas ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Estas normas especifican “los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI)” (ISO 27000.ES, 2005).

Las normas de Gestión de la Seguridad de la Información que son relevantes para esta investigación y que hasta la fecha son normadas por el Instituto Ecuatoriano de Normalización (INEN) son:

- ISO/IEC 27001: 2013 - Técnicas de Seguridad de las Tecnologías de la Información: Requisitos de los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 27002: 2013 - Técnicas de Seguridad de las Tecnologías de la Información: Código de Prácticas para la Gestión de la Seguridad de la Información.
- ISO/IEC 27005: 2008 - Técnicas de Seguridad de las Tecnologías de la Información: Gestión de riesgos de la Seguridad la Información.
- ISO 27799: 2008 - Informática de la Salud: Gestión de la Seguridad de la Información en Salud utilizando ISO / IEC 27002.

2.5.1 NORMA ISO/IEC 27001:2013

La Norma de Requisitos de los Sistemas de Gestión de la Seguridad de la Información - ISO/IEC 27001:2013, es la norma principal de la familia de la ISO/IEC 27000, y promueve la adopción de un enfoque basado en procesos y especifica los "requisitos para la creación, implantación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información" (ISO/IEC, 2013, pág. 1). Los requisitos establecidos en esta norma son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño y naturaleza.

La versión 2013 de la norma ISO/IEC 27001, alineó su estructura conforme a los lineamientos definidos en el Anexo SL de las directivas ISO/IEC, con el objetivo de mantener la compatibilidad entre las normas ISO de sistemas de gestión que se han ajustado a este anexo. El Anexo SL "es el estándar que define la nueva estructura de Alto Nivel para todos los sistemas de gestión de las Normas ISO" (ISO/IEC, 2013, pág. 1).

Los dominios de la norma ISO/IEC 27001:2013 corresponden a los diez diferentes capítulos que establecen los requerimientos que las organizaciones

deben cumplir para el establecimiento de un Sistema de Gestión de Seguridad de la Información:

- En los tres primeros capítulos se define el alcance que tiene la normativa ISO/IEC 27001: 2013 para poder certificar el SGSI a una organización.
- En el capítulo 4 (Contexto de la organización), se resalta la necesidad de hacer un análisis para identificar los problemas externos e internos que rodean a la organización. De esta forma se puede establecer el contexto del SGSI incluyendo las partes interesadas que deben estar dentro del alcance del SGSI.
- En el capítulo 5 (Liderazgo), se definen las responsabilidades de la alta dirección respecto al SGSI. Por ejemplo, “sus responsabilidades en la definición de la política de seguridad de la información alineada a los objetivos del negocio y la asignación de los recursos necesarios para la implementación del SGSI” (ISO/IEC, 2013, pág. 4).
- Dentro del capítulo 6 (Planificación), se desarrolla la definición de objetivos de seguridad claros que permitan elaborar planes específicos para su cumplimiento. En esta planificación debe también considerarse la identificación de aquellos riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- En el capítulo 7 (Apoyo), se describen los requerimientos para implementar el SGSI incluyendo recursos, personas y elementos de comunicación para las partes interesadas en el sistema.
- El capítulo 8 (Operación), establece los mecanismos para planear y controlar las operaciones y requerimientos de seguridad. Las evaluaciones periódicas de riesgos constituyen el enfoque central para la gestión del SGSI. Las vulnerabilidades y las amenazas a la información se utilizan para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad.
- En el capítulo 9 (Evaluación del desempeño), se definen las bases para medir la efectividad y desempeño del SGSI. Dichas mediciones se realizan usualmente a través de auditorías internas.
- Finalmente, el capítulo 10 (Mejora), propone, a partir de las no conformidades identificadas en el SGSI, establecer las acciones correctivas más efectivas para solucionarlas.

También, se puede indicar que al igual que la norma ISO/IEC 27001 del año 2005, el Anexo SL toma en consideración el modelo de mejora continua PDCA (Planear, Hacer, Verificar y Actuar). Este nuevo enfoque en la estructura de la norma ISO/IEC 27001:2013 basado en el Anexo SL, ayuda a las organizaciones que deseen integrar sus diferentes sistemas de gestión, como el de Calidad, Ambiental, Seguridad de la Información, etc., en un único sistema integrado de gestión. En la Tabla 3 se muestra la estructura de la norma ISO/IEC 27001:2013 y su relación con el ciclo PDCA.

Tabla 3. Dominios de la norma ISO/IEC 27001:2013 y relación con el ciclo PDCA

#	**ISO/IEC 27001:2013**	**PDCA**
0	Introducción	_
1	Alcance	_
2	Referencias normativas	_
3	Términos y definiciones	_
4	Contexto de la organización	P
5	Liderazgo	P
6	Planificación	P
7	Soporte	P
8	Operación	D
9	Evaluación del desempeño	C
10	Mejora	A

Fuente: Adaptado de (ISO/IEC, 2013, pág. iii)

El modelo PDCA mostrado en la Figura 2, está compuesto por planear – hacer – verificar – actuar y que aplicados a los procesos del Sistema de Gestión de Seguridad de la Información indica:

- **Planear (Plan):** “Establecer políticas, objetivos, procesos y procedimientos del SGSI, los cuales permiten optimizar el manejo del riesgo y obtener una idea

macro del mejoramiento de la Seguridad de la Información" (ISO/IEC, 2005, pág. vi)

- **Hacer (Do): "**Ejecutar las políticas, objetivos, procesos y procedimientos que se encuentran en el SGSI" (ISO/IEC, 2005, pág. vi) .
- **Verificar (Check):** "Hacer un levantamiento de información y verificar si se ha cumplido con los objetivos establecidos en el SGSI, lo cual generará un informe donde se encuentren plasmados los resultados y novedades encontradas" (ISO/IEC, 2005, pág. vi) .
- **Actuar (Act)**: "Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna del SGSI y la revisión gerencial u otra revisión relevante, para lograr el mejoramiento continuo del SGSI" (ISO/IEC, 2005, pág. vi) .

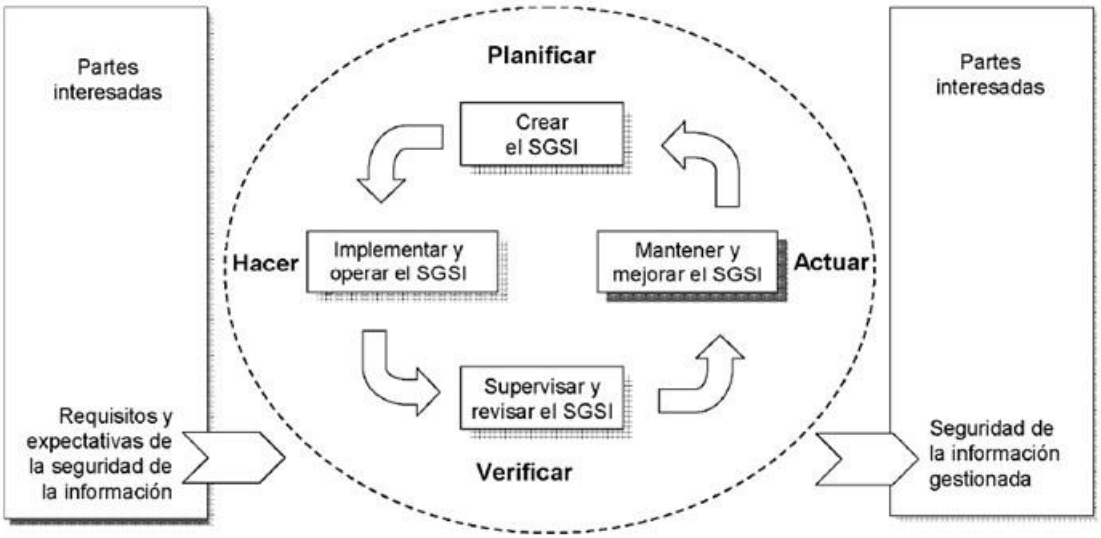


Figura 2. Modelo PDCA aplicado a los procesos SGSI.

Fuente: Tomado de (ISO/IEC, 2005, pág. vi)

2.5.2 NORMA ISO/IEC 27002:2013

La norma ISO/IEC 27002:2013, anteriormente conocida como ISO/IEC 17799, tiene por objeto proporcionar "directrices para normas organizacionales de

seguridad de la información y para las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta los riesgos del entorno de seguridad de la información de la organización" (ISO/IEC, 2013, pág. 1).

Esta Norma Internacional está diseñada para que "las organizaciones la utilicen como referencia para seleccionar controles dentro del proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI)" (ISO/IEC, 2013, pág. vi). En la Figura 3 se muestra el contenido de la Norma ISO/IEC 27002:2013.

Figura 3. Contenidos de la norma ISO 27002:2013

Fuente: Tomado de (UNIT- Instituto Uruguayo de Normas Técnicas, 2015)

Las 14 cláusulas de control de la seguridad y 114 controles de la norma ISO/IEC 27002:2013 proporcionan una guía general sobre las metas de gestión de la Seguridad de la Información más comúnmente aceptadas de manera que se obtenga una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos, logrando reducir las amenazas hasta tener un nivel de riesgo asumible por la organización. A continuación, en la Tabla 4 se muestra la estructura de la norma ISO/IEC 27002:2013.

Tabla 4. Estructura de la Norma ISO/IEC 27002:2013.

Norma ISO/IEC 27002:2013.
0. Introducción
1. Objeto
2. Referencias normativas
3. Términos y definiciones
4. Estructura de esta norma
5. Políticas de seguridad.
5.1. Directrices de la dirección en seguridad de la información.
6. Aspectos organizativos de la seguridad de la información.
6.1. Organización interna.
6.2. Dispositivos para movilidad y teletrabajo.
7. Seguridad ligada a los recursos humanos.
7.1. Antes de la contratación.
7.2. Durante la contratación.
7.3. Cese o cambio de puesto de trabajo.
8. Gestión de activos.
8.1. Responsabilidad sobre los activos.
8.2. Clasificación de la información.
8.3. Manejo de los soportes de almacenamiento.
9. Control de acceso.
9.1. Requisitos de negocio para el control de acceso.
9.2. Gestión de acceso de usuario.
9.3. Responsabilidad del usuario.
9.4. Control de acceso a sistemas y aplicaciones.
10. Criptografía
10.1. Controles criptográficos.
11. La seguridad física y del ambiente.
11.1. Áreas seguras.
11.2. Seguridad de los equipos.

Fuente: Adaptado de (ISO/IEC, 2013, pág. iii)

Norma ISO/IEC 27002:2013.
12. Seguridad de las operaciones
12.1. Responsabilidades y procedimientos de operación.
12.2. Protección contra código malicioso.
12.3. Copia de seguridad.
12.4. Registro de actividad y supervisión.
12.5. Control del software en explotación.
12.6. Gestión de vulnerabilidades técnicas.
12.7. Consideraciones de auditorías de los sistemas de información.
13. Seguridad de las comunicaciones.
13.1. Gestión de la seguridad en las redes.
13.2. Intercambio de información con partes externas.
14. Adquisición, desarrollo y mantenimiento de los sistemas de información.
14.1. Requisitos de seguridad de los sistemas de información.
14.2. Seguridad de los procesos de desarrollo y soporte.
14.3. Datos de prueba.
15. Relaciones con suministradores.
15.1. Seguridad de la información en las relaciones con suministradores.
15.2. Gestión de la prestación de servicios por suministradores.
16. Gestión de los incidentes en la seguridad de la información.
16.1. Gestión de incidentes de seguridad de la información y mejoras.
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
17.1. Continuidad de seguridad de la información.
17.2. Redundancias.
18. Cumplimiento.
18.1. Cumplimiento de los requisitos legales y contractuales.
18.2. Revisiones de la seguridad de la información.

Fuente: Adaptado de (ISO/IEC, 2013, pág. iii)

2.5.3 NORMA ISO/IEC 27005:2008

La norma ISO/IEC 27005:2008 brinda pautas para la Gestión de Riesgos en la Seguridad de la Información, dando soporte particular a los requisitos de un Sistema de Gestión de la Seguridad de la Información (SGSI). Sin embargo esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información, sino que corresponde a cada "organización definir su enfoque para la gestión del riesgo, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial" (ISO/IEC, 2008, pág. vi).

En esta norma de Gestión de riesgos de la Seguridad la Información, "se plantean las directrices para la gestión de riesgos en la seguridad de la información, y se relaciona estrechamente con los conceptos generales presentados en la Norma 27001" (ISO/IEC, 2008, pág. vi) ya que brinda un soporte a estos conceptos, y busca que se haga una implementación satisfactoria de la seguridad de la información con base en el enfoque de la gestión del riesgo. De igual manera esta norma es aplicable a cualquier tipo de organización (empresas comerciales, entidades del gobierno, etc.), e incluso a solo una parte de la organización, que quieran gestionar los riesgos que puedan comprometer su información.

ISO/IEC 27005:2008 no proporciona una metodología concreta de Análisis de Riesgos, sino que proporciona un conjunto de directrices para la correcta realización de un Análisis de Riesgos mediante la descripción de un proceso estructurado, riguroso y sistemático de los elementos que debe incluir toda buena metodología de Análisis de Riesgo. Constituye, por tanto, una ampliación del apartado 6.1 Acciones para abordar los riesgos y las oportunidades de la normativa ISO/IEC 27001:2013, en el que se presenta la gestión de riesgos como la piedra angular de un SGSI, pero sin prever una metodología específica para ello. La estructura de la norma se muestra en la Tabla 5.

Tabla 5. Estructura de la norma ISO/IEC 27005:2008

	Norma ISO/IEC 27005:2008
0	Introducción.
1	Objeto y campo de aplicación
2	Referencias normativas.
3	Términos y definiciones.
4	Estructura.
5	Fondo.
6	Descripción del proceso de ISRM.
7	Establecimiento Contexto.
8	Información sobre la evaluación de riesgos de seguridad (ISRA).
9	Tratamiento de Riesgos Seguridad de la Información.
10	Admisión de Riesgos Seguridad de la información.
11	Comunicación de riesgos de seguridad de información.
12	Información de seguridad Seguimiento de Riesgos y Revisión.
	Anexo A: Definición del alcance del proceso.
	Anexo B: Valoración de activos y evaluación de impacto.
	Anexo C: Ejemplos de amenazas típicas.
	Anexo D: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad.
	Enfoques ISRA: Anexo E.

Fuente: Adaptado de (ISO/IEC, 2008, pág. iii)

El proceso de gestión del riesgo de la seguridad de la información se puede aplicar a la organización en su totalidad, a una parte separada de la organización (un departamento, una ubicación física, un servicio), a cualquier sistema de información o a aspectos particulares del control. Dicho proceso de gestión del riesgo en la seguridad de la información consta de: establecimiento del contexto, valoración o evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo. Las actividades de valoración del riesgo y tratamiento del riesgo pueden ser iterativas, para conseguir

un equilibrio entre la reducción de tiempo y el esfuerzo que se requiere para identificar los controles, y que los riesgos altos se valoren de manera correcta, este proceso se muestra en la Figura 4.

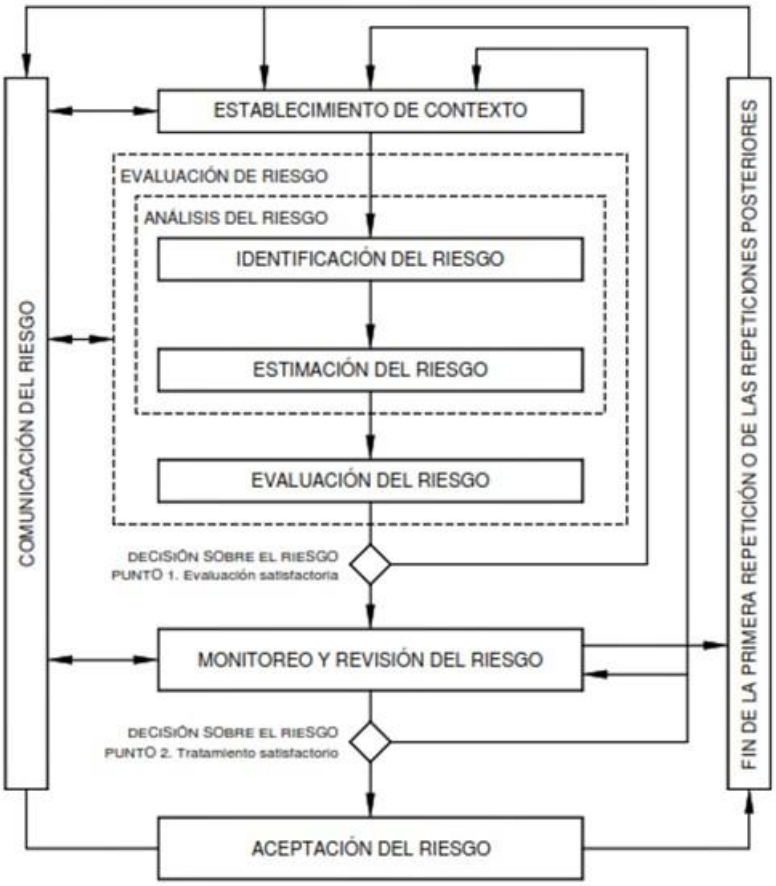


Figura 4 Proceso de gestión del riesgo de la seguridad de la información

Fuente: Adaptado de (ISO/IEC, 2008, pág. 5)

2.5.4 NORMA ISO 27799:2008

La ISO 27799:2008 fue publicada en junio del año 2008 y desarrollada por el Comité Técnico ISO/TC-215 responsable de Salud Informática. Dicho documento contiene una especificación de las consideraciones que se debe tener en cuenta en el análisis y diseño de un SGSI en instituciones relacionadas al cuidado de la salud. Esta norma “establece un conjunto de controles detallados para la gestión de la Seguridad de la Información de salud y proporciona directrices de buenas prácticas de Seguridad de la Información de salud” (ISO, 2008, pág. 1).

La norma ISO 27799:2008 “está pensada como un documento complementario a la ISO/IEC 27002. No pretende suplantar la norma ISO/IEC 27002 e ISO/IEC 27001, más bien es un complemento a estas normas más genéricas” (ISO, 2008, pág. v). En la Tabla 6 se muestra la estructura de la norma.

Tabla 6. Estructura de la norma ISO 27799:2008

ISO 27799:2008	
1.- Alcance	
2.- Referencias normativas	
3.- Términos y definiciones	
4.- Términos abreviados	
5.- Seguridad de la información sanitaria	• Objetivos de seguridad de la información en salud • Seguridad de la información dentro de la gobernanza de la información • Gobernanza de la información dentro del gobierno corporativo y clínico • Información de salud a proteger • Amenazas y vulnerabilidades en la seguridad de la información de salud
6.- Plan de acción práctico para la aplicación de la norma ISO/IEC 27002	• Taxonomía de las normas ISO/IEC 27002 e ISO/IEC 27001 • Compromiso de la administración con la implementación de ISO/IEC 27002 • Establecer, operar, mantener y mejorar el SGSI • Planificar: establecimiento del SGSI • Hacer: implementar y operar el SGSI • Comprobar: monitoreo y revisión del SGSI • Actuar: mantener y mejorar el SGSI
7.- Implicaciones para la salud de ISO/IEC 27002.	• General • Política de seguridad de la información • Organización de la seguridad de la información • Gestión de activos • Seguridad de los recursos humanos • Seguridad física y medio ambiental • Comunicaciones y gestión de operaciones • Control de acceso • Adquisición, desarrollo y mantenimiento de sistemas de información • Gestión de incidentes de seguridad de la información • Aspectos de la seguridad de la información en la gestión de la continuidad del negocio (BCM) • Conformidad
Anexo A (informativo): Las amenazas a la seguridad informática de la salud	
Anexo B: Tareas y documentación del SGSI	
Anexo C: Beneficios potenciales y atributos de las herramientas de apoyo	

Fuente: Adaptado de (ISO, 2008, pág. iii)

2.6 BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN (ITIL)

La Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) es "considerada un marco de trabajo que hace referencia a las mejores prácticas para la gestión de servicios de TI" (Van Bon & Van Der Veen, 2011, pág. 9). Dichas prácticas pueden ajustarse a los requerimientos de las organizaciones, de todo tamaño, y están dirigidas a alcanzar metas corporativas a través de:

- Un enfoque sistemático de los servicios de Tecnología de la Información centrado en los procesos y procedimientos.
- El establecimiento de estrategias para la gestión operativa de la infraestructura de Tecnología de la Información.

La gestión de servicios de Tecnología de la Información tiene como objetivos:

- Alinear la infraestructura de Tecnología de la Información con los procesos de negocio
- Reducir los riesgos asociados a los servicios de Tecnología de la Información.
- Proporcionar una correcta gestión de la calidad
- Generar valor al negocio.

ITIL v3 presenta un enfoque para la gestión de los servicios de Tecnología de la Información mediante el Ciclo de Vida de los servicios, el cual consta de cinco fases enumeradas a continuación:

a) **Estrategia del Servicio: "**Propone tratar la gestión de los servicios como un activo estratégico. De manera general se busca definir la perspectiva, planes y estándares que el proveedor requiere conocer para dar servicios que cumplan con los objetivos del negocio" (Van Bon & Van Der Veen, 2011).

b) **Diseño del Servicio:** En esta fase se busca "cubrir todos los principios y métodos para transformar los objetivos en servicios y activos para la

organización. Se definen los procesos, políticas, arquitectura de los servicios de modo que se abarquen los requisitos de la empresa" (Van Bon & Van Der Veen, 2011).

c) **Transición del Servicio:** Es la fase en el que se realiza "el desarrollo de los servicios, la adopción de los mismos en la organización y su mejora en el mantenimiento de ellos" (Van Bon & Van Der Veen, 2011).

d) **Operación del Servicio:** "Cubre las prácticas del día a día de los servicios, es decir, refiere a la operación y/o ejecución del servicio" (Van Bon & Van Der Veen, 2011).

e) **Mejora Continua del Servicio:** "Proporciona una guía base mediante la cual se busca mantener y mejorar los servicios en base a las fases anteriores" (Van Bon & Van Der Veen, 2011).

En la Tabla 7, se detalla el ciclo de vida con los 26 procesos de ITIL v3:

Tabla 7. Ciclo de vida y procesos de ITIL V3

Núm.	Procesos ITIL V3-2011	Ciclo de vida del Servicio
1	Gestión de la Estrategia para los servicios de TI	Estrategia del Servicio
2	Gestión del Portafolio de Servicios	
3	Gestión Financiera para los servicios de TI	
4	Gestión de la Demanda	
5	Gestión de las relaciones de negocios	
6	Coordinación del diseño	Diseño del Servicio
7	Gestión del Catálogo de Servicios	
8	Gestión del Nivel de Servicio	
9	Gestión de la Disponibilidad	
10	Gestión de la Capacidad	
11	Gestión de la Continuidad del Servicio de TI	
12	Gestión de la Seguridad de la información	
13	Gestión de Proveedores	

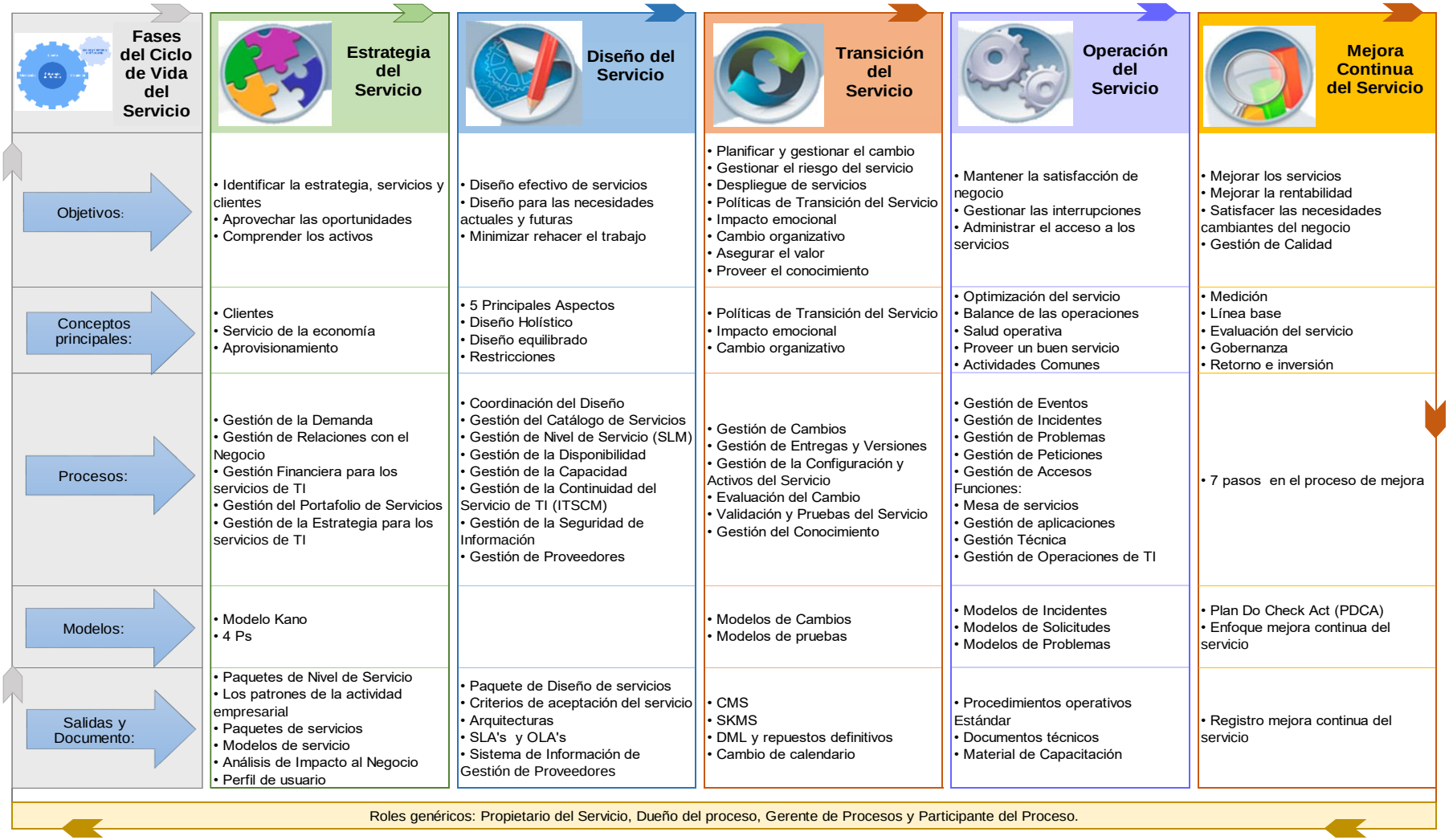
Fuente: Adaptado de (Van Bon & Van Der Veen, 2011)

Núm.	Procesos ITIL V3-2011	Ciclo de vida del Servicio
14	Planificación y Soporte de Transición	Transición del Servicio
15	Gestión del Cambio	
16	Gestión de la Configuración y servicios de A.	
17	Gestión de la Implementación y Ediciones	
18	Validación y Pruebas de Servicios	
19	Evaluación del cambio	
20	Gestión del Conocimiento	
21	Gestión de Eventos	Operación del Servicio
22	Gestión de Incidentes	
23	Cumplimiento de la Solicitud	
24	Gestión de Problemas	
25	Gestión del Acceso	
26	Siete pasos en el proceso de mejora - PDCA	Mejora Continua del Servicio

Fuente: Adaptado de (Van Bon & Van Der Veen, 2011)

A continuación en la tabla 8, se describirá un resumen de ITIL v3 en una sola página.

Tabla 8. ITIL v3 2011 en una sola página



Fases del Ciclo de Vida del Servicio	Estrategia del Servicio	Diseño del Servicio	Transición del Servicio	Operación del Servicio	Mejora Continua del Servicio
Objetivos:	• Identificar la estrategia, servicios y clientes • Aprovechar las oportunidades • Comprender los activos	• Diseño efectivo de servicios • Diseño para las necesidades actuales y futuras • Minimizar rehacer el trabajo	• Planificar y gestionar el cambio • Gestionar el riesgo del servicio • Despliegue de servicios • Políticas de Transición del Servicio • Impacto emocional • Cambio organizativo • Asegurar el valor • Proveer el conocimiento	• Mantener la satisfacción de negocio • Gestionar las interrupciones • Administrar el acceso a los servicios	• Mejorar los servicios • Mejorar la rentabilidad • Satisfacer las necesidades cambiantes del negocio • Gestión de Calidad
Conceptos principales:	• Clientes • Servicio de la economía • Aprovisionamiento	• 5 Principales Aspectos • Diseño Holístico • Diseño equilibrado • Restricciones	• Políticas de Transición del Servicio • Impacto emocional • Cambio organizativo	• Optimización del servicio • Balance de las operaciones • Salud operativa • Proveer un buen servicio • Actividades Comunes	• Medición • Línea base • Evaluación del servicio • Gobernanza • Retorno e inversión
Procesos:	• Gestión de la Demanda • Gestión de Relaciones con el Negocio • Gestión Financiera para los servicios de TI • Gestión del Portafolio de Servicios • Gestión de la Estrategia para los servicios de TI	• Coordinación del Diseño • Gestión del Catálogo de Servicios • Gestión de Nivel de Servicio (SLM) • Gestión de la Disponibilidad • Gestión de la Capacidad • Gestión de la Continuidad del Servicio de TI (ITSCM) • Gestión de la Seguridad de Información • Gestión de Proveedores	• Gestión de Cambios • Gestión de Entregas y Versiones • Gestión de la Configuración y Activos del Servicio • Evaluación del Cambio • Validación y Pruebas del Servicio • Gestión del Conocimiento	• Gestión de Eventos • Gestión de Incidentes • Gestión de Problemas • Gestión de Peticiones • Gestión de Accesos Funciones: • Mesa de servicios • Gestión de aplicaciones • Gestión Técnica • Gestión de Operaciones de TI	• 7 pasos en el proceso de mejora
Modelos:	• Modelo Kano • 4 Ps		• Modelos de Cambios • Modelos de pruebas	• Modelos de Incidentes • Modelos de Solicitudes • Modelos de Problemas	• Plan Do Check Act (PDCA) • Enfoque mejora continua del servicio
Salidas y Documento:	• Paquetes de Nivel de Servicio • Los patrones de la actividad empresarial • Paquetes de servicios • Modelos de servicio • Análisis de Impacto al Negocio • Perfil de usuario	• Paquete de Diseño de servicios • Criterios de aceptación del servicio • Arquitecturas • SLA's y OLA's • Sistema de Información de Gestión de Proveedores	• CMS • SKMS • DML y repuestos definitivos • Cambio de calendario	• Procedimientos operativos Estándar • Documentos técnicos • Material de Capacitación	• Registro mejora continua del servicio

Roles genéricos: Propietario del Servicio, Dueño del proceso, Gerente de Procesos y Participante del Proceso.

Fuente: Adaptado de (IT Training Zone, 2016)

2.7 COBIT 5

COBIT (Objetivos de Control para la información y Tecnologías relacionadas) es un marco de trabajo publicado por ISACA (Asociación de Control y Auditoría de Sistemas de Información) en el año 2012, con el objetivo de ayudar a las organizaciones a optimizar el valor de las TI manteniendo un equilibrio entre la generación de valor, la optimización de los niveles de riesgos y el uso eficiente de los recursos de la empresa.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el Gobierno y la Gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. (ISACA, 2012).

Con la versión 5 de COBIT, ISACA ofrece una guía para permitir que las Tecnologías de la Información sean gobernadas y gestionadas de una manera holística en toda la organización, cubriendo las áreas funcionales de responsabilidad de TI y el negocio de extremo a extremo considerando los intereses de las partes interesadas internas y externas.

Para el buen Gobierno y la Gestión de las TI empresariales, COBIT 5 se basa en 5 principios que son útiles para cualquier empresa en las diferentes líneas de negocio en las que se desarrolle. Estos 5 principios mostrados en la Figura 5, permiten a las organizaciones construir un marco de Gobierno y Gestión de TI efectivo que optimice la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

Figura 5 Principios de COBIT 5.

Fuente: Tomado de (ISACA, 2012, pág. 13).

En COBIT 5, la Gestión de TI consta de 4 dominios en relación con las áreas responsables de planificar, construir, ejecutar y supervisar, proporcionando una cobertura de extremo a extremo de las TI. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales:

- Alinear, Planificar y Organizar (APO).
- Construir, Adquirir e Implementar (BAI).
- Entregar, dar Servicio y Soporte (DSS).
- Supervisar, Evaluar y Valorar (MEA).

La Figura 6 muestra el conjunto completo de los 37 procesos de Gobierno y Gestión de TI de COBIT 5.

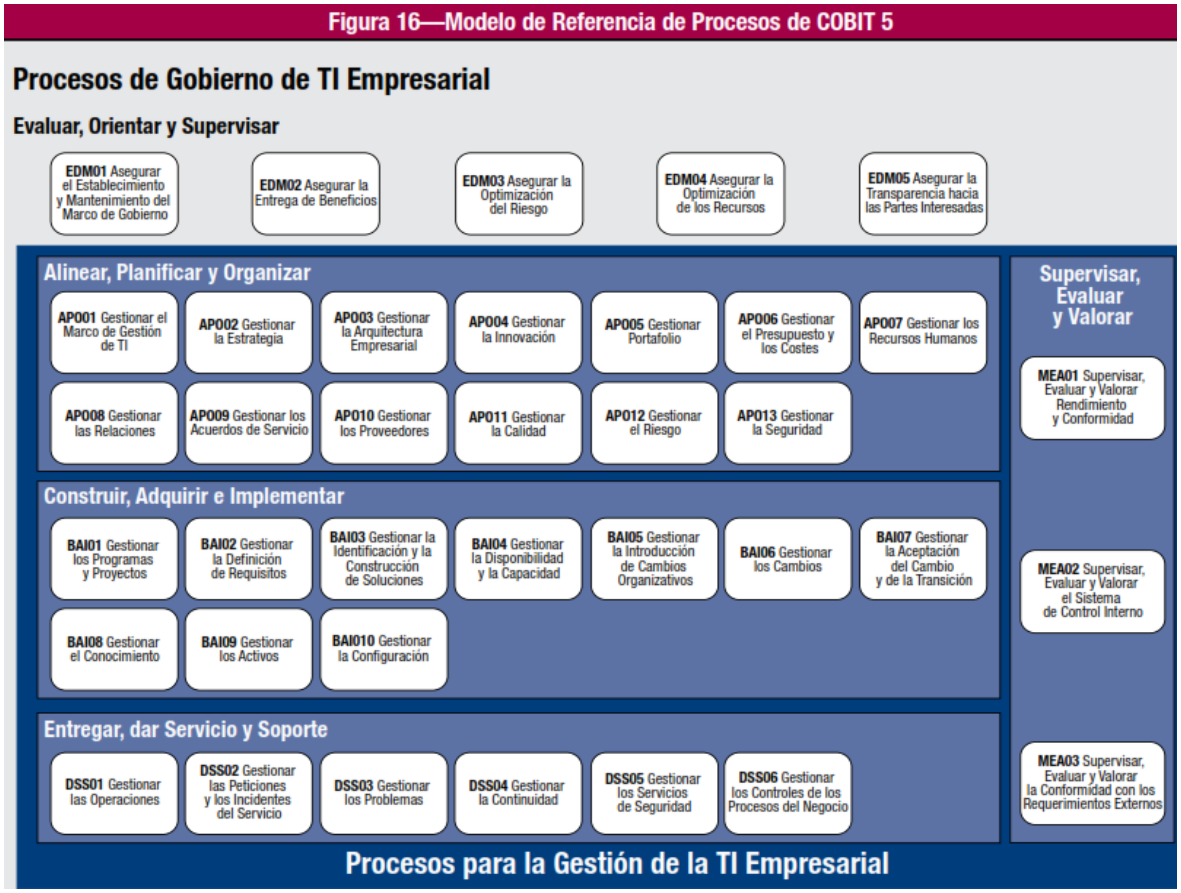


Figura 6 Modelo de referencia de procesos COBIT 5.

Fuente: Tomado de (ISACA, 2012, pág. 33).

ISACA proporciona guías de implementación de COBIT 5, que define la manera cómo aplicar las buenas prácticas de Gobierno y Gestión de TI para las organizaciones, proponiendo un modelo de referencia de 37 procesos de los cuales las empresas deberán analizar y evaluar cuales son necesarios para incrementar su competitividad y lograr eficiencia operativa. En la Figura 7 se muestra el ciclo de vida y sus siete fases:

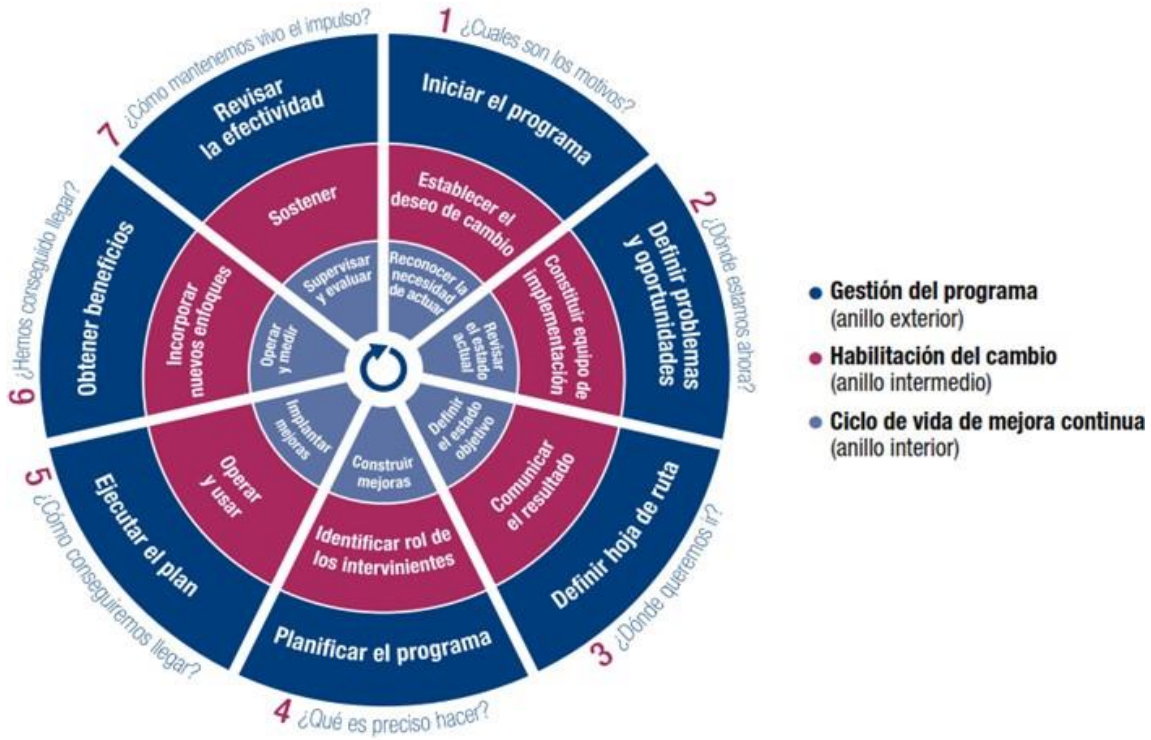


Figura 7 Las siete fases de la implementación del ciclo de vida.

Fuente: Tomado de (ISACA, 2012, pág. 37)

COBIT 5, dentro de su marco de trabajo establece la necesidad de una evaluación de la capacidad de los procesos de TI más rigurosa y confiable por lo que se apoya en la norma “ISO/IEC 15504 de Ingeniería de Software Evaluación de Procesos, este modelo alcanzará los mismos objetivos generales de evaluación de procesos y apoyo a la mejora de procesos, proporcionando un medio para medir el desempeño de los procesos de Gobierno o de Gestión de TI” (ISACA, 2012). El enfoque de COBIT 5 para medir la capacidad de los procesos se puede resumir conforme la Figura 8.

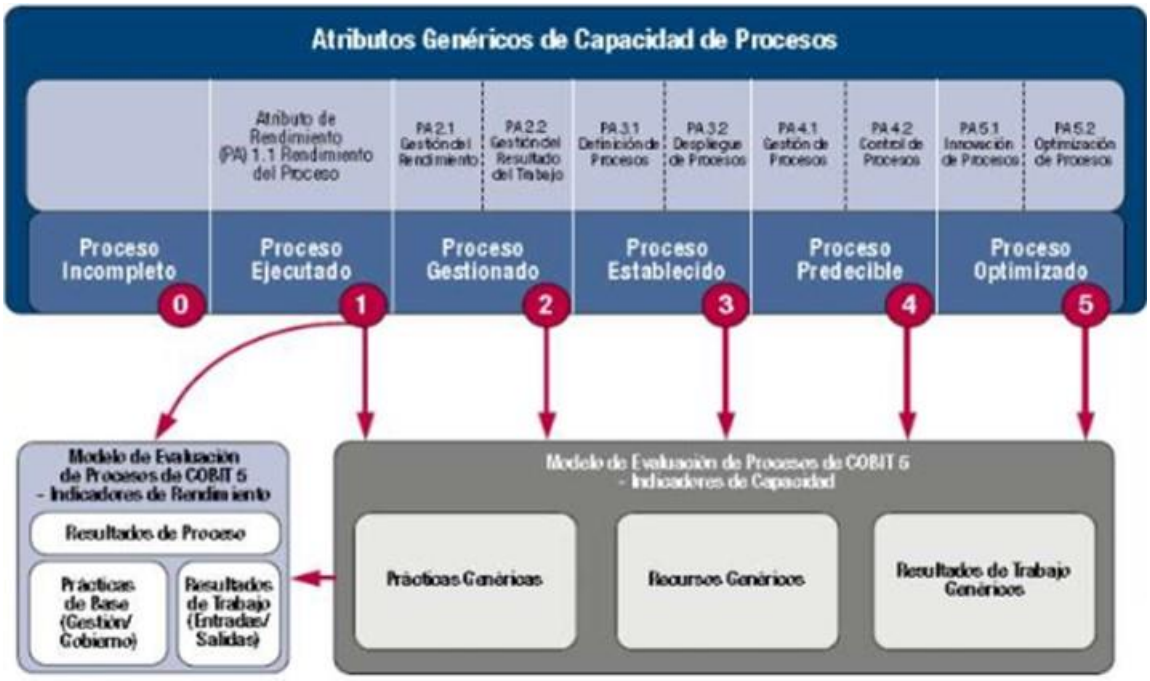


Figura 8 Modelo de Capacidad de Procesos COBIT 5.

Fuente: Tomado de (ISACA, 2012, pág. 42)

2.8 COMPARACIÓN ENTRE ISO 27000, COBIT 5 E ITIL V3

En la Tabla 9, se muestra un cuadro comparativo entre COBIT 5, ITIL V3 e ISO/IEC 27000 basado en las funciones, las áreas de cobertura, la organización, para qué se implementa y quienes los orientan (evalúan). Es de importancia mencionar que un marco de referencia, buena práctica o norma está diseñado para una función o área específica. A partir de la Tabla 9 y tomando en cuenta que el trabajo de titulación está relacionado con la seguridad de la información se considera como mejor opción la utilización de las normas de la familia ISO/IEC 27000, puesto que dicha norma posibilita además una certificación internacional para la organización.

Tabla 9. Comparación entre ISO/IEC 27000, COBIT 5 e ITIL v3

Área	COBIT 5	ITIL V3	ISO/IEC 27000
Funciones	Mapeo de procesos de TI	Mapeo de la gestión de niveles de servicio de TI	Marco de referencia de seguridad de la información
Dominios y procesos	4 Dominios y 37 Procesos	26 procesos	14 dominios, 14 cláusulas de control y 114 controles de la seguridad de la información
Creador	ISACA (Asociación de Auditoría y Control de Sistemas de Información)	OGC (Oficina de Comercio Gubernamental)	ISO (Organización Internacional de Normalización)
¿Para qué se Implementa?	Gobierno de TI / Auditoria de sistemas de Información	Gestión de niveles de servicio de TI	Implementación y gestión de un Sistema de Gestión de Seguridad de la Información
¿Quiénes lo evalúan?	Organizaciones relacionadas con la consultoría y auditoría en TI	Organizaciones relacionadas con la consultoría y auditoría en TI	Organizaciones relacionadas con la consultoría y auditoría en TI

Fuente: Adaptado de (Camelo, 2018); (ISO/IEC, 2013); (ISACA, 2012); (Van Bon & Van Der Veen, 2011)

CAPÍTULO 3: MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CLÍNICA MÉDICA FÉRTIL

3.1 DESCRIPCIÓN DE LA CLÍNICA MÉDICA FÉRTIL

3.1.1 ANTECEDENTES

En la ciudad de Ibarra, provincia de Imbabura la Clínica Médica Fértil presta sus servicios desde el año 2010 enfocándose siempre en brindar un servicio de calidad y calidez otorgando a los usuarios la mejor atención con profesionales calificados y equipando sus instalaciones con la más alta tecnología de acuerdo a las necesidades de sus usuarios.

La Clínica Médica Fértil fue creada por la Sra. Dra. Susana Navarro especialista en Otorrinolaringología junto a su esposo el Sr. Dr. Armando Pozo, quien es Ginecólogo – Obstetra y especialista en Fertilidad. Esta casa de salud mostrada en la Figura 9, cuenta con un área de emergencia y farmacia que funciona las 24 horas, de igual manera posee áreas de hospitalización, cirugía y neonatología; así como también presta servicios de diagnóstico en los cuales consta Laboratorio Clínico Hormonal, Servicio de Imagen y Apoyo Terapéutico.

Figura 9 Clínica Médica Fértil

Fuente: Tomado de (Clínica Médica Fértil, 2013)

3.1.2 MISIÓN Y VISIÓN

La Clínica Médica Fértil tiene como misión: “Brindar a la sociedad un servicio de salud de calidad, orientado siempre a la satisfacción de las necesidades de nuestros pacientes, con un completo equipo profesional y humano orientado al trabajo con responsabilidad social” (Clínica Médica Fértil, 2013).

Y como visión: “Ser sinónimo de excelencia en servicios de salud a nivel nacional, mejorando la calidad de vida de nuestros pacientes y sus familias” (Clínica Médica Fértil, 2013).

3.1.3 OBJETIVOS INSTITUCIONALES

3.1.3.1 Objetivo general

- “Brindar a la sociedad servicios de salud con calidad y calidez apuntando siempre a la mejora continua y a la satisfacción del cliente” (Clínica Médica Fértil, 2013).

3.1.3.2 Objetivos específicos

- “Asesorar a las familias con conocimientos científicos para una adecuada planificación familiar. Darse a conocer a través de la buena atención prestada a sus usuarios y su excelente equipo médico” (Clínica Médica Fértil, 2013).
- “Ampliar la infraestructura clínica para poder ofrecer mejores y más servicios médicos a la ciudadanía” (Clínica Médica Fértil, 2013).
- “Garantizar la seguridad ocupacional de todos los usuarios de la clínica tanto internos como externos fomentando un ambiente de trabajo seguro y saludable” (Clínica Médica Fértil, 2013).

3.1.4 POLÍTICA DE CALIDAD

En lo que se refiere a la calidad la Clínica Médica Fértil tiene como política, brindar servicios de salud con los más altos estándares de calidad, mediante la administración inteligente de recursos, la aplicación de normas y políticas, todo esto direccionado a brindar un servicio ágil y eficiente apuntando siempre a la mejora continua y satisfacción de los clientes.

3.1.5 MAPA DE PROCESOS

En la Figura 10 se muestra cómo se desarrollan las actividades dentro de la Clínica Médica Fértil y la forma de interactuar entre los diferentes procesos internos.

Figura 10 Mapa de Procesos

Fuente: Tomado de (Clínica Médica Fértil, 2013)

3.1.6 ORGANIGRAMA ESTRUCTURAL

A continuación, en la Figura 11 se detalla el organigrama de la Clínica Médica Fértil:

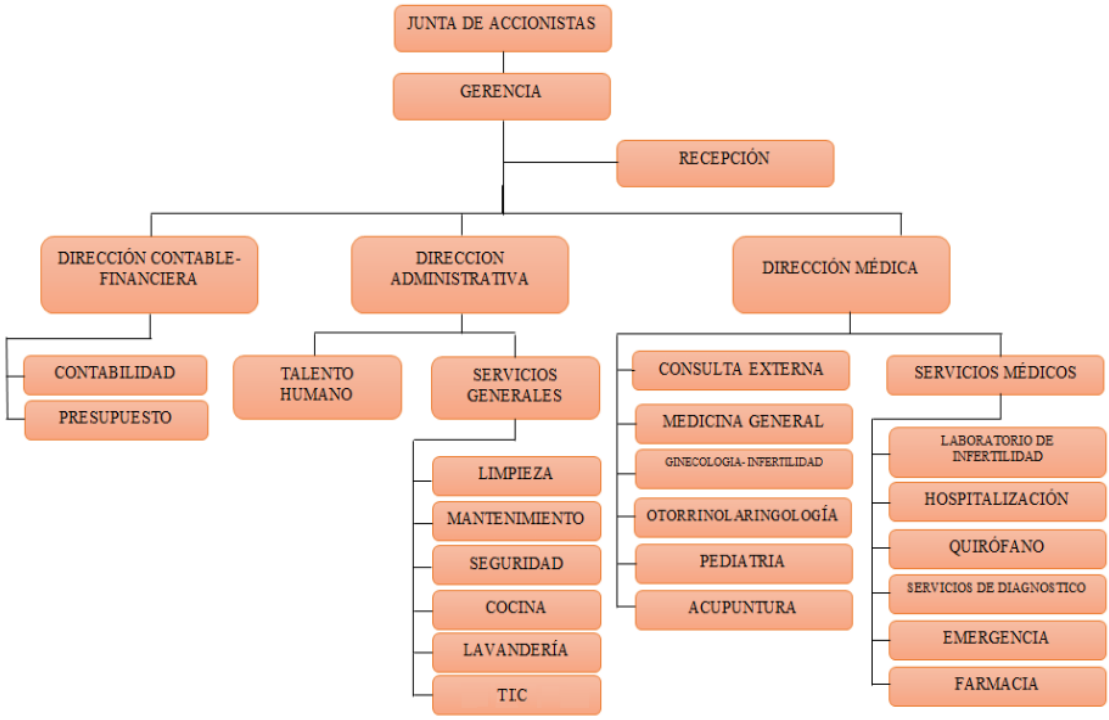


Figura 11 Organigrama estructural de la Clínica Médica Fértil

Fuente: Tomado de (Clínica Médica Fértil, 2013)

3.1.7 ESTADO DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

La Unidad de Gestión de Tecnologías de la Información y Comunicaciones (TIC) de la Clínica Médica Fértil, se encuentra conformado por 1 (uno) profesional de Tecnología de la información y 1 (uno) pasante. Dentro del organigrama vigente la unidad de TIC se encuentra como una unidad de apoyo y es considerado como un servicio general; entre las principales funciones que tiene son:

- Mantenimiento a las líneas de red.
- Acciones preventivas y correctivas de software y hardware.
- Informes sobre las acciones preventivas y correctivas de software y hardware realizados.
- Informes sobre las redes de conectividad.
- Mantenimiento de programas informáticos existentes.
- Sistemas de información en las diferentes áreas y página WEB de la clínica.
- Mantenimiento de la telefonía.
- Servicio de Internet a las diferentes unidades de la clínica.
- Inventario de los equipos tecnológicos computacionales y comunicacionales.
- Actas de la entrega recepción de los equipos adquiridos en coordinación con la Dirección Administrativa.

3.1.8 INFRAESTRUCTURA

3.1.8.1 Red de Datos

Actualmente la red de datos de la Clínica Médica Fértil es controlada por el proveedor de servicios de comunicaciones Corporación Nacional de Telecomunicaciones CNT EP, con una velocidad de 4MB. Se cuenta con un router Huawei HG532 proporcionado por el proveedor; éste router soporta estándar inalámbrico 802.11n y 4 puertos Ethernet.

En la Figura 12, se muestra el diagrama actual de la red de datos de la Clínica Médica Fértil.

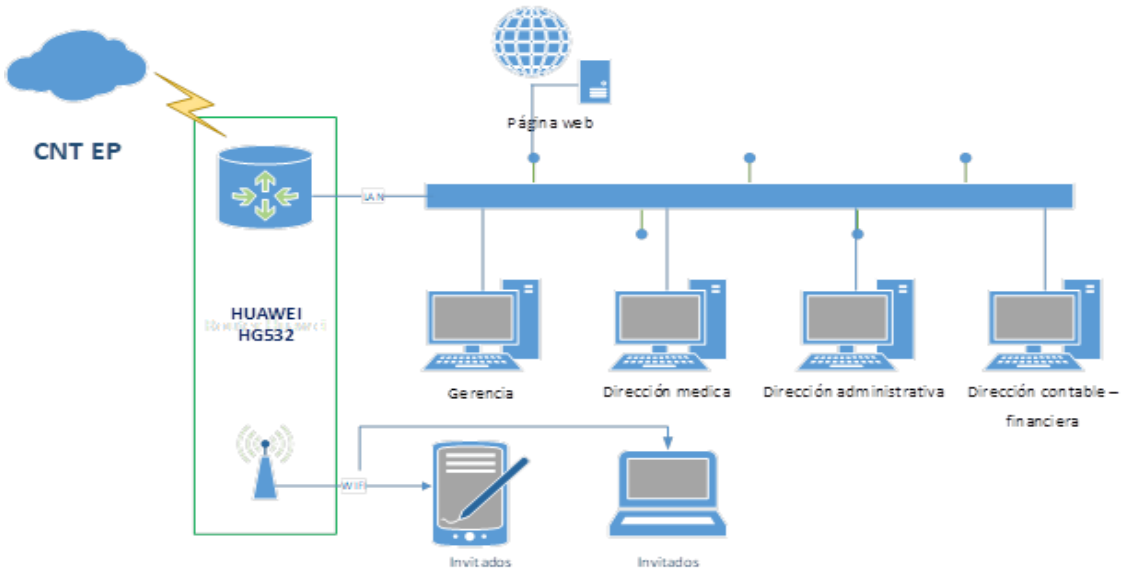


Figura 12 Red de datos de la Clínica Médica Fértil

Fuente: Elaborado por el autor

3.1.8.2 Equipos

A nivel de equipos en la Clínica Médica Fértil, se cuenta con el siguiente número de estaciones de trabajo conforme se muestra en la Tabla 10:

Tabla 10. Estaciones de trabajo

Área	Estaciones de trabajo
Gerencia	1
Dirección médica	6
Dirección administrativa	1
Dirección contable – financiera	2

Fuente: Elaborado por el autor

Además, se cuenta con dispositivos de telefonía, impresoras y servidores que se listan en la Tabla 11.

Tabla 11. Lista de equipos

Equipo	Descripción	Cantidad
Central telefónica Analógica	Panasonic kx-tes824	1
Router Inalámbrico	Huawei HG532	1
Impresora – Escáner	Samsung ML-1665; Epson EcoTank L220	3
Portátiles	HP Pavilion dm4; Lenovo G40.	4
Computadoras de escritorio	CPU HP, core i3 2,93ghz+ 750gb+ 4gb RAM+ Sistema Operativo Windows 8 (Pre Instalado).	5
Servidor de página web	Servidor HP Elite 8300, Procesador Intel Core i7-3770 (3.5 GHz) 3era Generación.	1
Servidor de Aplicaciones / Correo electrónico (Gmail)	Servidor HP Elite 8300, Procesador Intel Core i7-3770 (3.5 GHz) 3era Generación.	1
Endoscopio (torre)	Olympus Cv140	1
Ecógrafo	Hitachi Medical Systems: F37	1
Monitor de signos vitales	Storz Electronic Laparoflator 26012	1
Impresora de placas radiográficas	CARESTREAM DRYVIEW 5950	1
Datáfono	Verifone Vx510	1
Reloj Biométrico	BIOTRACK BT-BTIME	1
Teléfono analógico	Panasonic kx-t7730	1
Grabador de vídeo digital	Dvr ST-4KITAHD7016A-1M	1

Fuente: Elaborado por el autor

3.1.8.3 Aplicaciones

La Clínica Médica Fértil utiliza diferentes aplicaciones para la gestión de sus operaciones. En la Tabla 12 se listan las diferentes aplicaciones que permiten prestar los servicios médicos.

Tabla 12. Aplicaciones de la Clínica Médica Fértil

Aplicación	Tipo de aplicación	Comentarios
Paquete Office	Paquete Office Herramienta de ofimática	
Microsoft Windows	Sistema operativo	
Microsoft Windows server	Sistema operativo	servidor
Google Chrome, Firefox (Mozilla), Internet Explorer	Navegador web	
360 Total Security Essential	Programa antivirus	
SysLabs	software para laboratorios de análisis clínicos	Software del laboratorio Clínico
Latinium	software contable financiero administrativo	
Ginkgo CADx	Herramienta de análisis de datos de imagen médica (Visor DICOM)	sistema avanzado de visualización y gestión de imagen
AMIDE 3D	Herramienta de análisis de datos de imagen médica (Visor DICOM)	Herramienta de análisis de datos de imagen médica

Fuente: Elaborado por el autor

3.1.9 ANÁLISIS FODA DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Para diagnosticar el estado de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones (TIC) de la Clínica Médica Fértil se utiliza una

herramienta que permita identificar las Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) con respecto a la implementación de un SGSI, detallado en la Tabla 13. En el anexo 1 se muestra el grupo focal realizado para analizar el FODA.

Tabla 13. Análisis FODA de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones

Fortalezas	**Oportunidades**
• Apoyo de la Alta Dirección. • Posibilidad de trabajo en equipo con las diferentes áreas de la Clínica para la realización de proyectos. • Disponibilidad para auto capacitación del personal de la Unidad de TIC. • Centralización de las actividades de la Unidad de TIC, permitiendo que el soporte técnico y tiempo de respuesta sea más eficaz. • Uso correcto de los recursos informáticos por parte del personal de la Clínica	• Obtener la certificación NTE INEN - ISO/IEC 27001:2013. • Alinear la tecnología de información con el modelo del negocio de la Clínica. • Mejorar la imagen de la Clínica con los Clientes, en temas relacionados al manejo, confidencialidad y disponibilidad de la información.
Debilidades	**Amenazas**
• Procesos internos de la Clínica no posee documentación, sobre solución a incidentes relacionados con seguridad de la información. • Recursos humanos de la clínica tiene desconocimiento sobre los beneficios de implementar políticas y procedimientos de seguridad de la información. • Inexistencia de políticas y procedimientos sobre seguridad de la información para resguardar la información de la clínica. • Considerar a la Unidad de TIC como un servicio general de la clínica. • Costos elevados al aplicar los controles y herramientas de seguridad apropiados.	• Dificultad al aplicar los controles o mecanismos de seguridad apropiados por parte de los clientes. • Insatisfacción de los clientes respecto a los nuevos controles y herramientas de seguridad de la información. • La Clínica sea objeto de ataques o infiltraciones de seguridad de la información.

Fuente: Elaborado por el autor

3.2 DESCRIPCIÓN DEL MODELO

La familia de normas ISO/IEC 27000, específicamente la norma ISO/IEC 27001:2013, “describen un conjunto de requerimientos a cumplir para implementar un Sistema de Gestión de Seguridad de la Información, los cuales deben de ser implementados y documentados para poder evidenciar el cumplimiento de los mismos” (ISO/IEC, 2013, pág. 2). Estos lineamientos son identificados en un modelo, el cual se convierte en la base y estructura para la posterior implementación y gestión de un SGSI en la Clínica Médica Fértil.

Para implementar un SGSI existen diversos modelos que permiten ordenar e identificar los requerimientos que sugiere la norma ISO/IEC 27001:2013. Los modelos de Sistema de Gestión de Seguridad de la Información actuales están elaborados y estructurados para su aplicación en grandes organizaciones, debido a que éstos demandan una inversión considerable de recursos humanos, financieros y de tiempo, dado que las organizaciones de este tamaño pueden contar con los recursos necesarios para su implementación, incluso este tipo de empresas pueden darse el lujo de contratar entidades especializadas en la implementación de SGSI, denominadas consultoras, para poder guiarlas con estos tipos de proyectos.

En la elaboración del presente modelo de Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil, se debe considerar una novedad de la ISO/IEC 27001:2013 con respecto a anteriores versiones de la norma, que es la desaparición del ciclo PDCA como marco obligatorio para la gestión de mejora continua, indicando únicamente en su apartado 10.2 que “la organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información” (ISO/IEC, 2013, pág. 12). “No obstante, el ciclo PDCA está implícito en la propia estructura de la norma” (Gómez & Fernández, 2015, pág. 12), por lo cual en la Figura 13 se describe la concordancia entre la estructura de la norma ISO/IEC 27001:2013 y el modelo PDCA que servirá como base conceptual para la elaboración del presente modelo de SGSI para la Clínica Médica Fértil.

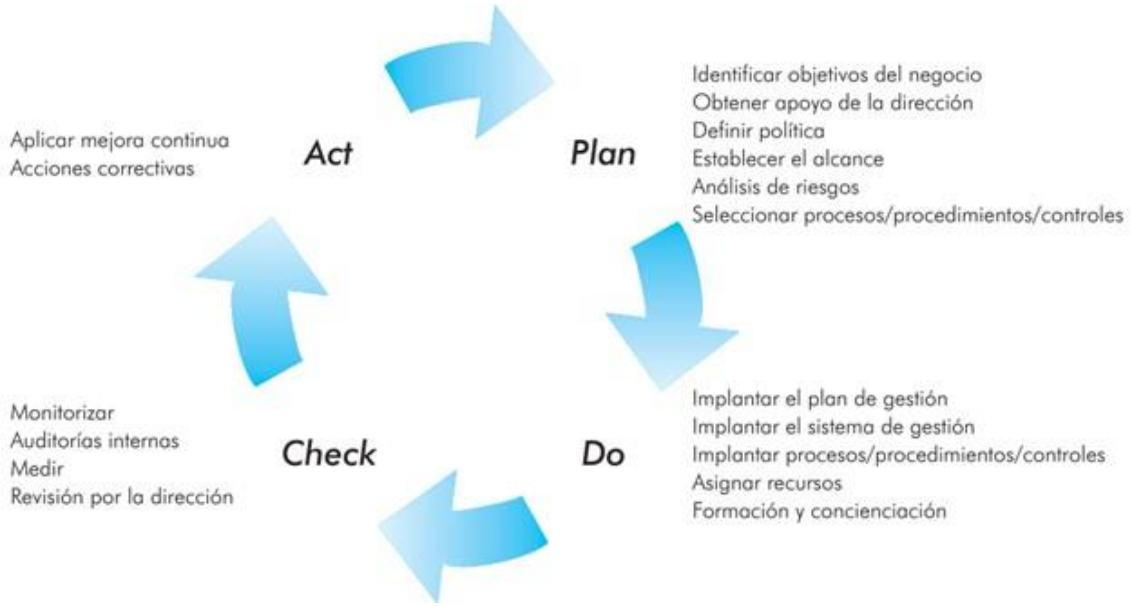


Figura 13 Concordancia entre la norma ISO/IEC 27001:2013 y el modelo PDCA

Fuente: Tomado de (Gómez & Fernández, 2015, pág. 13)

3.3 MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CLÍNICA MÉDICA FÉRTIL

El uso de las normas ISO/IEC 27001:2013, ISO/IEC 27005:2008, ISO/IEC 27002:2013 e ISO 27799:2008; permiten crear un modelo de un Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil. Dicho modelo abarca procesos y actividades dirigidas a salvaguardar la información de los pacientes de la clínica y sus trabajadores ante cualquier amenaza que se presente, preservando su confidencialidad, integridad y disponibilidad de la información.

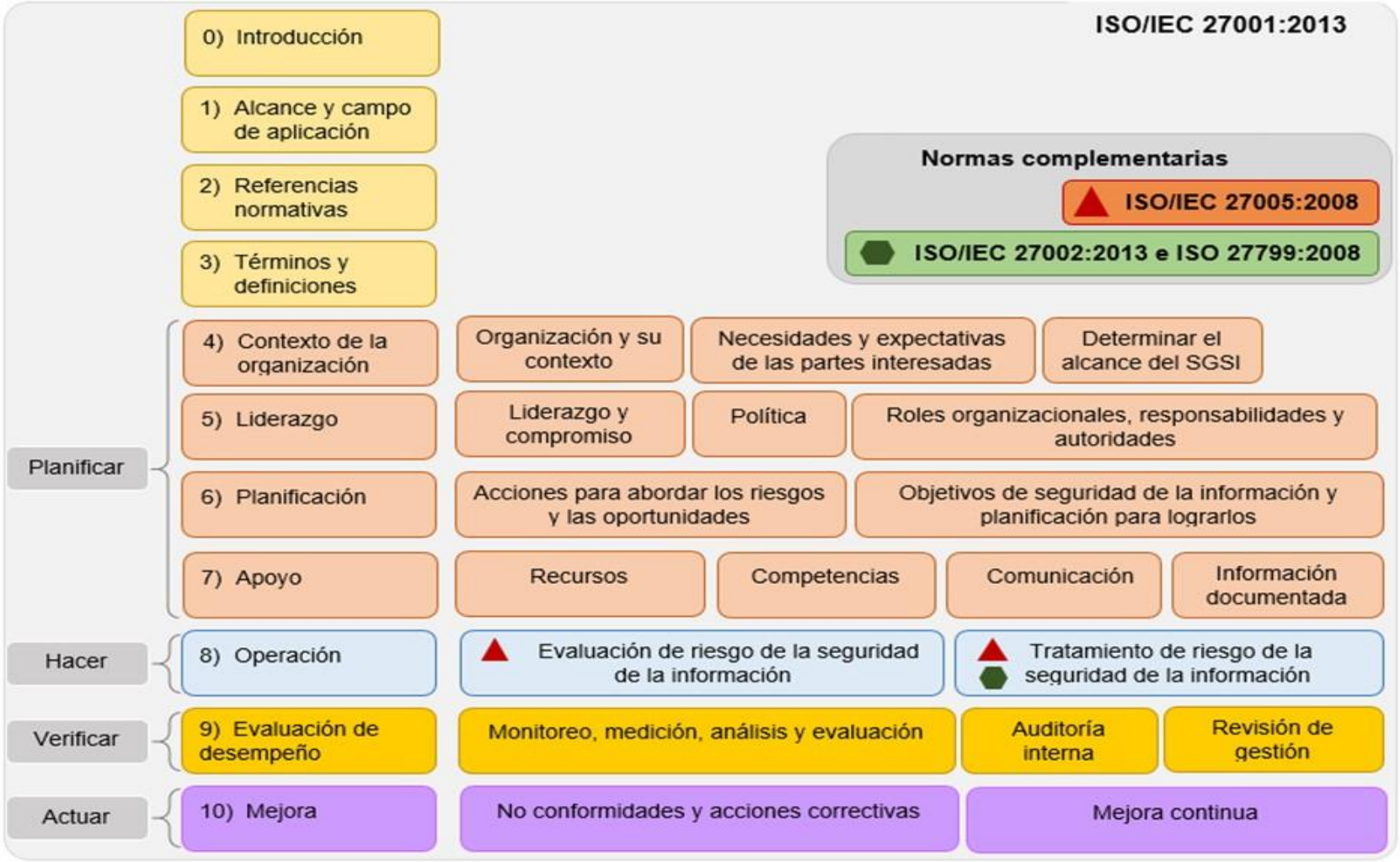


Figura 14 Modelo de un Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil

Fuente: Adaptado de (ISO/IEC, 2013); (ISO/IEC, 2008); (ISO/IEC, 2013); (ISO, 2008)

La estructura del modelo se basa en la norma ISO/IEC 27001:2013 la cual establece los requerimientos para una correcta implementación y gestión de un Sistema de Gestión de Seguridad de la Información en una organización; sin embargo para las organizaciones del sector salud que se encuentran interesados en proteger la información de los pacientes, observan que no puedan utilizar la norma ISO/IEC 27001:2013 por no ser lo suficientemente específica. Por lo cual la integración de la norma ISO 27799:2008 para la protección de la información personal del sector salud, agrega un conjunto detallado de objetivos de control y controles para la gestión de la Seguridad de la Información específica para el ámbito salud, aclarando ser un complemento para la norma ISO/IEC 27002:2013. La integración entre la norma ISO 27799:2008 e ISO/IEC 27001:2013, es similar a la norma ISO/IEC 27001:2013 e ISO 27002:2013. Así mismo, para la gestión de riesgos se acopla con la norma ISO/IEC 27005:2008 puesto que contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en un SGSI.

El modelo de un Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil en el ítem 3.2 propone al menos un documento por cada uno de los requisitos de ISO/IEC 27001:2013, “la información documentada asegura la efectividad del Sistema de Gestión de la Seguridad de la Información” (ISO/IEC, 2013, pág. 8); La ampliación de la documentación generada a partir del modelo propuesto dependerá de las necesidades particulares de la organización.

3.4 INSTRUMENTOS DE RECOLECCION DE INFORMACION

Para el desarrollo del modelo de Sistema de Gestión de Seguridad de la Información propuesto, se establece que los mecanismos e instrumentos para la recolección de la información de la Clínica Médica Fértil son:

- Grupo focal.
- Observaciones.
- Entrevistas con funcionarios y sobre todo con el personal de Tecnología de la información y comunicaciones (TIC).
- Documentación existente en el sistema de gestión calidad de la entidad.

También, se utilizará las diferentes fuentes de información, tales como normas, marcos de referencia, tesis, libros, textos, revistas, entre otros; existentes tanto en medios físicos, electrónicos y publicados en Internet.

3.5 METODOLOGÍA DE IMPLEMENTACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CLÍNICA MÉDICA FÉRTIL

La metodología de implementación del Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil se compone de las siguientes fases:

3.5.1 ESTABLECER UN LANZAMIENTO Y ANÁLISIS DEL CONTEXTO DE LA ORGANIZACIÓN

En la presente fase se realiza un análisis y descripción de la situación actual la Clínica Médica Fértil, tratando de comprender su perspectiva, procesos internos, dependencias, requisitos internos y externos y las motivaciones para la implantación de un SGSI.

Para conocer la situación actual respecto a la seguridad de la información de la Clínica Médica Fértil, se evalúa el nivel de cumplimiento de cada uno de los controles de la norma ISO/IEC 27001:2013 en su anexo A o su equivalente y con mayor grado de detalle la norma ISO/IEC 27002:2013. Para la estimación del riesgo se deberá establecer “una metodología de estimación que puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias” (ISO/IEC, 2008, pág. 14). La ponderación utilizada para la evaluación se describe en la Tabla 14.

Tabla 14. Ponderación para el nivel de cumplimiento de los dominios de la norma ISO/IEC 27002:2013

Sigla	Estado de Evaluación	Descripción
NC	No cumple	No existe y/o no se está haciendo
CP	Cumple parcialmente	Lo que la norma requiere (ISO/IEC 27002 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona.
CS	Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO/IEC 27002 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI cumple 100%

Fuente: Elaborado por el autor

3.5.2 DETERMINAR EL ALCANCE DEL SGSI

Se determinará qué elementos formarán parte del Sistema de Gestión de Seguridad de la Información, generalmente identificando los procesos de negocio sobre los que se aplicará el sistema; para determinar el alcance del SGSI la Clínica Médica Fértil debe considerar:

- “Los asuntos externos e internos de la organización que son importantes para su objetivo y que afecte su capacidad para lograr los resultados esperados de su Sistema de Gestión de la Seguridad de la Información” (ISO/IEC, 2013, pág. 3).
- "Comprender las necesidades y expectativas de las partes interesadas, tomando en consideración que los requisitos de las partes interesadas pueden incluir requerimientos legales y regulatorios, así como obligaciones contractuales” (ISO/IEC, 2013, pág. 3).
- Interferencias y dependencias entre las actividades realizadas por la organización del sector salud y aquellas realizadas por otras organizaciones adyacentes o proveedores.

“El alcance estará disponible como información documentada” (ISO/IEC, 2013, pág. 3), por lo cual debe existir un documento que servirá como evidencia donde se especificará el alcance del Sistema de Gestión de Seguridad de la Información y que contenga la aprobación y respaldo de Gerencia de la Clínica Médica Fértil.

3.5.3 REALIZAR LA DEFINICIÓN DE LA POLÍTICA Y OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La definición de los objetivos y políticas para el proceso de implementación del Sistema de Gestión de Seguridad de la Información permitirá establecer un sentido de dirección general para la Clínica Médica Fértil. A través de esta fase se logrará establecer los objetivos de la clínica en el ámbito de la seguridad de la información y los mecanismos para alcanzar dichos objetivos.

Al definir la política del Sistema de Gestión de Seguridad de la Información, se deberían tomar en cuenta los siguientes aspectos:

- “Establecer los objetivos del SGSI en base a los requerimientos organizacionales y las prioridades de seguridad de la información de la organización” (ISO/IEC, 2013, pág. 4).
- “Establecer el enfoque general y la guía de acción para lograr los objetivos del SGSI” (ISO/IEC, 2013, pág. 4).
- Considerar los requerimientos de la Clínica, legales o regulatorios y las obligaciones contractuales relacionadas con la seguridad de la información.
- Establecer el contexto de la gestión del riesgo dentro de la Clínica.
- “Determinar los criterios de evaluación de los riesgos y definir una estructura de evaluación del riesgo” (ISO/IEC, 2013, pág. 4).
- Obtener la aprobación de la Gerencia de la clínica.

El entregable de la presente fase es un documento que describe los objetivos y política del Sistema de Gestión de Seguridad de la Información y de igual manera aprobada por la Gerencia de la Clínica Médica Fértil.

3.5.4 DEFINIR LOS RECURSOS, COMPETENCIAS, COMUNICACIÓN E INFORMACIÓN DOCUMENTADA

La Clínica Médica Fértil deberá determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información. De igual manera, deberá establecer procesos internos para la elección de personal médico y administrativo que permita “asegurar que estas personas sean competentes basados en una educación, capacitación o experiencia adecuada” (ISO/IEC, 2013, pág. 11).

Los Responsables de la implementación, deberán definir los procedimientos de comunicación interna y externa pertinentes al Sistema de Gestión de Seguridad de la Información; así como también la creación, actualización y control de la información documentada.

3.5.5 ESTABLECER ACCIONES PARA ABORDAR LOS RIESGOS Y LAS OPORTUNIDADES

En la presente fase se debe determinar los riesgos y oportunidades que necesitan ser cubiertos para asegurar que el Sistema de Gestión de la Seguridad de la Información pueda lograr el resultado esperado. Para lo cual se debe realizar actividades que tienen relación con “la evaluación y el tratamiento del riesgo de la seguridad de la información” (ISO/IEC, 2013, pág. 5).

En lo que se refiere a la evaluación del riesgo, la norma ISO/IEC 27001:2013 establece que la “organización debe definir y aplicar un proceso de evaluación de riesgo de la seguridad de la información” (ISO/IEC, 2013, pág. 5) que establezca y mantenga los criterios de riesgo de la seguridad de la información, así como también asegurar que las evaluaciones de riesgo de la seguridad de la información, producen resultados consistentes, válidos y comparables, una y otra vez; “el entregable de esta fase es la información documentada acerca del proceso de

evaluación de riesgo de la seguridad de la información" (ISO/IEC, 2013, pág. 5). Dicha documentación deberá contener las siguientes actividades:

3.5.5.1 Desarrollar el inventario de activos de información

Se deben identificar los activos que dan soporte a los procesos de negocio de la Clínica Médica Fértil en el alcance del Sistema de Gestión de la Seguridad de la Información y cuantificar su valor en términos de confidencialidad, integridad y disponibilidad. "Tomando en consideración que se define como activo todo aquello que tiene valor para la organización y que por lo tanto debe ser protegido" (ISO/IEC, 2008, pág. 10).

La identificación de los activos se debería llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo; De igual manera se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. "El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda" (ISO/IEC, 2008, pág. 10). El entregable de esta actividad es un documento con el inventario de los activos de información de los principales procesos de la organización dentro del alcance del Sistema de Gestión de la Seguridad de la Información.

Para la identificación de los activos, se debe tomar en cuenta los tipos de activos que existen en la Clínica Médica Fértil tanto los activos primarios y de soporte. A continuación, se muestra una clasificación de los mismos.

- Los activos primarios:
    - Servicios médicos y procesos del negocio
    - Información / Datos
- Los activos de soporte (de los cuales dependen los elementos primarios del alcance) de todos los tipos:
    - Hardware

- Software
- Redes de comunicaciones
- Personas
- Sitio / Instalaciones
- Estructura de la organización.

3.5.5.2 Realizar una valoración de los activos

La valoración de los activos sirve para determinar el impacto que el deterioro, falla o pérdida de los mismos tiene sobre la confidencialidad, disponibilidad e integridad de la información de la Clínica Médica Fértil. Para ello se deberá aplicar una escala de valor a los activos y de esa manera poder relacionarlos apropiadamente; “El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización” (ISO/IEC, 2008, pág. 10).

La valoración de activos es un factor clave en la evaluación del impacto de un escenario de incidente y considerando que el incidente puede afectar a más de un activo (por ejemplo, activos independientes) o únicamente una parte de un activo; dependiendo del grado de impacto en caso de pérdida, falla, o deterioro del activo, se asignara un valor de 1 al 3, siendo 1 el de menor impacto y 3 el de mayor impacto. El rango de valorización que debe poseer el activo para ser considerado dentro del análisis de riesgo dependerá de las personas interesadas en el Sistema de Gestión de Seguridad de la Información y de la Gerencia de la Clínica.

En la Tabla 15 se describen los requisitos de confidencialidad, integridad y disponibilidad que se debe asignar a cada uno de los activos de la Clínica Médica Fértil en relación con su nivel de impacto: Alto (3), Medio (2) y Bajo (1), siendo la valoración total del activo la suma de los tres valores.

Tabla 15. Requisitos de Confidencialidad, Integridad y Disponibilidad por Activo

Requisito	Nivel de valoración		
	Bajo = 1	Medio = 2	Alto = 3
Confidencialidad	La información es de carácter público y no se tiene ningún impacto sobre el resultado del proceso en caso de ser accedido por personas no autorizadas.	La información es de uso interno exclusivamente o uso restringido solamente y de ser accedida por personas no autorizadas no afectaría en mayor grado el resultado o pondría en riesgo la empresa.	La información es de carácter Secreto y en caso de ser accedida por personas no autorizadas, el impacto final sobre el proceso o resultado de la empresa sería muy grave.
Integridad	El daño o modificación no autorizada no es crítico para las aplicaciones empresariales y el impacto en la empresa es insignificante o menor.	El daño o modificación no autorizada no es crítico, pero si es notorio para las aplicaciones empresariales y el impacto en la empresa es significativo.	El daño o modificación no autorizada es crítica para la organización y el impacto es importante y podría conllevar la falta grave o total de la aplicación o sistema empresarial.
Disponibilidad	Se puedes tolerar que el activo no esté disponible por más de un día	Se puede tolerar que el activo no esté disponible por máximo de medio día a un día.	No se puede tolerar que el activo no esté disponible por más de unas cuantas horas, o incluso menos.

Fuente: Elaborado por el Autor

3.5.5.3 Identificar amenazas

En esta etapa se deben identificar las amenazas asociadas a cada uno de los procesos de negocio de la Clínica Médica Fértil, activos de información, probabilidad de ocurrencia y vulnerabilidades ante dichas amenazas, lo que permitirá estimar el impacto de la materialización de cualquier falla de seguridad de la información dentro de la clínica.

Las amenazas suelen ser causas potenciales de incidentes que ocasionan daños en los activos de información; Las amenazas pueden clasificarse como:

- D (deliberadas): “Son todas las acciones deliberadas que tienen como objetivo los activos de la información” (ISO/IEC, 2008, pág. 39).
- A (accidentales): “Se utiliza para las acciones humanas que pueden dañar accidentalmente los activos de información” (ISO/IEC, 2008, pág. 39).
- E (ambientales): “Se utiliza para todos los incidentes que no se basa en las acciones humanas” (ISO/IEC, 2008, pág. 39).

En la Tabla 16, se describe los diferentes tipos y ejemplos de amenazas comunes aplicables al modelo de Sistema de Gestión de Seguridad de la Información, así como también su código para identificarlas posteriormente.

Tabla 16. Tipos y ejemplo de amenazas comunes

Tipo	Amenazas	Código
Daño físico	Fuego, daño por agua, Contaminación, accidente importante, destrucción del equipo o los medios, polvo, corrosión, congelamiento, etc.	A1
Eventos naturales	Fenómenos climáticos, fenómenos sísmicos, fenómenos volcánicos, fenómenos meteorológicos, inundación, etc.	A2
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado, pérdida de suministro de energía, falla en el equipo de telecomunicaciones, etc.	A3
Perturbación debida a la radiación	Radiación electromagnética, radiación térmica, Impulsos electromagnéticos, etc.	A4
Compromiso de la información	Interceptación de señales de interferencia comprometedoras, espionaje remoto, escucha subrepticia, hurto de medios o documentos, hurto de equipo, recuperación de medios reciclados o desechados, divulgación, datos provenientes de fuentes no confiables, manipulación con hardware, manipulación con software, detección de la posición, etc.	A5
Fallas técnicas	Falla del equipo, mal funcionamiento del equipo, saturación del sistema de información, mal funcionamiento del software, Incumplimiento en el mantenimiento del sistema de información, etc.	A6
Acciones no autorizadas	Uso no autorizado del equipo, copia fraudulenta del software, uso de software falso o copiado, corrupción de los datos, procesamiento ilegal de los datos, etc.	A7

Tipo		Amenazas	Código
Compromiso de las funciones		Error en el uso, abuso de derechos, falsificación de derechos, negación de acciones, incumplimiento en la disponibilidad del personal, etc.	A8
Fallas Humanas intencionales A9	Pirata informático, intruso ilegal	Piratería, ingeniería social, intrusión, accesos forzados al sistema, acceso no autorizado al sistema	A9.1
	Criminal de la computación	Crimen por computador (por ejemplo, espionaje cibernético), acto fraudulento (por ejemplo, repetición, personificación, interceptación), soborno de la información, suplantación de identidad, intrusión en el sistema.	A9.2
	Terrorismo	Bomba / terrorismo, guerra* (warfare) de información, ataques contra el sistema (por ejemplo, negación distribuida del servicio), penetración en el sistema, manipulación del sistema, etc.	A9.3
	Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros)	Ventaja de defensa, ventaja política, explotación económica, hurto de información, intrusión en la privacidad personal, ingeniería social, penetración en el sistema, acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)	A9.4
	Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Asalto a un empleado, chantaje, observar información de propietario, abuso del uso del computador, soborno de información, ingreso de datos falsos o corruptos, código malintencionado (por ejemplo, virus, bomba lógica, caballo troyano), etc.	A9.5

Fuente: Adaptado de (ISO/IEC, 2008, pág. 49)

Un mayor detalle sobre la relación entre el origen y los tipos de amenazas se puede encontrar en el anexo 2. Dentro del proceso de valorización del riesgo, la norma ISO/IEC 27005:2008 indica que “la estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias de análisis” (ISO/IEC, 2008, pág. 14).

3.5.5.4 Efectuar una valorización de amenazas

En la presente etapa se debe realizar una ponderación del impacto en caso de materializarse la amenaza. Así mismo, el rango de valorización que debe poseer la amenaza para ser considerado dentro del análisis de riesgo dependerá del responsable de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones y la Gerencia de la Clínica. En la Tabla 17 se describe la ponderación a utilizar para las amenazas.

Tabla 17. Ponderación del impacto en caso de materializarse la amenaza

Ponderación	Calificación
Alto	3
Medio	2
Bajo	1

Fuente: Elaborado por el Autor

Dentro de la metodología propuesta, se debe considerar que al utilizar catálogos de amenazas o los resultados de valoraciones anteriores de las amenazas en la organización del sector salud, “es conveniente ser consciente de que existe un cambio continuo de las amenazas importantes, en especial si cambia el ambiente del negocio o los sistemas de información” (ISO/IEC, 2008, pág. 11).

3.5.5.5 Realizar una identificación de los controles existentes

Posterior al proceso de identificar y valorizar las amenazas, se debe realizar la identificación de los controles existentes en la organización que permitan brindar

de alguna manera confidencialidad, integridad y disponibilidad a la información para evitar trabajo o costos innecesarios en la implementación de un Sistema de Gestión de Seguridad de la Información, por ejemplo, en la duplicación de los controles.

Para la identificación de los controles existentes o planificados, las siguientes actividades pueden ser útiles:

- Revisión de los documentos que contengan información sobre los controles.
- Verificación con las personas responsables de la seguridad de la información.
- Efectuar una revisión en el sitio de los controles existentes.
- Revisión de los resultados de las auditorías internas.

3.5.5.6 Efectuar una identificación de las vulnerabilidades

Se procede a identificar las vulnerabilidades del activo por las distintas fuentes que las pueden originar, utilizando como guía algunos de los dominios de la norma ISO 27002:2013 y una lista de vulnerabilidades proporcionadas por la Norma ISO/IEC 27005:2008 que se detalla en el anexo 3.

“La vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso consistencia del sistema y/o de sus datos o aplicaciones” (ISO/IEC, 2008, pág. 12). Se puede decir que la vulnerabilidad en sí mismo no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza se concrete afectando o dañando los sistemas e información. El resultado de esta etapa es un documento con una lista de las vulnerabilidades con relación a los activos, las amenazas y los controles existentes.

3.5.5.7 Realizar una evaluación de la probabilidad de incidentes

Después de identificar y valorizar las amenazas e incidentes es necesario evaluar la probabilidad de cada escenario y el impacto de que ocurra. Se deberán

tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas.

La valoración cuantitativa del 1 al 3 que se muestra en la Tabla 18, permitirá indicar que tan probable es que una amenaza se concrete con una o varias de las vulnerabilidades encontradas.

Tabla 18. Probabilidad de que la amenaza explote la vulnerabilidad

Ponderación	Calificación
Alto	3
Medio	2
Bajo	1

Fuente: Elaborado por el Autor

3.5.5.8 Establecer un nivel de estimación del riesgo

Para cada activo de información de la Clínica Médica Fértil se calcula el riesgo, “que será una combinación de la probabilidad de un escenario de incidente y sus consecuencias” (ISO/IEC, 2008, pág. 15). El proceso de estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. Estos valores pueden ser cuantitativos o cualitativos. La estimación del riesgo se basa en las consecuencias evaluadas y la probabilidad. Además, en el proceso de estimación del riesgo se puede considerar el beneficio de los costos, los intereses de las partes involucradas y otras variables.

La calificación del riesgo se realizará haciendo una multiplicación entre la probabilidad del incidente tratado en el ítem 3.5.5.7 y el impacto en caso de materializarse la amenaza del ítem 3.5.5.4, a continuación, en la Tabla 19 se muestra el nivel de estimación de riesgo a utilizar dentro de la metodología.

Tabla 19. Nivel de estimación del riesgo

Estimación del riesgo	Rango
Alto	6,1 - 9
Medio	3,1 - 6
Bajo	0 - 3

Fuente: Elaborado por el Autor

3.5.6 REALIZAR EL TRATAMIENTO DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Luego de completar la evaluación de riesgos, la Clínica Médica Fértil “deberá definir y aplicar un proceso de tratamiento de riesgo de la seguridad de la información”. Dentro de las estrategias de llevar el tratamiento del riesgo están:

- **Eliminación o evitación:** Consiste en eliminar la amenaza eliminando la causa que puede provocarla.
- **Transferencia:** Esta posibilidad busca trasladar las consecuencias de un riesgo a una tercera parte junto con la responsabilidad de la respuesta.
- **Mitigación:** Busca reducir la probabilidad o las consecuencias de sucesos adversos a un límite aceptable antes del momento de activación. Es importante que los costos de mitigación sean inferiores a la probabilidad del riesgo y sus consecuencias. Para llevar a cabo la mitigación de riesgos es necesario: seleccionar, implantar, y verificar los controles y establecer indicadores. La selección de los controles se podrá realizar utilizando como referencia la Norma ISO/IEC 27002:2013
- **Aceptación:** Se utiliza cuando se decide no actuar contra el riesgo antes de su activación. La aceptación puede ser activa, cuando se incluye un plan de contingencia que será ejecutado si el riesgo se presenta, o pasiva, cuando no requiere de ninguna acción, únicamente se realiza la gestión del riesgo.

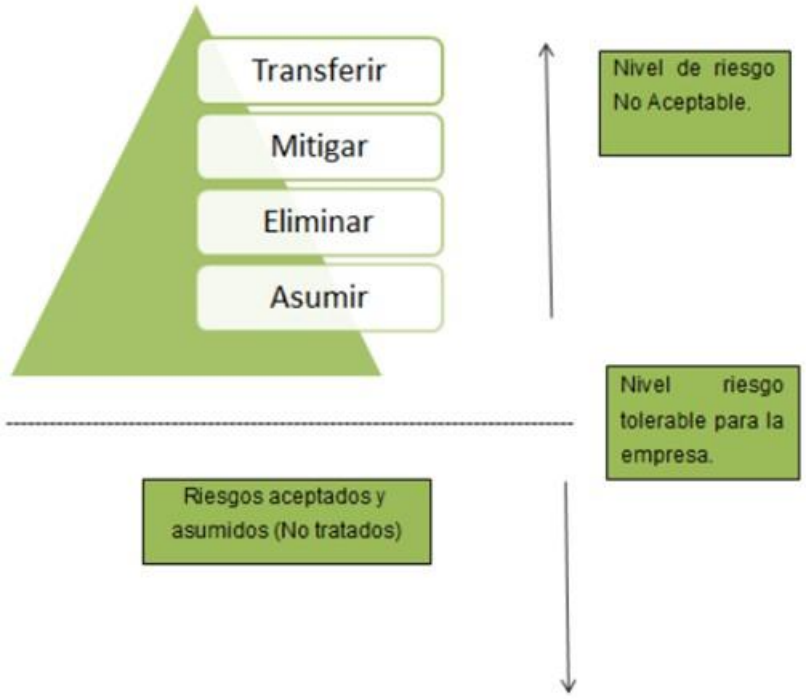


Figura 1. Tratamiento del riesgo en el SGSI

Fuente: Adaptado de (ISO 27000.ES, 2005)

Para el tratamiento del riesgo se debe “determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de la información escogida” (ISO/IEC, 2013, pág. 6). Los controles seleccionados permitirán garantizar que cada aspecto del activo, que se valoró con cierto riesgo, quede cubierto y auditable. Estos controles se toman de la ISO/IEC 27002:2013; sin embargo, la norma ISO/IEC 27001:2013 aclara que “los controles propuestos no son exclusivos y podrían adoptarse otros tipos de controles” (ISO/IEC, 2013, pág. 6). En este punto en la metodología propuesta se recomienda también el uso de los controles de la norma ISO 27799:2008 puesto que “establece un conjunto de controles detallados para la gestión de la Seguridad de la Información de salud y proporciona directrices de buenas prácticas de Seguridad de la Información de salud” (ISO, 2008, pág. 1). Para la implementación de las políticas de seguridad de la información, se tendrá como referencia el mapeo realizado entre las normas ISO 27799:2008 e ISO/IEC 27002:2013 que consta en el anexo 4.

Posterior a determinar los controles a aplicar, se planteará la realización de algunos proyectos que involucre las políticas y herramientas para el proceso de implementación del Sistema de Gestión de Seguridad de la Información en la clínica.

Además, se debe considerar que en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información, siempre existen riesgos residuales, los cuales deben ser evaluados y categorizados como aceptables o no-aceptables. La aceptación de dichos riesgos residuales debe estar realizado por un comité de seguridad de la información el cual decidirá que controles deben ser implementados en el futuro. El resultado de esta fase es el documento denominado declaración de aplicabilidad el cual detallará los proyectos propuestos a implementar, dicho documento debe tener la aceptación de la Gerencia de la Clínica y el encargado de la Unidad de Tecnologías de la Información.

El objetivo del Plan de tratamiento del riesgo es definir cuál es la estrategia de tratamiento de riesgo, selección de controles, herramientas, información documentada, responsable de implementar los controles, lo que permitirá garantizar:

- Un funcionamiento efectivo y eficiente de la organización del sector salud.
- Controles internos efectivos.
- Conformidad con las leyes y reglamentos vigentes.

3.5.7 IMPLEMENTAR LOS PROYECTOS PROPUESTOS

De una manera planificada y organizada se deberán implementar los proyectos propuestos. Puede ser conveniente comenzar la implantación por aquellas acciones, controles y herramientas que con un menor esfuerzo aporte un gran valor a la organización.

3.5.8 FORMAR Y CONCIENCIAR AL PERSONAL

Para que la implantación de los procedimientos sea efectiva, es necesario concienciar y formar a todas las personas implicadas. La formación y capacitación de cada usuario deberá ser acorde con las funciones que desempeñe dentro de la clínica y su rol en la implementación del Sistema de Gestión de Seguridad de la Información. Todo el personal implicado en el SGSI debe ser concienciado en la importancia de su labor para salvaguardar la información y formado en cómo desarrollar su trabajo aplicando las normas y procedimientos de seguridad de la información definidos.

3.5.9 REALIZAR UNA AUDITORÍA INTERNA Y REVISIÓN DEL SGSI

Esto permitirá comprobar el grado de ajuste del Sistema de Gestión de Seguridad de la Información a los requisitos de la norma y determinar si está alineado con los objetivos de la Clínica Médica Fértil. En términos generales, con la auditoría interna se pretende:

- Comprobar que el SGSI definido se ajusta a los requisitos de la norma.
- Comprobar que la actividad de la organización se lleva de acuerdo a lo especificado en el SGSI.

El equipo auditor seleccionado debe garantizar la independencia sobre las actividades a auditar y disponer de la experiencia y formación necesarias para este tipo de auditorías.

En al Figura 16, se muestra un resumen de la metodología de implementación del modelo de Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil.

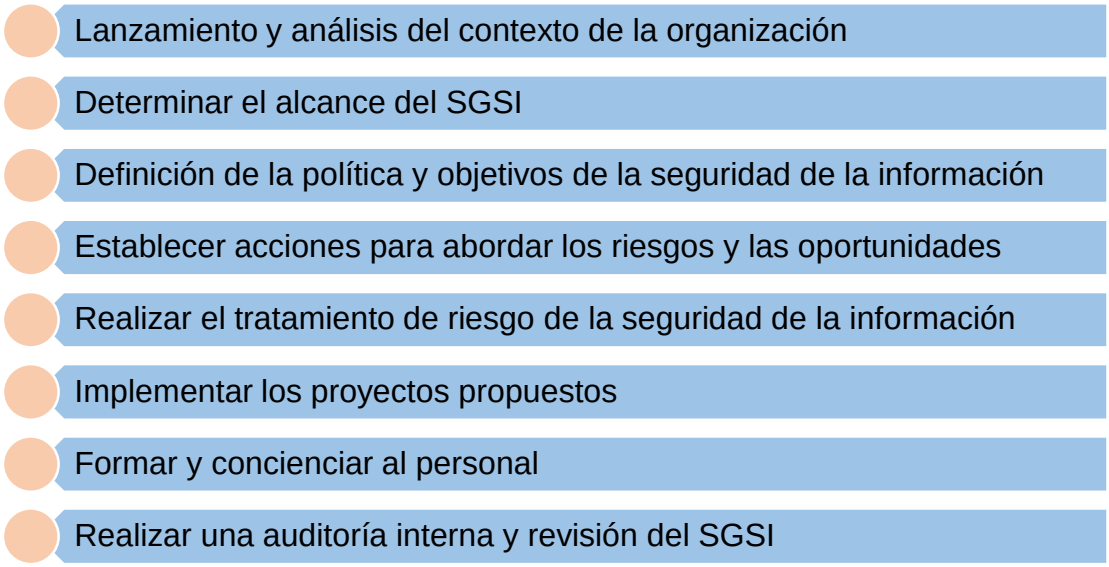


Figura 15 Metodología de implementación del modelo de SGSI para la Clínica Médica Fértil

Fuente: Elaborado por el autor

3.6 ANÁLISIS DE COSTO FRENTE A BENEFICIOS SOBRE LA IMPLEMENTACIÓN DE UN SGSI EN INSTITUCIONES DEL SECTOR SALUD

Actualmente, el uso de las tecnologías de la información en el sector salud ha propiciado un mejoramiento en el proceso médico asistencial; sin embargo, también ha ocasionado una gran cantidad de incidentes derivados de deficiencias en la seguridad de las instalaciones del sector salud, o a causa de errores o descuidos del personal en la manipulación de los datos de pacientes. Los beneficios de implementar un SGSI depende del nivel de madures de la organización y del compromiso de las partes interesadas que auspician y desarrollan el proyecto. Por lo cual, para analizar los beneficios y costos de implementar un Sistema de Gestión de Seguridad de la Información en instituciones del sector salud, se hará referencia a las consecuencias en base a estudios y estadísticas de no tener implementadas políticas y controles que permitan mitigar los riesgos de amenazas y vulnerabilidades de seguridad de la información.

En el Ecuador no existe un estudio específico sobre ataques o infiltraciones de seguridad de la información en hospitales o centros de salud. Sin embargo

conforme un reporte del estado de la ciberseguridad en las organizaciones de salud en 2016, elaborado por ESET y el *instituto Ponemon,* afirma que un “77% de las organizaciones del sector salud sufre ciberataques, con un promedio anual de 11,4 ataques a su seguridad informática” (ESET Smart Security, 2016). Del estudio mencionado podemos indicar que los ‘hackers’ tienen mayor interés en los historiales médicos, los datos de pago y las pruebas clínicas e investigaciones médicas de las instituciones.

La información sobre salud de un paciente es tanto personal como crítica y debido a su importancia los datos de salud digital se han convertido en uno de los productos más codiciados para los piratas informáticos que operan en el mercado negro. “Mientras en el mercado negro la información de una tarjeta de crédito puede costar entre USD 5 y 15, un historial médico sobrepasa los USD 50” (El comercio, 2017). La razón de este precio es sencilla: una tarjeta solo permite el acceso a un canal de información; mientras que, un registro de un paciente incluye todos los datos personales del mismo (dirección domiciliaria, récord financiero, enfermedades, etc.).

La industria del sector salud es especialmente vulnerable a ataques porque carece de las protecciones incorporadas y de la concienciación sobre seguridad de la información, que sí tienen otros sectores como el financiero o telecomunicaciones. Los ataques a sistemas informáticos de salud se despliegan como ataques dirigidos, websites comprometidas, spam, dispositivos móviles infectados que exponen datos confidenciales además de provocar distracciones y problemas los responsables de TI. A continuación se detalla los casos más representativos de perdida de información en hospitales de Estados Unidos y Europa a consideración de (Healthcare IT News, 2017), (HIPAA Journal, 2018) y (HealthITSecurity, 2017) .

- **Organización:** Indiana Hospital

  El 11 de enero del 2018, se informó sobre el ataque de ransomware en el hospital de Indiana. El hospital pagó un rescate de 55000 Dólares Americanos para deshacerse del ransomware que había infectado sus sistemas y estaba

obstaculizando las operaciones; Durante el ataque en el hospital de Indiana, los piratas informáticos lograron codificar más de 1400 archivos y los marcaron con la frase "*Lo Siento"*. El CEO del Indiana Hospital, indico que "restaurar la información a través de las copias de seguridad habría tomado días o incluso semanas. Por lo cual se decidió pagar el rescate para recuperar el acceso a los datos de sus pacientes" (Tripwire, 2018).

- **Organización:** VisionQuest Eyecare
  VisionQuest Eyecare, con sede en Indiana descubrió un ciberataque en su red el 22 de enero de 2017, un incidente que, según los informes, afectó a 85.995 personas. La información potencialmente comprometida incluía nombres de pacientes, direcciones, números de teléfono, fechas de nacimiento, números de Seguro Social, información de seguros de salud o visión, datos de reclamaciones médicas e información clínica.

- **Organzacion:** Harrisburg Gastroenterology Ltd
  El acceso no autorizado a la información del paciente puede haber ocurrido en Harrisburg Gastroenterology Ltd, en el Centro de Endoscopia y Cirugía de Harrisburg, dijo la organización en una carta de notificación enviada a principios del año 2017. Harrisburg Gastroenterology Ltd informó a OCR (Oficina de Derechos Civiles) que 93.323 personas pueden haber resultado afectadas, mientras que el Centro de Endoscopia y Cirugía de Harrisburg tuvo 9.092 pacientes posiblemente afectados por el incidente.

- **Organización:** McLaren Medical Group (MMG)
  McLaren Medical Group con sede en Michigan, tuvieron un ataque acceso a su sistema informático por una parte no autorizada, lo que posiblemente haya impactado a 106.008 personas. El sistema accedido almacenaba documentos escaneados, incluida información relacionada con autorizaciones, pedidos, programación de citas médicas y datos similares.

- **Organización:** Centro de cirugía oral y facial de Arkansas (Arkansas Oral & Facial Surgery Center)

El Centro de Cirugía Oral y Facial Arkansas experimentó un ataque de ransomware en su red informática el 26 de julio de 2017, con 128.000 personas afectadas con el robo de Imágenes Radiológicas; El ransomware se había instalado antes esa mañana o la noche anterior, según la organización, el ransomware ha dejado inaccesibles los archivos y documentos de imágenes de los pacientes.

- **Organización:** Peachtree Neurological Clinic, P.C.
  La Clínica Neurológica Peachtree, con sede en Atlanta, Georgia, informó que había sido víctima de un ataque de ransomware, lo que podría haber impactado a 176.295 personas. Peachtree se negó a pagar el rescate exigido y pudo restaurar los archivos encriptados a través de los registros de respaldo. También se descubrió que el sistema informático había sido accedido previamente sin el conocimiento de Peachtree entre febrero de 2016 y mayo de 2017. En este ataque el sistema informático afectado contenía: Los nombres de pacientes, direcciones, números de teléfono, números de seguro social, fechas de nacimiento, números de licencia de conducir, información de tratamiento y procedimiento, información de recetas e información de seguro de salud.

- **Organización:** Pacific Alliance Medical Center (PAMC)
  Pacific Alliance Medical Center tomó conocimiento el 14 de junio de 2017 de que su sistema informático en red se había visto afectado por un incidente cibernético. Ciertos archivos habían sido encriptados y no se podían leer, indicó la organización. La OCR establece que 266.123 personas probablemente se vieron afectadas por el incidente.

- **Organización:** Urology Austin, PLLC
  Urology Austin, PLLC, con sede en Texas, experimentó un ataque de ransomware el 22 de enero de 2017 que pudo haber involucrado la información de 279.663 personas. La información potencialmente afectada incluyó nombres de pacientes, direcciones, fechas de nacimiento, números de Seguro Social e información médica. En este caso la organización no pagó el rescate y restauró la información del paciente de una copia de seguridad.

- **Organización:** Women's Healthcare Group of Pennsylvania
  Women's Healthcare Group of Pennsylvania descubrió el 16 de mayo de 2017 que uno de sus centros de práctica tenía un servidor y una estación de trabajo infectados por un virus. Los dispositivos afectados fueron eliminados inmediatamente y se lanzó una investigación; La OCR informó que posiblemente 300.000 personas fueron impactadas.

- **Organización:** Airway Oxygen, Inc.
  Airway Oxygen, Inc, con sede en Michigan, informó a principios del año 2018 que fue víctima de un ataque de ransomware que probablemente afectó a 500,000 personas. La organización indico que los números de las cuentas bancarias, los números de tarjeta de débito o crédito y los números de la Seguridad Social estaban involucrados.

En la Tabla 20, se resumen los Ciberataques masivos contra organizaciones del sector salud, indicando la cantidad de Información de paciente potencialmente comprometida y un costo aproximado por la recuperación de cada archivo y documento de paciente, tomando en consideración el valor en el mercado negro mencionado en la investigación realizada por diario El Comercio.

Tabla 20. Lista de ciberataques a organizaciones del sector salud

Organización	Información de pacientes potencialmente comprometida	Costo aproximado para recuperación de información comprometida en Dólares Americanos
Indiana Hospital	1400 (Rescate pagado)	$ 55.000
VisionQuest Eyecare	85995	$ 4.299.750
Harrisburg Gastroenterology Ltd	93323	$ 4.666.150
McLaren Medical Group (MMG)	106008	$ 5.300.400
Centro de cirugía oral y facial de Arkansas	128000	$ 6.400.000

Clínica Neurológica Peachtree	176295	$ 8.814.750
Pacific Alliance Medical Center	266123	$ 13.306.150
Urology Austin, PLLC	279663	$ 13.983.150
Women's Healthcare Group of Pennsylvania	300000	$ 15.000.000
Airway Oxygen, Inc.	500000	$ 25.000.000

Fuente: Elaborado por el autor

Acorde a la tabla 20, se puede identificar el valor que tiene la información de las organizaciones del sector salud en el mercado negro, así como la recuperación de los mismos. Por tal motivo crece la importancia de implementar controles y políticas de seguridad de la información que permitan mitigar o eliminar las amenazas y vulnerabilidades que existen sobre los activos de información.

3.7 CERTIFICACIÓN DE LA NORMA ISO/IEC 27001

El tema de la certificación en aspectos de seguridad de información para organizaciones del sector salud aún no ha sido considerado con la seriedad que se merece en el ámbito empresarial; sin embargo, no hay duda que en el muy corto plazo será una cuestión importante e incluso obligatoria para cualquier organización sea público o privado y que desee desarrollarse en el mercado del sector salud.

Una de las ventajas para una empresa certificada en ISO/IEC 27001 es su reconocimiento externo. Disponer de una certificación significa que una tercera parte independiente y acreditada avala que los niveles del Sistema de Gestión de Seguridad de la Información de la organización cumplen con los estándares internacionalmente.

En el Ecuador, la entidad de certificación formal es SAE - (Servicio de Acreditación Ecuatoriano, 2018). La primera empresa ecuatoriana en obtener una

certificación ISO 27001 fue Telconet y su entidad de certificación fue internacional SGS United Kingdom. Movistar que también se certificó en febrero 2012, fue auditada por la Asociación Española de Normalización y Certificación AENOR. Acorde a una investigación anual realizada por la Organización Internacional de Normalización (ISO), hasta el año 2017 Ecuador posee 11 organizaciones con certificación ISO 27001 (Organización Internacional de Normalización, 2017). El sitio oficial de la organización ISO no proporciona información sobre cuáles son las 11 empresas que en Ecuador están certificadas.

Para aprobar una acreditación, la entidad certificadora realizará los siguientes pasos:

3.7.1 INICIO: SOLICITUD DE CERTIFICACIÓN Y PRE-AUDITORIA

Como paso inicial se realizará una solicitud de auditoría en la página web de SAE, donde la organización interesada debe pedir a la entidad de certificación este hecho. Luego, la empresa certificadora ha de responder exponiendo su oferta y compromiso para el proceso de certificación. Si la oferta está acorde y es aceptada, la empresa certificadora prosigue con la designación de auditores, alcance y fijación de fechas. En este punto si se requiere se puede realizar una auditoría previa para dar información acerca de la situación actual y dar orientación para facilitar la superación de la auditoría real.

3.7.2 FASE 1: REVISIÓN DE LA DOCUMENTACIÓN

Uno de los objetivos de la auditoría que corresponde a la fase 1 es la revisión de la documentación que exige la norma, la cual permite a la Entidad de Certificación la comprensión del SGSI dentro del contexto de la política de seguridad, objetivos y aproximación a la gestión de riesgos de la empresa. En esta fase, el auditor buscará la documentación mínima requerida por la norma y los registros sobre los controles del Anexo A de la norma ISO/IEC 27001.

Esta fase sirve como punto de referencia útil a la hora de preparar la auditoría de fase 2 y ofrece una oportunidad para evaluar el grado de preparación de la empresa. Si falta alguno de estos elementos, significa que la empresa no está lista para la fase 2 de auditoría.

3.7.3 FASE 2: AUDITORÍA “IN SITU”

Esta auditoría también es conocida como auditoría principal y está guiada por las conclusiones del informe de auditoría de fase 1. Se redactará el plan de auditoría basándose en estas conclusiones y se enviará con la debida antelación a la organización proponiendo el equipo auditor, itinerario, tiempos, recursos necesarios, entre otros. En la fecha programada se llevará a cabo la auditoría en las instalaciones de la organización donde esté desplegado e implantado el SGSI.

El enfoque de dicha auditoría no se trata de la documentación si no sobre si la empresa realmente está haciendo lo que sus documentos y la norma indican qué hacer. Es decir que se hará una verificación sobre si el SGSI se aplica o está solamente en letra muerta mediante entrevistas con el personal de la organización y control de los registros presentados. Entre los registros obligatorios se incluyen los de formación, capacitación, habilidades, experiencias y calificaciones, auditoría interna, revisión por parte de la gerencia y medidas correctivas y preventivas.

Se debe tomar en cuenta que después de obtener la certificación ISO 27001, dicho certificado tiene una duración de tres años (al tercer año se hace una auditoría de recertificación) pudiendo ser suspendido durante este periodo si la Entidad Certificadora detecta algún otro incumplimiento grave en sus visitas de control y seguimiento realizadas semestral o al menos anualmente. En la Figura 17 se muestra el proceso de certificación de la norma ISO/IEC 27001.

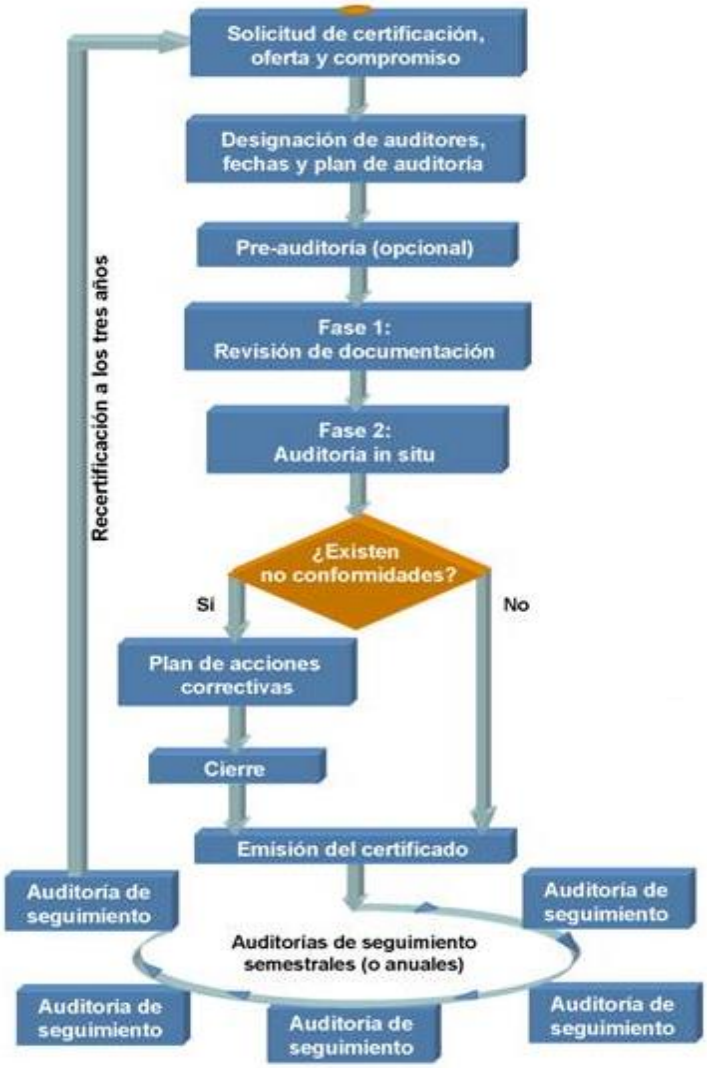


Figura 16 Proceso de certificación de la norma ISO/IEC 27001

Fuente: Tomado de (iso27000.es, 2012)

CAPÍTULO 4: VALIDACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA CLÍNICA MÉDICA FÉRTIL

En el capítulo 4, se realiza la aplicación del modelo de Sistema de Gestión de Seguridad de la Información en la Clínica Médica Fértil, conforme a la metodología descrita en el apartado 3.5 de este documento, detallando las políticas de seguridad de la información.

4.1 LANZAMIENTO Y ANÁLISIS DEL CONTEXTO DE LA ORGANIZACIÓN

Para la fase de lanzamiento y análisis del contexto se toma en consideración la descripción de la Clínica Médica Fértil realizada en el ítem 3.1. De igual manera para identificar el estado actual de la seguridad de la información en la clínica, se evaluará el nivel de cumplimiento de la norma ISO/IEC 27002:2013.

4.1.1 ESTADO ACTUAL DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES CON RESPECTO A LA NORMA ISO/IEC 27002:2013

En el presente ítem se describe el estado de la seguridad de la información en la Clínica Médica Fértil, en el proceso se evalúa el nivel de cumplimiento de cada uno de los dominios descritos por la norma ISO/IEC 27002:2013. La encuesta es realizada al responsable de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones. En la Figura 18 se muestra los resultados del análisis realizado.

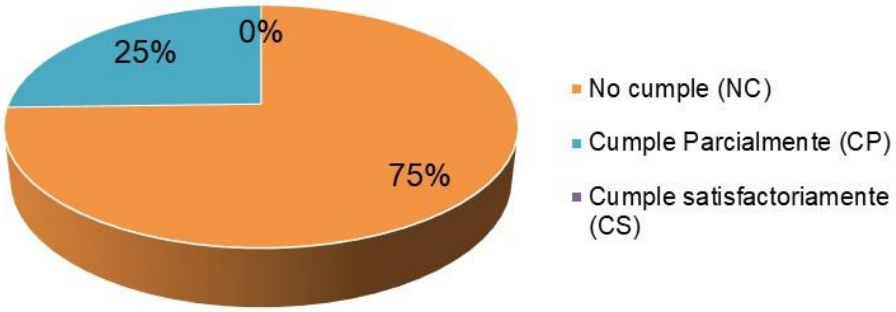


Figura 17 Nivel de cumplimiento de los dominios de la norma ISO/IEC 27002:2013

Fuente: Elaborado por el autor

Acorde al grafico 18 y la Tabla 21, se puede indicar que 85 de los controles tienen una valoración de “No Cumple” y que equivalen a un 75%, mientras que 29 controles tienen una valoración de “Cumple Parcialmente” y equivale a un 25%, así como también existe 0 controles con calificación de “Cumple satisfactoriamente”. El total de los controles suma 114. El detalle de la valoración por dominio y control de seguridad de la información para conocer la situación actual se encuentra en el anexo 4.

Tabla 21. Nivel de cumplimiento de los dominios de la norma ISO/IEC 27002:2013

Control en la Normativa	Sección	NC	CP	CS	Controles evaluados
5.	Políticas de seguridad de la información	1	1	0	2
6.	Organización de la seguridad de la información	4	3	0	7
7.	Seguridad ligada a los recursos humanos	3	3	0	6
8.	Gestión de activos	8	2	0	10
9.	Control de acceso	9	5	0	14
10.	Criptografía	1	1	0	2
11.	Seguridad física y del entorno	11	4	0	15
12.	Seguridad de las operaciones	11	3	0	14
13.	Seguridad de las comunicaciones	6	1	0	7
14.	Adquisición, desarrollo y mantenimiento de sistemas de información	11	2	0	13

Control en la Normativa	Sección	NC	CP	CS	Controles evaluados
15.	Relaciones con los proveedores	4	1	0	5
16.	Gestión de incidentes de seguridad de la información	6	1	0	7
17.	Aspectos de seguridad de la información de la gestión de continuidad de negocio	4	0	0	4
18.	Cumplimiento	6	2	0	8
Suma Total		**85**	**29**	**0**	**114**

Fuente: Elaborado por el autor

4.2 ALCANCE DEL SGSI

Tabla 21. Alcance del sistema de gestión de seguridad de la información

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
Organización: Clínica Médica Fértil
Objetivo: Establecer que elementos de la Clínica Médica Fértil formarán parte del Sistema de Gestión de Seguridad de la Información, a través de cual se permita brindar confidencialidad, integridad y disponibilidad a los servicios médicos y los sistemas de información existentes.
Descripción: Por su naturaleza, las entidades prestadoras de servicios de salud realizan sus atenciones en ambientes en los cuales se dificulta el control sobre el público que accede entre los cuales se tiene pacientes, visitas, médicos, trabajadores y público en general, siendo difícil la segmentación de las personas que pertenecen a cada uno de estos grupos. Por tal motivo el Sistema de Gestión de Seguridad

de la Información de la Clínica Médica Fértil abarca todas las áreas administrativas, servicios médicos e infraestructura tecnológica tanto a nivel interno como a nivel externo de la organización. La implementación del Sistema de Gestión de Seguridad de la Información a través de las políticas y procedimientos permitirá brindar confidencialidad, integridad y disponibilidad a los servicios médicos, información de los pacientes y los sistemas de información existentes.

Para el análisis y determinación de riesgos del SGSI, se realiza dos actividades: el establecimiento de escenarios de riesgo y el consenso de valores asignados a cada activo de información, utilizando el método “Delphi” en donde su objetivo es la consecución de un consenso basado en la discusión de expertos una vez aplicado un cuestionario.

Por otro lado, se debe considerar que no es posible hacer pruebas con la información real de los pacientes y sistemas informáticos relacionados, debido que por normas éticas y morales no se puede tener acceso a dicha información clasificada sin autorización de la Gerencia y los pacientes.

Las funciones de las áreas involucradas en el Sistema de Gestión de Seguridad de la Información son las siguientes:

1. **Gerencia**:
    - Representar a la institución legalmente.
    - Autorizar el ingreso del personal necesario.
    - Establecer objetivos a corto y largo plazo.
    - Autorizar la compra de insumos para la institución.
    - Tomar decisiones respecto a sanciones al personal por incumplimiento de normas.
    - Desarrollar estrategias para mantener la buena imagen de la Clínica.
    - Identificar, analizar y resolver los problemas que se presenten en la institución.

- Supervisar la contabilidad y cierres de caja.
- Tomar decisiones en favor de la institución.

2. Dirección Administrativa

2.1. Talento Humano:

- Planear, organizar, dirigir y controlar los programas, estrategias y acciones a desarrollar para el óptimo aprovechamiento de las habilidades del personal.
- Proponer medidas técnico administrativas para el mejor funcionamiento de los recursos existentes.
- Supervisa y distribuye las actividades del personal.
- Velar por el cumplimiento de las normas y procedimientos de higiene y seguridad, establecidos por la organización.
- Elaborar y controlar el proceso de reclutamiento, selección, ingreso e inducción del personal.
- Proyectar y coordinar programas de capacitación y entrenamiento para los empleados.
- Coordinar y controlar el proceso de desincorporación del personal.

2.2. Servicios generales:

- Dar cumplimiento a las políticas y normas de seguridad e higiene emitidas.
- Mantenimiento de equipos médicos.
- Limpieza y seguridad de las instalaciones.
- Mantener el orden e higiene de los materiales o enseres utilizados.
- Informar del deterioro de los equipos médicos e instalaciones de la clínica.
- Brindar apoyo en las tareas administrativas de la Institución.
- Tratamiento de reciclaje de desechos infecciosos.
- Suministrar, controlar y conservar en buen estado físico y logístico interno de la Institución.

3. Dirección Contable – Financiera.

3.1. Contabilidad

- Realizar un listado de los insumos médicos y administrativos faltantes.
- Realizar las cotizaciones.
- Pago a proveedores.
- Facturación de servicios médicos.
- Control de inventario (Laboratorio, Farmacia, Emergencia, Consultorios).
- Preparar los registros para realizar las declaraciones.
- Recibir, examinar, clasificar y codificar los documentos contables.
- Archivar documentos contables.
- Mantener actualizados los registros contables.

3.2. Presupuesto

- Registro de ingresos, gastos y control de inventarios.
- Pago a empleados de la institución.
- Realizar el cierre del ejercicio al finalizar el periodo.
- Verificar y consolidar saldos contables.
- Asesorar a gerencia en la toma de decisiones financieras.
- Llevar un adecuado control de los activos fijos de la Clínica y su respectiva depreciación.
- Elaborar de Conciliaciones Bancarias.
- Preparar y presentar informes acerca de la situación financiera a los accionistas.

4. Consulta Externa:

- Brindar un servicio ambulatorio para pacientes con una cita asignada de los diferentes tipos de diagnósticos que posee la clínica: Medicina General, Otorrinolaringología, Ginecología – Infertilidad, Pediatría y Acupuntura.

5. Servicios Médicos:

- Brindar a los pacientes un eficiente servicio médico de las diferentes atenciones que presta la clínica:
    - Hospitalización
    - Quirófano

○ Emergencia ○ Farmacia ○ Servicios de diagnóstico (Imagenología) ○ Laboratorio de Infertilidad Se debe considerar que en organigrama estructural vigente de la Clínica Médica Fértil la Unidad de Tecnología de la información y Comunicaciones se encuentra como una unidad de apoyo y es considerado como un servicio general; sin embargo, las funciones de la unidad de TIC se encuentran descrita en el ítem 3.1.7.

Fuente: Elaborado por el autor

4.3 POLÍTICA Y OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Tabla 22. Política y objetivos de la seguridad de la información

POLÍTICA Y OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
Organización: Clínica Médica Fértil
Objetivo: Describir y establecer la política y objetivos del Sistema de Gestión de Seguridad de la Información en la Clínica Médica Fértil, que permita especificar las condiciones, derechos y obligaciones de cada uno de los miembros de la organización con respecto a la utilización de los activos y sistemas informáticos.
Descripción: La política y objetivos propuestos para el presente SGSI es la siguiente: **1. Política del SGSI:** La Clínica Médica Fértil enfocada en brindar un servicio de salud de calidad, orientado siempre a la satisfacción de los pacientes y en cumplimiento de la misión, visión y objetivos estratégicos, establece la función del Sistema de Gestión de Seguridad de la Información con el objetivo de:

- Cumplir con los requerimientos legales y reglamentarios aplicables a la Clínica Médica Fértil y al Sistema de Gestión de Seguridad de la Información.
- Entregar servicio de salud de calidad, con sentido de pertenencia, actitud proactiva y comunicación continua y oportuna.
- Gestionar los riesgos de la entidad a través de la aplicación de estándares y controles orientados a preservar la seguridad de nuestra información.
- Mantener buenas prácticas de seguridad de la información que garantizan la Disponibilidad, Integridad y Confidencialidad de la información, proporcionando confianza en nuestras partes interesadas.
- Implementar el sistema de gestión de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores de la Clínica Médica Fértil.
- Garantizar la continuidad de los servicios y la seguridad de la información.
- Garantizar la Disponibilidad, Integridad y Confidencialidad de los datos personales y sensibles de sus pacientes en todo uso que a estos se les pueda dar, siguiendo los lineamientos otorgados por la ley y el uso ético de los mismos.
- Los colaboradores de la Clínica Médica Fértil deben comprometerse con el cumplimiento de lo establecido por el presente documento, así como con las políticas y procedimientos relacionados del SGSI – tanto los ya vigentes como los que se publiquen posteriormente.

Aplicabilidad de la Política del SGSI:

Esta política aplica a toda la Clínica Médica Fértil, sus colaboradores, proveedores, terceros y demás partes interesadas.

2. Objetivos del SGSI:

- Ofrecer un servicio médico de calidad a las pacientes, garantizando que se apliquen los controles necesarios para asegurar su información.
- Cumplir con los requerimientos legales en cuanto a la protección de la información de los pacientes.

• Establecer y monitorear un Sistema de Gestión de Seguridad de la Información que identifique los riesgos a los que se expone la información en la Clínica Médica Fértil y pueda definir controles para los mismos. • Concienciar al personal sobre la importancia del SGSI, así como su responsabilidad sobre el cumplimiento de lo dispuesto por el SGSI. • Garantizar el acceso a la información de la Clínica Médica Fértil de acuerdo con los niveles de la organización y criterios de seguridad que establezca la entidad, la normatividad aplicable y/o las partes interesadas. • Mantener la disponibilidad e integridad de la información de la entidad, teniendo en cuenta los requisitos de seguridad aplicables y los resultados de la valoración y el tratamiento de los riesgos identificados. • Asegurar que la información de la Clínica Médica Fértil esté disponible para los usuarios o procesos autorizados en el momento en que así lo requieran.

Fuente: Elaborado por el autor

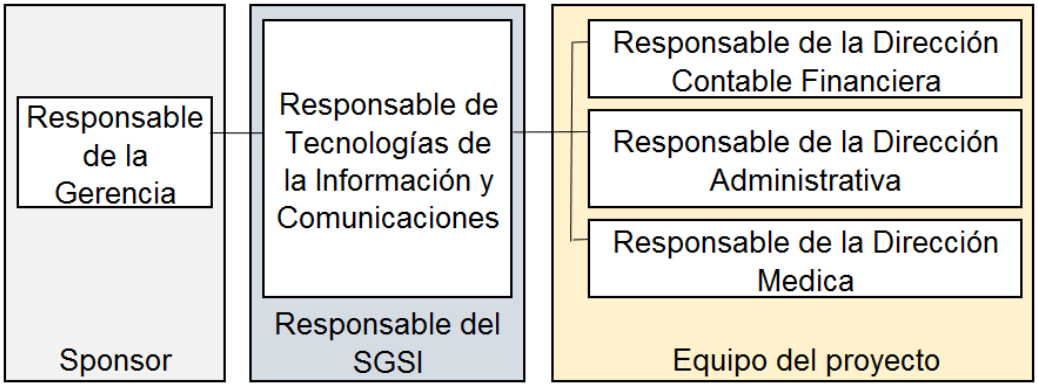
4.4 RECURSOS, COMPETENCIAS, COMUNICACIÓN E INFORMACIÓN DOCUMENTADA

Tabla 23. Recursos, competencias, comunicación e información documentada

RECURSOS, COMPETENCIAS, COMUNICACIÓN E INFORMACIÓN DOCUMENTADA
Organización: Clínica Médica Fértil
Objetivo: Describir y establecer los recursos, competencias, comunicación e información documentada que servirán como apoyo en el proceso de implementación del Sistema de Gestión de Seguridad de la Información en la Clínica Médica Fértil.

Recursos:

Se define la estructura organizativa de la Clínica Médica Fértil que proporcionará el apoyo necesario en todo el ciclo de vida de implementación del Sistema de Gestión de Seguridad de la Información. Dentro de las responsabilidades del equipo del proyecto está gestionar los Recursos Humanos, Administrativos y Financieros.



Competencias:

Se evaluará a cada miembro del equipo del proyecto por la experiencia y conocimiento que posee en el desarrollo de un Sistema de Gestión de Seguridad de la Información, en caso de tener falencias se dará una capacitación previa sobre el tema para que exista una comunicación más fluida sobre temas de confidencialidad, integridad y disponibilidad de la información. El encargado de la capacitación será el responsable de Tecnologías de la Información y Comunicaciones.

Comunicación:

1. **Guía para reuniones formales del Equipo de Proyecto:**

- Se deberá fijar la agenda con anterioridad.
- Se deberá coordinar e informar la fecha, hora y lugar con los participantes.
- Se deberá empezar puntual.
- Se deberá fijar los objetivos de la reunión, los roles, los procesos grupales de trabajo, y los métodos de solución de polémicas.
- Se deberá cumplir a cabalidad los roles de facilitador (dirige el proceso grupal de trabajo) y de anotador (toma nota de los resultados formales de la reunión).
- Se deberá terminar puntual.

- Se deberá emitir un acta de reunión la cual se debe repartir a los participantes (previa revisión por parte de ellos).

2. **Comunicaciones entre miembros del equipo:** Serán realizadas principalmente por correo electrónico o utilizando un repositorio digital de documentos para compartir la información.
3. **Comunicaciones masivas a todos los colaboradores del Proyecto:** se informará mediante correo electrónico, así como también las capacitaciones sobre las políticas y procesos definidos.

Información documentada:

Los formatos y versiones de la documentación generada dentro del Sistema de Gestión de Seguridad de la Información en la Clínica Médica Fértil serán definidos por el equipo del proyecto y almacenado en un repositorio digital.

Fuente: Elaborado por el autor

4.5 ACCIONES PARA ABORDAR LOS RIESGOS Y LAS OPORTUNIDADES

En esta fase se genera toda la información documentada acerca del proceso de evaluación de riesgo de la seguridad de la información. Conforme se muestra en la Tabla 24, se inicia con el inventario de los activos de la Clínica Médica Fértil:

Tabla 24. Inventario de los activos de la Clínica Médica Fértil

#	Nombre del activo	Descripción del activo	Tipo de activo	Propietario del activo
1	Servicios Médicos	Servicios clínicos especializados y de emergencia prestado a los pacientes	Servicios médicos y procesos del negocio	Responsable de Gerencia
2	Consulta Externa	Servicio ambulatorio para pacientes con una cita asignada previamente que acceden a atenciones	Servicios médicos y procesos del negocio	Responsable de Gerencia

		médicas para diferentes tipos de diagnósticos.		
3	Historia Clínica	Documentación y registros informáticos que contiene datos, valoraciones e información generado en cada uno de los procesos asistenciales a un paciente	Información / Datos	Responsable de Dirección Médica
4	Informe de resultados de pruebas de laboratorio	Base de datos con resultados de exámenes de laboratorio específicos.	Información / Datos	Responsable de Servicios Médicos Especializados
5	Informe de tratamientos de fertilidad	Archivos donde se registra todo el proceso de fertilidad para fecundación de las pacientes.	Información / Datos	Responsable de Servicios Médicos Especializados
6	Informe de pruebas de Endoscopia	Información que refleja los resultados de tomografías o ecografía	Información / Datos	Responsable de Servicios Médicos Especializados
7	Informe de resultados de Ecografías	Archivos físico y digital de las imágenes obtenidas de pacientes	Información / Datos	Responsable de Servicios Médicos Especializados
8	Torre de Endoscópica	Equipo para la realización técnica de exploración gastro-endoscópicas, contiene puerto USB para observar la imagen en la pantalla de un PC y almacena videos e imágenes en su memoria flash interna	Hardware	Responsable de Servicios Médicos Especializados

9	Monitor de signos vitales	Dispositivo que permite detectar, procesar y desplegar en forma continua los parámetros fisiológicos del paciente; Conexión USB o inalámbrica y memoria interna para mediciones de los pacientes	Hardware	Responsable de Servicios Médicos Especializados
10	Ecógrafo	Aparato de diagnóstico electro médico utilizado para realizar ecografías o ultrasonidos; integra mini computador, lectograbadora de CD/DVD y puertos USB	Hardware	Responsable de Servicios Médicos Especializados
11	Impresora de placas radiográficas	Dispositivos que permite imprimir imágenes de resultados de ecografías, endoscopías, entre otros.	Hardware	Responsable de Servicios Médicos Especializados
12	Computador recepción	Computador que se utiliza para agendar citas médicas	Hardware	Responsable de Recepción
13	Computador Contabilidad	Computador donde se realizan actividades relacionadas a el área de contabilidad	Hardware	Responsable de Contabilidad
14	Computador Presupuesto	Computador donde se realizan actividades relacionadas a el área de Presupuestos	Hardware	Responsable de Presupuesto
15	Computador Laboratorio	Computador donde se ingresan los resultados de exámenes de laboratorio	Hardware	Responsable de Servicios Médicos Especializados

16	Computador Consultorio Ginecología	Computador donde se lleva un registro del historial clínico de pacientes respecto a Ginecologia	Hardware	Responsable de Consulta externa
17	Portátil del área de Emergencia	Computador donde se lleva un registro de historial clínico de los pacientes en el área de emergencia	Hardware	Responsable de Servicios Médicos Especializados
18	Portátil del área de Farmacia	Computador donde se lleva un registro e inventario de los medicamentos.	Hardware	Responsable de Servicios Médicos Especializados
19	Portátil Consultorio de Otorrinolarin-gología	Computador donde se lleva un registro de historial clínico de pacientes respecto a Otorrinolaringología	Hardware	Responsable de Consulta externa
20	Portátil Consultorio de Pediatría	Computador donde se lleva un registro de historial de pacientes respecto a Pediatría	Hardware	Responsable de Consulta externa
21	Impresora del área de recepción	Equipo conectado para el área de recepción y contabilidad	Hardware	Responsable de Recepción
22	Impresora del área de laboratorio	Equipo conectado para imprimir resultados de exámenes de laboratorio	Hardware	Responsable de Servicios Médicos Especializados
23	Impresora del área de Pediatría / Ginecología	Equipo utilizado para imprimir información de pacientes respecto a Pediatría / ginecología	Hardware	Responsable de Consulta externa

24	Antivirus	Programa informático que protege a los equipos de cómputo de los virus	Software	Responsable de Servicios Generales
25	Recursos de Ofimática	Aplicación o paquete de aplicaciones que tiene funciones ofimáticas, es decir, que sirven para facilitar el trabajo en el ámbito de una oficina.	Software	Responsable de Servicios Generales
26	Grabador de vídeo digital	Equipo de gestión de vídeo para el control, la grabación y el archivo de vídeos que provienen de cámaras de video vigilancia	Hardware	Responsable de Servicios Generales
27	Cámara de video vigilancia	Equipo de monitoreo y grabación de imágenes de una área determinada.	Hardware	Responsable de Servicios Generales
28	Servidor HP Elite 8300	Servidor para Pagina WEB / Aplicaciones / Correo electrónico	Hardware	Responsable de Servicios Generales
29	Reloj Biométrico	Sistema de control de ingreso del personal	Hardware	Responsable de Servicios Generales
30	Central telefónica Analógica	Equipo telefónico que permite la comunicación entre el personal de la organización	Redes de comunicaciones	Responsable de Servicios Generales
31	Teléfono analógico	Equipo telefónico que permite la comunicación entre el personal de la organización	Redes de comunicaciones	Responsable de Servicios Generales
32	Red LAN	Red LAN usada por equipos móviles para acceder a los	Redes de comunicaciones	Responsable de Servicios Generales

		recursos de la red corporativa de la clínica		
33	Red WLAN	Red WLAN usada por equipos móviles para acceder a los recursos de la red corporativa de la clínica	Redes de comunicaciones	Responsable de Servicios Generales
34	Módem	Equipo que permite ofrecer acceso a Internet por la línea telefónica a los computadores	Redes de comunicaciones	Responsable de Servicios Generales
35	Switch	Dispositivo de 8 puertos de interconexión de equipos en red	Redes de comunicaciones	Responsable de Servicios Generales
36	Registros Contables - Financieros	Documentación que contienen datos relacionados con las operaciones económicas y financieras de la clínica	Información / Datos	Responsable de Contabilidad
37	Registros de asistencia del personal	Documentación del control digital de entrada/salida del personal	Información / Datos	Responsable de Talento Humano
38	Base de datos talento humano	Información que dispone este departamento debidamente actualizada en donde incluye información completa del personal que labora como datos personales, cargo, salario, beneficios, horarios, cursos o actividades realizadas.	Información / Datos	Responsable de Talento Humano
39	Consultorios	Espacio físico en el cual un médico o varios médicos asociados atienden a sus pacientes	Sitio / Instalaciones	Responsable de Servicios Generales

40	Laboratorio	Espacio físico en el cual se encuentran equipamiento médico para realizar pruebas y diagnóstico de los pacientes.	Sitio / Instalaciones	Responsable de Servicios Generales
41	Quirófano	Espacio físico acondicionada para la práctica de operaciones quirúrgicas a aquellos pacientes que así lo demanden	Sitio / Instalaciones	Responsable de Servicios Generales
42	Página WEB	Documento de tipo electrónico, el cual contiene información digital de la Clínica	Software	Responsable de Servicios Generales
43	Talento Humano	Talento humano que labora en la diferentes áreas de la clínica	Personas	Gerencia

Fuente: Elaborado por el autor

Posteriormente, se realiza la valoración de los activos que permitirá determinar el impacto que el deterioro, falla o pérdida de los mismos tiene sobre la confidencialidad, disponibilidad e integridad de la información de la Clínica Médica Fértil. La valoración de la Tabla 25, se realiza tomando en consideración los criterios de la Gerencia y del responsable de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones de la clínica.

Tabla 25. Valorización de los activos de la Clínica Médica Fértil

#	Nombre del activo	Confi-dencialidad	Integridad	Disponi-bilidad	Valoración
1	Servicios Médicos	3	3	3	3,00
2	Consulta Externa	3	3	3	3,00
3	Historia Clínica	3	3	3	3,00

4	Informe de resultados de pruebas de laboratorio	3	3	3	3,00
5	Informe de tratamientos de fertilidad	3	3	3	3,00
6	Informe de pruebas de Endoscopia	3	3	3	3,00
7	Informe de resultados de Ecografías	3	3	3	3,00
8	Torre de Endoscópica	3	3	2	2,67
9	Monitor de signos vitales	3	3	2	2,67
10	Ecógrafo	3	3	2	2,67
11	Impresora de placas radiográficas	3	3	2	2,67
12	Computador recepción	2	2	1	1,67
13	Computador Contabilidad	2	2	1	1,67
14	Computador Presupuesto	2	2	1	1,67
15	Computador Laboratorio	2	2	3	2,33
16	Computador Consultorio Ginecología	2	2	1	1,67
17	Portátil del área de Emergencia	3	3	3	3,00
18	Portátil del área de Farmacia	3	3	3	3,00

19	Portátil Consultorio Otorrinolaringología	2	2	1	1,67
20	Portátil Consultorio de Pediatría	2	2	1	1,67
21	Impresora del área de recepción	2	2	1	1,67
22	Impresora del área de laboratorio	2	2	1	1,67

#	Nombre del activo	Confi-dencialidad	Integridad	Disponi-bilidad	Valoración
23	Impresora del área de Pediatría / Ginecología	2	2	1	1,67
24	Antivirus	2	2	2	2,00
25	Recursos de Ofimática	2	2	1	1,67
26	Grabador de vídeo digital	2	1	1	1,33
27	Cámara de video vigilancia	2	2	1	1,67
28	Servidor HP Elite 8300	3	3	2	2,67
29	Reloj Biométrico	2	2	1	1,67
30	Central telefónica Analógica	2	1	1	1,33
31	Teléfono analógico	2	1	1	1,33
32	Red LAN	2	2	2	2,00
33	Red WLAN	2	2	1	1,67
34	Módem	2	2	2	2,00
35	Switch	2	2	2	2,00

36	Registros Contables - Financieros	3	3	2	2,67
37	Registros de asistencia del personal	3	3	2	2,67
38	Base de datos talento humano	2	2	1	1,67
39	Consultorios	1	1	1	1,00
40	Laboratorio	2	1	1	1,33
41	Quirófano	2	2	3	2,33
42	Página WEB	2	2	2	2,00
43	Talento Humano	2	2	3	2,33

Fuente: Elaborado por el autor

En la Tabla 26, se muestra los activos de la Clínica Médica Fértil que serán considerados dentro del análisis de riesgo. Cabe señalar que en la selección de los activos participó la Gerencia de la clínica y el responsable de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Tabla 26. Activos de la Clínica Médica Fértil considerados dentro del análisis de riesgo.

#	Nombre del activo	Tipo de activo
1	Servicios Médicos	Servicios médicos y procesos del negocio
2	Consulta Externa	Servicios médicos y procesos del negocio
3	Historia Clínica	Información / Datos
4	Informe de resultados de pruebas de laboratorio	Información / Datos
5	Informe de tratamientos de fertilidad	Información / Datos
6	Informe de pruebas de Endoscopia	Información / Datos
7	Informe de resultados de Ecografías	Información / Datos
8	Torre de Endoscópica	Hardware

9	Monitor de signos vitales	Hardware
10	Ecógrafo	Hardware
11	Impresora de placas radiográficas	Hardware
12	Computador Laboratorio	Hardware
13	Portátil del área de Emergencia	Hardware
14	Portátil del área de Farmacia	Hardware
15	Antivirus	Software
16	Servidor HP Elite 8300	Hardware
17	Red LAN	Redes de comunicaciones
18	Módem	Redes de comunicaciones
19	Switch	Redes de comunicaciones
20	Registros Contables – Financieros	Información / Datos
21	Registros de asistencia del personal	Información / Datos
22	Quirófano	Sitio / Instalaciones
23	Página WEB	Software
24	Talento Humano	Personas

Fuente: Elaborado por el autor

Conforme al modelo propuesto se realiza la identificación y valorización de las amenazas sobre los activos de la Clínica Médica Fértil. En la Tabla 27 se muestra la ponderación del impacto en caso de materializarse la amenaza. Posteriormente en la Tabla 28 se indica que tan probable es que una amenaza se concrete con una o varias de las vulnerabilidades encontradas en los activos de la Clínica Médica Fértil. De igual manera, el proceso fue analizado y seleccionado por la Gerencia de la clínica y el responsable de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Tabla 27. Valorización de las amenazas sobre los activos de la Clínica Médica Fértil

#			1	2	3	4	5
Nombre del activo			Servicios Médicos	Consulta Externa	Historia Clínica	Informe de resultados de pruebas de laboratorio	Informe de tratamientos de fertilidad
Tipo de activo			Servicios médicos y procesos del negocio	Servicios médicos y procesos del negocio	Información / Datos	Información / Datos	Información / Datos
Tipo Amenaza	Daño físico		3	3	3	2	2
	Eventos naturales		2	2	1	1	1
	Pérdida de los servicios esenciales		3	3	1	2	2
	Perturbación debida a la radiación		1	1	1	1	1
	Compromiso de la información		3	3	3	3	3
	Fallas técnicas		3	3	2	2	2
	Acciones no autorizadas		3	3	3	2	2
	Compromiso de las funciones		3	3	3	3	3
	Fallas Humanas intencionales	Pirata informático, intruso ilegal	3	3	3	3	3
		Criminal de la computación	3	3	3	3	3
		Terrorismo	3	3	3	3	3
		Espionaje industrial	3	3	3	3	3
		Intrusos	3	3	3	3	3
Valoración			2,77	2,77	2,46	2,38	2,38

#			6	7	8	9	10
Nombre del activo			Informe de pruebas de Endoscopia	Informe de resultados de Ecografías	Torre de Endoscópica	Monitor de signos vitales	Ecógrafo
Tipo de activo			Información / Datos	Información / Datos	Hardware	Hardware	Hardware
Tipo Amenaza	Daño físico		2	2	2	3	3
	Eventos naturales		1	1	1	1	1
	Pérdida de los servicios esenciales		2	2	3	3	3
	Perturbación debida a la radiación		1	1	2	1	2
	Compromiso de la información		3	3	2	2	2
	Fallas técnicas		2	2	3	3	3
	Acciones no autorizadas		2	2	3	3	3
	Compromiso de las funciones		3	3	2	2	2
	Fallas Humanas intencionales	Pirata informático, intruso ilegal	3	3	2	2	2
		Criminal de la computación	3	3	2	2	2
		Terrorismo	3	3	2	2	2
		Espionaje industrial	3	3	2	2	2
		Intrusos	3	3	3	3	3
Valoración			2,38	2,38	2,23	2,23	2,31

#			11	12	13	14	15
Nombre del activo			Impresora de placas radiográficas	Computador Laboratorio	Portátil del área de Emergencia	Portátil del área de Farmacia	Antivirus
Tipo de activo			Hardware	Hardware	Hardware	Hardware	Software
Tipo Amenaza	Daño físico		3	2	2	2	1
	Eventos naturales		1	1	1	1	1
	Pérdida de los servicios esenciales		3	2	2	2	2
	Perturbación debida a la radiación		2	1	1	1	1
	Compromiso de la información		2	2	2	2	2
	Fallas técnicas		3	3	3	3	1
	Acciones no autorizadas		3	3	3	3	1
	Compromiso de las funciones		2	2	2	2	1
	Fallas Humanas intencionales	Pirata informático, intruso ilegal	2	3	3	3	3
		Criminal de la computación	2	3	3	3	3
		Terrorismo	2	3	3	3	3
		Espionaje industrial	2	3	3	3	3
		Intrusos	3	3	3	3	2
Valoración			2,31	2,38	2,38	2,38	1,85

#			16	17	18	19
Nombre del activo			**Servidor HP Elite 8300**	**Red LAN**	**Módem**	**Switch**
Tipo de activo			**Hardware**	**Redes de comunicaciones**	**Redes de comunicaciones**	**Redes de comunicaciones**
Tipo Amenaza	Daño físico		2	2	2	2
	Eventos naturales		1	1	1	1
	Pérdida de los servicios esenciales		2	2	2	2
	Perturbación debida a la radiación		1	1	1	1
	Compromiso de la información		3	2	2	2
	Fallas técnicas		3	2	3	3
	Acciones no autorizadas		3	2	2	2
	Compromiso de las funciones		3	2	2	2
	Fallas Humanas intencionales	Pirata informático, intruso ilegal	3	2	3	3
		Criminal de la computación	3	2	2	2
		Terrorismo	3	2	2	2
		Espionaje industrial	3	2	2	2
		Intrusos	3	2	3	3
Valoración			2,54	1,85	2,08	2,08

#			20	21	22	23	24
Nombre del activo			**Registros Contables - Financieros**	**Registros de asistencia del personal**	**Quirófano**	**Página WEB**	**Talento Humano**
Tipo de activo			**Información / Datos**	**Información / Datos**	**Sitio / Instalaciones**	**Software**	**Personas**
Tipo Amenaza	Daño físico		2	2	3	1	2
	Eventos naturales		1	1	2	1	1
	Pérdida de los servicios esenciales		1	2	3	2	2
	Perturbación debida a la radiación		1	1	1	1	1
	Compromiso de la información		2	2	1	3	3
	Fallas técnicas		1	1	1	3	2
	Acciones no autorizadas		1	1	1	1	2
	Compromiso de las funciones		3	2	1	2	3
	Fallas Humanas intencionales	Pirata informático, intruso ilegal	3	3	2	3	3
		Criminal de la computación	2	2	1	2	3
		Terrorismo	2	2	1	3	3
		Espionaje industrial	3	3	2	3	3
		Intrusos	3	3	2	3	3
Valoración			1,92	1,92	1,62	2,15	2,38

Fuente: Elaborado por el autor

Tabla 28. Probabilidad de que una amenaza explote la vulnerabilidad de los activos de la Clínica

#		1	2	3	4	5	6
Nombre del activo		Servicios Médicos	Consulta Externa	Historia Clínica	Informe de resultados de pruebas de laboratorio	Informe de tratamientos de fertilidad	Informe de pruebas de Endoscopia
Tipo de activo		Servicios médicos y procesos del negocio	Servicios médicos y procesos del negocio	Información / Datos	Información / Datos	Información / Datos	Información / Datos
Tipo vulnerabilidades	Hardware	3	3	3	3	3	2
	Software	2	2	3	2	2	2
	Redes de comunicaciones	2	2	2	2	2	2
	Personal	3	3	3	3	3	3
	Sitio / Instalaciones	2	2	2	2	2	2
	Organización	3	3	3	3	3	3
Valoración		2,50	2,50	2,67	2,50	2,50	2,33

#		7	8	9	10	11	12	13
Nombre del activo		**Informe de resultados de Ecografías**	**Torre de Endoscópica**	**Monitor de signos vitales**	**Ecógrafo**	**Impresora de placas radiográficas**	**Computador Laboratorio**	**Portátil del área de Emergencia**
Tipo de activo		**Información / Datos**	**Hardware**	**Hardware**	**Hardware**	**Hardware**	**Hardware**	**Hardware**
Tipo vulnerabilidades	Hardware	2	3	3	3	3	3	3
	Software	2	2	2	2	2	2	2
	Redes de comunicaciones	2	1	1	1	1	2	2
	Personal	3	2	1	2	2	3	3
	Sitio / Instalaciones	2	2	2	2	2	2	2
	Organización	3	2	2	2	2	3	3
Valoración		2,33	2,00	1,83	2,00	2,00	2,50	2,50

#		14	15	16	17	18	19
Nombre del activo		**Portátil del área de Farmacia**	**Antivirus**	**Servidor HP Elite 8300**	**Red LAN**	**Módem**	**Switch**
Tipo de activo		**Hardware**	**Software**	**Hardware**	**Redes de comunicaciones**	**Redes de comunicaciones**	**Redes de comunicaciones**
Tipo vulnerabilidades	Hardware	3	1	2	3	2	2
	Software	2	3	2	1	1	1
	Redes de comunicaciones	2	2	2	2	2	2
	Personal	3	2	3	2	2	2
	Sitio / Instalaciones	2	1	1	2	1	1
	Organización	3	2	3	2	2	2
Valoración		2,50	1,83	2,17	2,00	1,67	1,67

#		20	21	22	23	24
Nombre del activo		**Registros Contables - Financieros**	**Registros de asistencia del personal**	**Quirófano**	**Página WEB**	**Talento Humano**
Tipo de activo		**Información / Datos**	**Información / Datos**	**Sitio / Instalaciones**	**Software**	**Personas**
Tipo vulnerabilidades	Hardware	2	2	1	2	3
	Software	2	2	1	3	2
	Redes de comunicaciones	1	2	1	2	2
	Personal	2	2	1	2	3
	Sitio / Instalaciones	2	2	2	1	2
	Organización	3	3	2	2	3
Valoración		2,00	2,17	1,33	2,00	2,50

Fuente: Elaborado por el autor

Continuando con la metodología propuesta, se realiza la actividad de identificación de los controles existentes en la Clínica Médica Fértil, sin embargo, por considerar a la Unidad de Gestión de Tecnologías de la Información y Comunicaciones como un servicio general acorde a la Figura 11, no existe procedimientos y evidencias de controles, políticas e información documentada que permita brindar confidencialidad, integridad y disponibilidad a la información generada en la clínica.

Posteriormente, tomando en consideración los resultados de la tabla 27 y tabla 28, se analiza el impacto en caso de materializarse una amenaza y la probabilidad de ocurrencia de un incidente y en la Tabla 29 se calcula el nivel de estimación de riesgo de los activos de la Clínica Médica Fértil, haciendo una multiplicación entre ambos valores calculados en la tabla 27 y tabla 28.

Tabla 29. Nivel de estimación del riesgo a los activos de la Clínica Médica Fértil.

#	**Nombre del activo**	**Tipo de activo**	**Impacto en caso de materializarse la amenaza**	**Probabilidad de que la amenaza explote la vulnerabilidad**	**Estimación del riesgo**
1	Servicios Médicos	Servicios médicos y procesos del negocio	2,77	2,50	6,93
2	Consulta Externa	Servicios médicos y procesos del negocio	2,77	2,50	6,93
3	Historia Clínica	Información / Datos	2,46	2,67	6,56
4	Informe de resultados de pruebas de laboratorio	Información / Datos	2,38	2,50	5,96
5	Informe de tratamientos de fertilidad	Información / Datos	2,38	2,50	5,96

#	Nombre del activo	Tipo de activo	Impacto en caso de materializarse la amenaza	Probabilidad de que la amenaza explote la vulnerabilidad	Estimación del riesgo
6	Informe de pruebas de Endoscopia	Información / Datos	2,38	2,33	5,56
7	Informe de resultados de Ecografías	Información / Datos	2,38	2,33	5,56
8	Torre de Endoscópica	Hardware	2,23	2,00	4,46
9	Monitor de signos vitales	Hardware	2,23	1,83	4,09
10	Ecógrafo	Hardware	2,31	2,00	4,62
11	Impresora de placas radiográficas	Hardware	2,31	2,00	4,62
12	Computador Laboratorio	Hardware	2,38	2,50	5,96
13	Portátil del área de Emergencia	Hardware	2,38	2,50	5,96
14	Portátil del área de Farmacia	Hardware	2,38	2,50	5,96
15	Antivirus	Software	1,85	1,83	3,38
16	Servidor HP Elite 8300	Hardware	2,54	2,17	5,50
17	Red LAN	Redes de comunicaciones	1,85	2,00	3,69
18	Módem	Redes de comunicaciones	2,08	1,67	3,46
19	Switch	Redes de comunicaciones	2,08	1,67	3,46
20	Registros Contables - Financieros	Información / Datos	1,92	2,00	3,85
21	Registros de asistencia del personal	Información / Datos	1,92	2,17	4,17

22	Quirófano	Sitio / Instalaciones	1,62	1,33	2,15
23	Página WEB	Software	2,15	2,00	4,31
24	Talento Humano	Personas	2,38	2,50	5,96

Fuente: Elaborado por el autor

De la Tabla 29, se puede identificar que los activos primarios de la Clínica Médica Fértil tienen una alta estimación del riesgo, por lo cual las políticas de seguridad de la información deben estar dirigidas a mitras dichas amenazas y vulnerabilidades. En este caso debido al enfoque holístico del SGSI en la clínica, se elaborarán políticas de seguridad de la información para los activos de información con nivel de estimación de riesgo de medio y alto conforme a la Tabla 19.

4.6 TRATAMIENTO DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Posterior al análisis de riesgos realizado en la Tabla 29, en la Tabla 30 se elabora el resumen de los controles a implementar en la Clínica Médica Fértil teniendo en consideración de manera global los dominios con sus respectivos objetivos y controles, dichos controles permitirán ser la base para diseñar los proyectos propuestos.

Se debe considerar que, debido a la estructura organizacional de la Clínica Médica Fértil, el encargado de implementar los controles será el responsable de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Tabla 30. Controles a implementar en la Clínica Médica Fértil

Control en la Normativa	Sección
5.	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
5.1	DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

5.1.1	Políticas de seguridad de la información
5.1.2	Revisión de las políticas de seguridad de la información
6.	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
6.1	ORGANIZACIÓN INTERNA
6.1.1	Funciones y responsabilidades de la seguridad de la información
6.1.2	Separación de funciones
6.1.3	Contacto con autoridades
6.1.4	Contacto con grupos de interés especial
6.1.5	Seguridad de la información en la gestión de proyectos
6.2	DISPOSITIVOS MÓVILES Y TELETRABAJO
6.2.1	Política para dispositivos móviles
6.2.2	Teletrabajo
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
7.1	ANTES DE ASUMIR EL EMPLEO
7.1.1	Selección
7 .1.2	Términos y condiciones del empleo
7.2	DURANTE LA EJECUCIÓN DEL EMPLEO
7.2.1	Responsabilidades de la dirección
7.2.2	Concientización, educación y formación en la seguridad de la información
7.2.3	Proceso disciplinario
7.3	TERMINACIÓN O CAMBIO DE EMPLEO
7.3.1	Terminación o cambio de responsabilidades de empleo
8.	GESTIÓN DE ACTIVOS
8.1	RESPONSABILIDAD SOBRE LOS ACTIVOS
8.1.1	Inventario de activos
8.1.2	Propiedad de los activos
8.1.3	Uso aceptable de los activos

8.1.4	Devolución de activos
8.2	CLASIFICACIÓN DE LA INFORMACIÓN
8.2.1	Clasificación de la información
8.2.2	Etiquetado de la información
8.2.3	Manejo de activos
8.3	MANEJO DE LOS MEDIOS
8.3.1	Gestión de medios removibles
8.3.2	Disposición de los medios
8.3.3	Transferencia de medios físicos
9.	CONTROL DE ACCESO
9.1	REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO
9.1.1	Política de control de acceso
9.1.2	Acceso a redes y a servicios en red
9.2	GESTIÓN DEL ACCESO DE USUARIOS
9.2.1	Registro y cancelación del registro de usuarios
9.2.2	Suministro de acceso de usuarios
9.2.3	Gestión de derechos de acceso privilegiado
9.2.4	Gestión de información de autenticación secreta de usuarios
9.2.5	Revisión de los derechos de acceso de usuarios
9.2.6	Retiro o ajuste de los derechos de acceso
9.3	RESPONSABILIDADES DE LOS USUARIOS
9.3.1	Uso de información de autenticación secreta
9.4	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES
9.4.1	Restricción de acceso a la información
9.4.2	Procedimiento de ingreso seguro
9.4.3	Sistema de gestión de contraseñas
9.4.4	Uso de programas utilitarios privilegiados
9.4.5	Control de acceso a códigos fuente de programas

11.	SEGURIDAD FÍSICA Y DEL ENTORNO
11.1	ÁREAS SEGURAS
11.1.1	Perímetro de seguridad física
11.1.2	Controles físicos de entrada
11.1.3	Seguridad de oficinas, recintos e instalaciones
11.1.4	Protección contra amenazas externas y ambientales
11.1.5	Trabajo en áreas seguras
11.1.6	Áreas de despacho y carga
11.2	EQUIPAMIENTO
11.2.1	Ubicación y protección de los equipos
11.2.2	Servicios de suministro
11.2.3	Seguridad del cableado
11.2.4	Mantenimiento de equipos
11.2.5	Retiro de activos
11.2.6	Seguridad de equipos y activos fuera de las instalaciones
11.2.7	Disposición segura o reutilización de equipos
11.2.8	Equipos de usuario desatendidos
11.2.9	Política de escritorio limpio y pantalla limpia
12.	SEGURIDAD DE LAS OPERACIONES
12.1	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES
12.1.1	Procedimientos de operación documentados
12.1.2	Gestión de cambios
12.1.3	Gestión de capacidad
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación
12.2	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS
12.2.1	Controles contra códigos maliciosos
12.3	COPIAS DE RESPALDO
12.3.1	Respaldo de la información

12.4	REGISTRO Y SEGUIMIENTO
12.4.1	Registro de eventos
12.4.2	Protección de la información de registro
12.4.3	Registros del administrador y del operador
12.4.4	Sincronización de relojes
13.	SEGURIDAD DE LAS COMUNICACIONES
13.1	GESTIÓN DE LA SEGURIDAD DE LAS REDES
13.1.1	Controles de redes
13.1.2	Seguridad de los servicios de red
13.1.3	Separación en las redes
13.2	TRANSFERENCIA DE INFORMACIÓN
13.2.1	Políticas y procedimientos de transferencia de información
13.2.2	Acuerdos sobre transferencia de información
13.2.3	Mensajería electrónica
13.2.4	Acuerdos de confidencialidad o de no divulgación
16.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
16.1	GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN
16.1.1	Responsabilidades y procedimientos
16.1.2	Reporte de eventos de seguridad de la información
16.1.3	Reporte de debilidades de seguridad de la información
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos
16.1.5	Respuesta a incidentes de seguridad de la información
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información
16.1.7	Recolección de evidencia
17.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO
17.1	CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

17.1.1	Planificación de la continuidad de la seguridad de la información
17.1.2	Implementación de la continuidad de la seguridad de la información
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
18.	CUMPLIMIENTO
18.1	CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
18.1.2	Derechos de propiedad intelectual
18.1.3	Protección de registros
18.1.4	Privacidad y protección de información de datos personales.
18.1.5	Reglamentación de controles criptográficos
18.2	REVISIONES DE SEGURIDAD DE LA INFORMACIÓN
18.2.1	Revisión independiente de la seguridad de la información
18.2.2	Cumplimiento con las políticas y normas de seguridad
18.2.3	Revisión del cumplimiento técnico

Fuente: Adaptada de la norma ISO/IEC: 27002:2013

En la Tabla 30, se presenta el resumen de los controles a implementar en la Clínica Médica Fértil y que conforme al análisis realizado involucra la mayoría de los controles que contiene la norma ISO/IEC 27002:2013. En el anexo 6 se muestra el proceso de selección de controles para el tratamiento del riesgo.

4.6.1 PROYECTOS PROPUESTOS PARA LA IMPLEMENTACIÓN DEL SGSI EN LA CLÍNICA

La elección de los proyectos propuestos surge a partir del análisis de riesgos y el resumen de los controles a implementar en la Clínica Médica Fértil, priorizando la implementación de los proyectos que aporten mejoras en la seguridad en el menor plazo posible y que las herramientas elegidas sean de código abierto. Cabe

indicar que los proyectos propuestos están dirigidos a mitigar amenazas mencionadas en la Tabla 16 de acuerdo a su codificación.

4.6.1.1 Implantación de políticas de seguridad de la información

Dominios cubiertos: Políticas de seguridad, aspectos organizativos de la seguridad de la información, seguridad ligada a los recursos humanos, gestión de activos, control de acceso, seguridad física y del ambiente, seguridad de las operaciones, seguridad de las comunicaciones, gestión de los incidentes, gestión de la continuidad del negocio y cumplimiento.

Objetivo: Implantar el conjunto de políticas de seguridad de la información propuestos, que dirija el comportamiento de la Clínica Médica Fértil como conjunto, para el cumplimiento del Sistema de Gestión de la Seguridad de la Información.

Descripción: Las políticas de seguridad de la información contienen las directrices y lineamientos que regirán la seguridad de la información en la clínica y las responsabilidades y obligaciones de todos los colaboradores y terceros que tengan acceso a la información de la Clínica Médica Fértil. Así mismo, en el anexo 6 se muestra la documentación generada y socializada a nivel de la Gerencia para el Sistema de Gestión de Seguridad de la Información en la Clínica Médica Fértil.

En las Tablas de la 31 hasta la 43, se detalla las políticas de seguridad de la información propuestos para la implementación del SGSI:

Tabla 31. Políticas de seguridad de la información

1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	
Objetivo	Proporcionar orientación y recibir el apoyo de la Gerencia, para asegurar los activos de información a través de la implementación de controles de seguridad que permitan garantizar la integridad y disponibilidad de los activos de Información de la Clínica Médica Fértil.

Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.

Directrices específicas:

1.1. La Clínica Médica Fértil mantendrá un inventario de sus activos informáticos.

1.2. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones de la Clínica Médica Fértil tendrá un inventario actualizado del software instalado en los equipos de cómputo y prohibirá la instalación de programas ajenos al inventario institucional.

1.3. Todo Software debe responder a una necesidad para su instalación, y debe responder a una licencia de su autor inventariada según cada equipo de cómputo.

Analizar, diseñar e implementar programas de auditoria interna para el sistema de gestión de seguridad informática en los activos de información del área administrativa y de historias clínicas de la Clínica Médica Fértil.

1.4. Todo el personal debe contener una contraseña asignada por la Unidad de Gestión de Tecnologías de la Información y Comunicaciones y esta debe responder a un alto nivel de seguridad, la adjudicación de esta contraseña es responsabilidad del encargado de TIC y es responsabilidad del empleado mantenerla en secreto y no transferirla a terceros.

1.5. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones realizará una revisión periódica según cronograma para verificar descargas o instalaciones no autorizadas de programas en los equipos de la clínica.

1.6. Los empleados no podrán utilizar los activos de información para fines personales.

1.7. Los empleados no podrán utilizar los activos de información para ingresar a servicios de internet diferentes a los requeridos para el cumplimiento de sus funciones.

1.8. Los empleados no deberán utilizar medios de almacenamiento externos diferentes a los que son propiedad de la Clínica Médica Fértil. 1.9. Están prohibidas las copias de correos, bases de datos, archivos administrativos sin previa autorización y la exportación de estos a medios de almacenamiento diferentes a los de la Clínica Médica Fértil. 1.10. Es responsabilidad de los empleados conocer el funcionamiento básico de equipos como escáner, impresoras entre otros, en caso de no conocer obligatoriamente debe solicitar instrucción a la Unidad de Gestión de Tecnologías de la Información y Comunicaciones. 1.11. Está completamente prohibida la manipulación, desensamble, adaptación o modificación de los equipos de cómputo o de radio imagen por parte de empleados, esta función es de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones. 1.12. En el ejercicio de sus funciones los empleados de la Clínica tendrán que considerar específicamente los siguientes factores, que son únicos para el sector salud: derechos y responsabilidades éticas del personal, consentimiento informativo de los pacientes, intercambio de información con fines de investigación y ensayos clínicos, derechos de los pacientes sobre confidencialidad, integridad y disponibilidad de su información.	
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, Gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 32. Políticas de capacitación y concientización de seguridad de la Información

2. POLÍTICAS DE CAPACITACIÓN Y CONCIENTIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Objetivo	Mitigar la indisponibilidad del personal ante incidentes de seguridad de la información a través de procesos de

	capacitación y concientización dirigidos a los funcionarios del área médica y administrativa.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las personas involucradas con historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la clínica tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
2.1. La Clínica Médica Fértil identificará acciones o procedimientos realizados de manera incorrecta con el fin de generar un proceso de capacitación para mejora de procedimientos. 2.2. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones de la Clínica Médica Fértil, identificará acciones o procedimientos realizados por los funcionarios que representen riesgo para los activos de información. 2.3. La Gerencia de la Clínica Médica Fértil generará convocatorias para licitar contratos de capacitación en seguridad informática con expertos las cuales estarán dirigidas a los funcionarios de la clínica. 2.4. Los funcionarios deben asistir a la capacitación y es obligación cumplir con la totalidad de las horas establecidas para tal fin. 2.5. La empresa externa o personal externo que realice la capacitación debe certificar a los funcionarios sobre el cumplimiento y aprobación de la misma.	
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 33. Políticas de confidencialidad

3. POLÍTICAS DE CONFIDENCIALIDAD	
Objetivo	Evitar de manera efectiva la divulgación de la información estableciendo controles y acuerdos de confidencialidad con los funcionarios de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
3.1. La gerencia de la Clínica Médica Fértil, emitirá una circular informativa sobre los perjuicios que representa para la entidad la divulgación de la información dirigida a sus funcionarios en general. 3.2. La gerencia y el departamento de talento humano realizarán una reunión informativa dirigida a todos los funcionarios de la clínica con el fin de notificarles las sanciones legales y laborales a las que habrá lugar en caso de incumplir el acuerdo de confidencialidad, esto se realizará previo a la firma por parte de los funcionarios del acuerdo de confidencialidad. 3.3. El departamento Talento humano emitirá un acuerdo de confidencialidad dirigido a los funcionarios en general la cual debe ser firmada con copia a la hoja de vida donde se establecen los procesos y procedimientos que se deben ejecutar para evitar la divulgación de la información.	
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 34. Políticas de aspectos organizativos de la seguridad de la información

4. POLÍTICAS DE ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
Objetivo	Establecer responsabilidades según la asignación de funciones para mejorar el nivel de seguridad informática en el área médica y administrativa de la Clínica Médica Fértil, así como también a las historias clínicas de los pacientes.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
4.1. La Clínica Médica Fértil tendrá la responsabilidad sobre la seguridad de la información personal de salud y otros datos protegidos relacionados con la salud, haciendo hincapié en la necesidad de una infraestructura de gestión de seguridad de información explícita y robusta. 4.2. Las funciones de cada uno de los funcionarios deben estar en el manual de procedimientos y funciones de la clínica. 4.3. Cada funcionario tendrá asignada una contraseña para acceso a los activos de información, su asignación es responsabilidad de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones de la clínica. 4.4. Los funcionarios deben permanecer dentro de sus dependencias en los horarios establecidos, a excepción de aquellos a quienes les sea otorgado un permiso o se haya cambiado el horario por notificación escrita (físico o digital) de su jefe inmediato con respectiva copia a la oficina de recursos humanos. 4.5. Es responsabilidad de los funcionarios conocer el correcto funcionamiento de los activos informáticos de la Clínica.	

4.6. Es responsabilidad de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones capacitar a los funcionarios con relación al correcto funcionamiento de los activos de información. 4.7. Es responsabilidad de talento humano informar a la Unidad de Gestión de Tecnologías de la Información y Comunicaciones sobre vinculación o desvinculación de los funcionarios para realizar los procesos de asignación de credenciales de acceso o eliminación de las mismas, en caso de desvinculación el departamento de TIC generará un documento del ex funcionario dirigido a talento humano para proceder con liquidación u otros trámites pertinentes. 4.8. Es responsabilidad de los funcionarios de la Clínica, la custodia de sus credenciales de acceso, esta debe ser intransferible y de uso personal, en caso contrario se generar un reporte negativo con respectiva sanción disciplinaria por parte de recursos humanos.	
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 35. Políticas de seguridad ligada a los recursos humanos

5. POLÍTICAS DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
Objetivo	Establecer parámetros para garantizar una adecuada protección de los activos de información de la Clínica Médica Fértil desde el área de recursos humanos.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	

5.1. Se deben definir los perfiles de aspirantes a vacantes de la Clínica Médica Fértil que respondan a los requerimientos para el correcto uso de los activos de información.

5.2. Se deben verificar los antecedentes de los aspirantes y realizar las respectivas validaciones de antecedentes judiciales, fiscales, académicos entre otros que garanticen un uso responsable y confiable de los activos de información.

5.3. Se debe aclarar al nuevo funcionario de la Clínica Médica Fértil sobre los términos y condiciones de contratación al igual que del manejo y uso responsable y eficiente de los activos informáticos.

5.4. El jefe inmediato o compañeros deben informar oportunamente de algún comportamiento sospechoso, incumplimiento de funciones u omisión de las mismas a la oficina de recursos humanos para establecer posibles sanciones o despidos.

5.5. Es responsabilidad de los funcionarios de la Clínica Médica Fértil solucionar inconvenientes dentro de su entorno laboral dentro del cumplimiento de sus funciones asignadas o solicitar apoyo de otros departamentos si así se requiere Responsabilidades de gestión.

5.6. Es responsabilidad de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones realizar una concienciación, educación y capacitación en seguridad de la información de los activos de la información de la Clínica.

5.7. Los funcionarios que sean sorprendidos cometiendo actos que atenten contra el manual de procedimiento o contra la seguridad de los activos de la información en cualquiera de sus clasificaciones tendrán derecho un proceso disciplinario realizado por la oficina de recursos humanos quienes determinaran las sanciones o acciones pertinentes antes el caso.

5.8. La Clínica Médica Fértil incluirá en los términos y condiciones de empleo de los empleados que procesan o procesarán información personal de salud una declaración sobre la responsabilidad del empleado por la seguridad de la información.

5.9. Los términos y condiciones de empleo deben:

	○ a) Incluir la referencia a las penas (sanción) que sean posibles cuando se identifique el incumplimiento de la política de seguridad de la información; ○ b) Velar por que las condiciones relativas a la confidencialidad de la información personal sobre la salud sobrevivan al término del empleo a perpetuidad.
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 36. Políticas de seguridad de gestión de activos

6. POLÍTICAS DE SEGURIDAD DE GESTIÓN DE ACTIVOS	
Objetivo	Definir procesos por los cuales se garantiza la protección adecuada de los activos de información de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
6.1.	La Unidad de Gestión de Tecnologías de la Información y Comunicaciones mantendrá un inventario actualizado con todos los activos de información en sus diferentes clasificaciones en el cual se especificará el responsable del uso y cuidado para el cumplimiento de funciones en el área administrativa y de historias clínicas de la entidad.
6.2.	Cada funcionario se hace responsable del uso adecuado de los diferentes activos informáticos de la Clínica, así como de informar de manera

	oportuna anomalías en su funcionamiento o contenido a la Unidad de Gestión de Tecnologías de la Información y Comunicaciones y su jefe inmediato. 6.3. Cada activo informático físico contará con una placa para su identificación y este debe estar en el lugar destinado para el ejercicio de sus funciones y no podrá ser transferido a otro departamento u oficina salvo autorización escrita (física o digital) del departamento de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones. 6.4. Los activos informáticos no tendrán un uso diferente para el cual han sido adquiridos, queda prohibido la realización de actividades personales diferentes a las requeridas por la Clínica Médica Fértil. 6.5. Los dispositivos médicos que registran o reportan información de los pacientes pueden requerir consideraciones de seguridad especiales en relación con el entorno en el que operan y con las emisiones electromagnéticas que ocurren durante su operación. Tales dispositivos deben ser identificados de manera única. 6.6. Los sistemas de información de salud de la Clínica Médica Fértil están obligados a informar a los usuarios de la confidencialidad de la información de salud personal, a la que se puede acceder desde el sistema y la salida impresa de la información debe ser etiquetada como confidencial cuando contenga información de salud personal.
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 37. Políticas de seguridad de control de acceso

7. POLÍTICAS DE SEGURIDAD DE CONTROL DE ACCESO	
Objetivo	Asegurar un acceso controlado, físico o lógico, a los activos informáticos de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
7.1.	La Clínica Médica Fértil dotará a los funcionarios y contratistas de todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones dentro del área administrativa y en especial de las historias clínicas de los pacientes.
7.2.	Se prohíbe la instalación a la red del hospital de cualquier dispositivo electrónico ajeno al inventario que no sean autorizados por la Unidad de Gestión de Tecnologías de la Información y Comunicaciones de la Clínica Médica Fértil, dentro de los cuales están: teléfonos móviles, computadores portátiles, Tablet, y demás elementos parecidos.
7.3.	La Unidad de Gestión de Tecnologías de la Información y Comunicaciones proveerá a los funcionarios las claves pertinentes para el acceso a los servicios de red y sistemas de información, estas claves son de uso personal e intransferible y es responsabilidad del usuario el manejo que se las mismas, quien trasfiera la contraseña a un tercero se verá involucrado en un proceso disciplinario o legal según el riesgo que represente este acto.
7.4.	Tan solo el personal de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones podrá realizar la instalación de software o hardware en los equipos, servidores e infraestructura de tecnológica y de comunicaciones de la Clínica Médica Fértil.
7.5.	Se debe capacitar y controlar que los funcionarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas,

las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

7.6. Los usuarios son responsables del manejo de contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos del área administrativa, médica y en especial de las historias clínicas de los pacientes.

7.7. Queda prohibida la escritura de las claves dentro de los activos de información, por ejemplo, documentos digitales, correos electrónicos, bases de datos entre otros

7.8. La modificación cambio o reasignación de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato previa solicitud escrita con firma física o firma digital.

7.9. Se impedirá el acceso a cualquier funcionario que haya intentado el ingreso, sin éxito, a un equipo, sistema o archivo informático, en forma consecutiva por tres veces.

7.10. Solo los funcionarios de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones podrán desbloquear el acceso a un funcionario cuya clave haya sido ingresada sin éxito con previo estudio del incidente presentado al funcionario.

7.11. El acceso a los sistemas de información de salud que procesan información de los pacientes estará sujeto a un proceso formal de registro de usuarios.

7.12. Los detalles del registro de los usuarios de los sistemas de información, serán revisados periódicamente para asegurar que sean completos, precisos y que todavía se requiera el acceso.

7.13. Además de la orientación dada por ISO/IEC 27002, se debe prestar especial atención a los usuarios que razonablemente se espera que proporcionen atención médica de emergencia, ya que pueden necesitar acceso a la información personal de salud en situaciones de emergencia, en donde un sujeto de la atención puede no tener acceso.

7.14. La Clínica Médica Fértil debe determinar las responsabilidades de los usuarios, respetar los derechos y las responsabilidades éticas de los

profesionales de la salud, según lo acordado en la ley y aceptado por los miembros de los organismos profesionales de salud. 7.15. Los sistemas de información de salud de la Clínica Médica Fértil que procesan información de los pacientes deberán: ○ a) asegurar que cada paciente pueda ser identificado de manera única dentro del sistema; ○ b) ser capaz de fusionar registros duplicados o múltiples si se determina que múltiples registros para el mismo sujeto de cuidado, han sido creados sin intención o durante una emergencia médica.	
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 38. Políticas de seguridad física y del entorno

8. POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO	
Objetivo	Garantizar la seguridad física y ambiental de los activos de información de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
8.1. El encargado de infraestructura debe garantizar la seguridad estructural de los lugares donde serán instalados los activos de información.	

8.2. La Gerencia de la Clínica Médica Fértil asignara a una empresa de vigilancia un contrato del servicio de seguridad para establecer controles físicos de entrada, seguridad de oficinas, despachos y recursos. 8.3. La Gerencia de la Clínica Médica Fértil en coordinación con la Unidad de Gestión de Tecnologías de la Información y Comunicaciones realizara la adquisición de seguros contra amenazas externas y ambientales que potencialmente pueden afectar a los activos informáticos. 8.4. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones verificara de manera periódica situaciones relacionadas con emplazamiento y protección de equipos, seguridad del cableado y mantenimiento de los equipos generando un reporte de la situación presentada y apoyados por reportes entregados de manera verbal o escrita por parte de los funcionarios del área administrativa y médica. 8.5. En los lugares donde se encuentren almacenados equipos como servidores o conglomeraciones de cableado, se prohíbe fumar, comer o beber; de igual forma se prohíbe el almacenamiento de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio. 8.6. Los cables deben estar marcados para identificar fácilmente los elementos conectados y evitar interrupciones del servicio, también beben existir planos que describan las conexiones del cableado. 8.7. Los funcionarios del área administrativa y médica deberán bloquear sus equipos al momento de levantarse de su puesto de trabajo para evitar alteraciones a la integridad de los activos de información necesarios para el cumplimiento de sus funciones. 8.8. La Clínica Médica Fértil deberá situar una estación de trabajo que permita el acceso a la información personal de salud de una manera que evite la visualización no deseada o el acceso por parte de los sujetos de atención y el público.	
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos

Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 39. Políticas de seguridad de las operaciones

9. POLÍTICAS DE SEGURIDAD DE LAS OPERACIONES	
Objetivo	Asegurar la operatividad de los activos de información de acuerdo a las amenazas a las que se exponen los activos informáticos de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
9.1.	La Unidad de Gestión de Tecnologías de la Información y Comunicaciones garantizará según sus estrategias de seguridad la prohibición de la instalación de programas ajenos a los requeridos por los funcionarios para el cumplimiento misional de la organización.
9.2.	La Unidad de Gestión de Tecnologías de la Información y Comunicaciones establecerá una programación para realizar copias de seguridad, semanales, mensuales, bimestrales y anuales de los activos de información del área administrativa y médica, con el fin de garantizar su disponibilidad, confidencialidad e integridad ante cualquier impacto de amenazas y en concordancia con los requerimientos de la entidad hospitalaria.
9.3.	La Unidad de Gestión de Tecnologías de la Información y Comunicaciones solicitará a las directivas del hospital licitar con empresas especializas al menos 2 veces al año y al menos una vez por semestre pruebas de Pentesting con el fin de gestionar soluciones a posibles vulnerabilidades encontradas en el área administrativa y médica de la Clínica.

Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 40. Políticas de seguridad de las comunicaciones

10. POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES	
Objetivo	Asegurar el tráfico y envío de información en las redes, así como también activos informáticos de la red de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
10.1. Los funcionarios están obligados a utilizar de manera razonable el Internet y con propósitos laborales. 10.2. Todos los funcionarios de la Clínica Médica Fértil tienen prohibido el ingreso a sitios con contenidos contrarios a los propósitos misionales y visiónales de la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la organización, en caso de evidenciarse este comportamiento se procederá con el proceso disciplinario o legal. 10.3. La descarga de archivos de internet que realicen los funcionarios deben responder a propósitos laborales y esto debe hacerse de forma razonable para no afectar el servicio de Internet/Intranet. 10.4. El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para funcionarios cuyos propósitos de sus	

funciones sean facilitar canales de comunicación con la comunidad norte del país que atiende la Clínica Médica Fértil.

10.5. La Clínica Médica Fértil no se hace responsable por información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador, que sea creado a nombre personal, como redes sociales, twitter, facebook, youtube o blogs, ya que se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que haya generado dichas publicaciones en los diferentes medios.

10.6. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones debe llevar un control de ingreso y salida del personal que visita el centro de datos sin excepción e ideara la manera más oportuna y segura de llevar dichos registros atendiendo los parámetros de calidad de la organización.

10.7. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones deberán garantizar que todos los equipos informáticos del área administrativa y médica cuenten con un sistema alterno de respaldo de energía ante las frecuentes fallas eléctricas de la región.

10.8. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones en coordinación con la oficina de recursos humanos programara capacitaciones al personal de aseo sobre la forma en que se debe realizar la limpieza externa de los equipos que hacen parte de los activos de red de la Clínica Médica Fértil.

10.9. Los funcionarios tienen prohibido ingerir alimentos o bebidas cerca de los activos informáticos, también tienen prohibido acceder a ellos bajo los efectos de sustancias psicoactivas.

10.10. Es obligación de los funcionarios de la Clínica reducir la presencia de elementos como papel y cualquiera que pueda representar riesgo de propagación de fuego, se debe mantener organizado el puesto de trabajo.

10.11. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones garantizara que las zonas de disposición de los activos de información estén provistas de:

- Señalización apropiada de todos y cada uno de los diferentes equipos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
- Sistema de refrigeración por aire acondicionado de precisión.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Se debe garantizar el servicio de fluido eléctrico de manera constante y eficaz, se debe instalar en cada uno de los equipos una UPS para mitigar fallas en el servicio de energía.
- Realizar actividades periódicas de soporte y mantenimiento dentro de la red de datos.
- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan y que el montaje de este no afecte la movilidad de usuarios y funcionarios.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas, el montaje de estos no afecte la movilidad de usuarios y funcionarios.
- Las puertas de acceso a lugares donde se encuentren activos de información importantes para el área administrativa y médica deben permanecer cerradas.
- Los equipos informáticos del centro de datos y que manejen información relevante para la organización, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

10.12. La Clínica Médica Fértil para transmitir información personal de salud por medio de mensajes electrónicos deben tomar medidas para garantizar su confidencialidad e integridad. Es importante señalar que la seguridad del correo electrónico y los mensajes instantáneos que contienen información personal sobre la salud pueden incluir procedimientos de encriptación.

10.13. El correo electrónico entre profesionales de la salud que contenga información personal de los pacientes debe ser cifrado en tránsito. Uno de los enfoques es el uso de certificados digitales.

10.14. Crear un registro de auditoría seguro, para cada vez que un usuario acceda, cree, actualice o archiva información de salud personal a través del sistema. El registro de auditoría debe identificar de forma única al usuario, identificar de forma única al paciente, identificar la función realizada por el usuario (creación de registros, acceso, actualización, etc.) y anotar la hora y la fecha en la que el usuario utilizo el sistema.

10.15. Se deberá instalar en los equipos de escritorio y portátiles un software de protección para virus como troyanos, malware, software espía, etc.

10.16. Implementar un sistema de seguridad que permita monitorear el tráfico de red y notificar alguna actividad sospechosa; El sistema debe permitir concentrar la seguridad, centralizar los accesos, generar alarmas de seguridad, traducir direcciones (NAT), monitorear y registrar el uso de Servicios de WWW y FTP, etc.

10.17. Implementar una subred independiente, pero siempre interna, que permita controlar de mejor manera el acceso a los servidores de la clínica.

10.18. Establecer una red de área local que permita agrupar un conjunto de equipos de manera lógica y no física; la red de área local deberá permitir una mayor flexibilidad en la administración y en los cambios de la red.

10.19. Los grupos de equipos que contengan información relevante para la clínica, deberán estar separados del resto de la red interna, que permita disminuir las posibilidades de violaciones de información confidencial.

10.20. Se deberán establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución del Software y/o Sistemas operativos que posee la Clínica Médica Fértil; Para lo cual se debe contar con: a) Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos); b) Backups del Software Base; c) Backups de los Datos (Bases de Datos, passwords, y todo archivo necesario para la correcta ejecución).

Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 41. Políticas de gestión de incidentes de seguridad de la información

11. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
Objetivo	Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
11.1. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones debería establecer las responsabilidades y procedimientos de gestión de incidentes y asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	
11.2. Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible a la Unidad de Gestión de Tecnologías de la Información y Comunicaciones.	
11.3. Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la Clínica Médica Fértil, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	

11.4. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros. 11.5. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que pueda servir como evidencia. 11.6. La Clínica Médica Fértil debe considerar las implicaciones de la recopilación de evidencia con el propósito de establecer negligencia médica.	
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 42. Políticas de aspectos de seguridad de la información de la gestión de continuidad de negocio

12. POLÍTICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	
Objetivo	Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	

12.1. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones debería determinar los 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. 12.2. Se debería incluir dentro del proceso de gestión de continuidad de negocio la continuación de la seguridad de la información para recuperación de desastres. 12.3. La Gerencia de la clínica en conjunto con la Unidad de Gestión de Tecnologías de la Información y Comunicaciones, deberá estructurar la gestión adecuada para mitigar y responder a un evento perturbador usando personal interno con la autoridad, experiencia y competencia necesarias. 12.4. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones debería 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. 12.5. La planificación de la gestión de la continuidad del negocio: debe incluir la planificación de la gestión de la crisis sanitaria, ya que los incidentes principales suelen dar lugar a escasez de personal que limita la capacidad de aplicar con éxito los planes de gestión de la continuidad. Ejemplo de brote de SARS (Síndrome respiratorio agudo y grave).	
Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Tabla 43. Políticas de cumplimiento

13. POLÍTICAS DE CUMPLIMIENTO	
Objetivo	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas

	con seguridad de la información y de cualquier requisito de la Clínica Médica Fértil.
Aplicabilidad	Dirigida a todos los funcionarios y áreas de la Clínica Médica Fértil, incluyendo las historias clínicas de los pacientes y demás activos de información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
13.1. La Gerencia de la clínica en conjunto con la Unidad de Gestión de Tecnologías de la Información y Comunicaciones, deberían identificar y documentar explícitamente todos los requisitos estatutarios, reglamentarios y contractuales para cumplirlos y se mantenerlos actualizados para cada sistema de seguridad de la información. 13.2. Las Historias clínicas de los pacientes se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación y contractuales. 13.3. Se debería asegurar la privacidad y la protección de la información de los pacientes, como se exige en la legislación y la reglamentación pertinentes. 13.4. La Unidad de Gestión de Tecnologías de la Información y Comunicaciones debería revisar periódicamente los sistemas informáticos administrativos y médicos para determinar el cumplimiento con las políticas y normas de seguridad de la información. 13.5. La Clínica Médica Fértil debe manejar el consentimiento informativo de los pacientes. Siempre que sea posible, se debe obtener el consentimiento informativo de los pacientes antes de que la información personal de salud sea enviada por correo electrónico, por fax o comunicada por conversación telefónica, o de otra forma divulgada a las partes externas a la organización del sector salud.	

Responsables	Unidad de Gestión de Tecnologías de la Información y Comunicaciones, funcionarios del área administrativa, médica y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Elaborado por el autor

Responsable: Gerencia de la Clínica y responsable de Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Amenazas a mitigar: A1, A3, A5, A6, A7, A8 y A9.

4.6.1.2 Instalación de un sistema de backup y recuperación

Dominios afectados: Políticas de seguridad, seguridad de las operaciones, seguridad de las comunicaciones, gestión de los incidentes, gestión de la continuidad del negocio y cumplimiento.

Objetivo: Implementar un sistema centralizado de gestión de tareas de creación, recuperación y almacenamiento de copias de seguridad, tanto de servidores, como de carpetas compartidas y de aplicaciones de negocio (web corporativa, bases de datos, aplicación de contabilidad).

Descripción: Además de la implantación de las políticas de seguridad, uno de los puntos más críticos para la Clínica Médica Fértil es asegurar la continuidad de negocio y evitar pérdidas de datos médicos. Una herramienta de respaldo de información es Bacula, como uno de los principales sistemas código abierto que permite generar respaldos de la información empresarial, acorde a investigaciones realizadas por (open source, 2018) & (Linuxtechi, 2018).

Bacula Community, es una colección de herramientas de respaldo, capaces de cubrir las necesidades de respaldo de equipos bajo redes IP. Se basa en una "arquitectura cliente-servidor que resulta eficaz y fácil de manejar, dada la amplia gama de funciones y características que brinda; copiar y restaurar ficheros dañados o perdidos" (Bacula.org, 2018). Además, debido a su desarrollo y estructura modular, Bacula Community se adapta tanto al uso personal como profesional.

Entre las características de Bacula Community están:

- La comunicación entre componentes puede cifrarse.
- Es capaz de manejar varios volúmenes físicos (encadenados) si los datos no caben en uno, y recordar e identificar cuál es el correcto. Por ejemplo, cintas DAT y DVDs.
- Administración centralizada.
- Respaldo y recuperación en red.
- Plataforma heterogénea (Linux, Mac OS X, Unix, Windows).
- Diferentes tipos de almacenamiento (Tape, disk, USB, CD/DVD, disco duro).
- Fácil ubicación de la información respaldada.
- Recuperación en cualquier punto del tiempo.
- Maneja hasta 2000 equipos.

Responsable: Gerencia de la Clínica y responsable de Unidad de Gestión de Tecnologías de la Información y Comunicaciones

Amenazas a mitigar: A5, A6, A7, A8 y A9.

4.6.1.3 Implementación y migración de dispositivos de seguridad de red (router y firewall)

Dominios afectados: Políticas de seguridad, aspectos organizativos de la seguridad de la información, seguridad ligada a los recursos humanos, gestión de activos, control de acceso, seguridad física y del ambiente, seguridad de las operaciones, seguridad de las comunicaciones, gestión de los incidentes, gestión de la continuidad del negocio y cumplimiento

Objetivo: Implementar un firewall y migrar el router actual debido a que no ofrece las funcionalidades de seguridad y prestaciones necesarias para dar servicio a todo el personal y pacientes que integran la Clínica Médica Fértil.

Descripción: Se plantea reubicar en la topología de red actual al dispositivo Huawei HG532 provisto por CNT E.P. e implementar un router/firewall que permita gestionar el correcto servicio de red de datos y seguridad informática en la Clínica. El equipo debe tener la capacidad de doble WAN, creación de redes de área local virtuales (VLAN), gestión de políticas de firewall, creación de túneles VPN, traducción de direcciones de red (NAT) y gestión de puntos de acceso Wifi. A través del presente proyecto se plantea una nueva topología de red para la Clínica Médica Fértil como se muestra en la Figura 19.

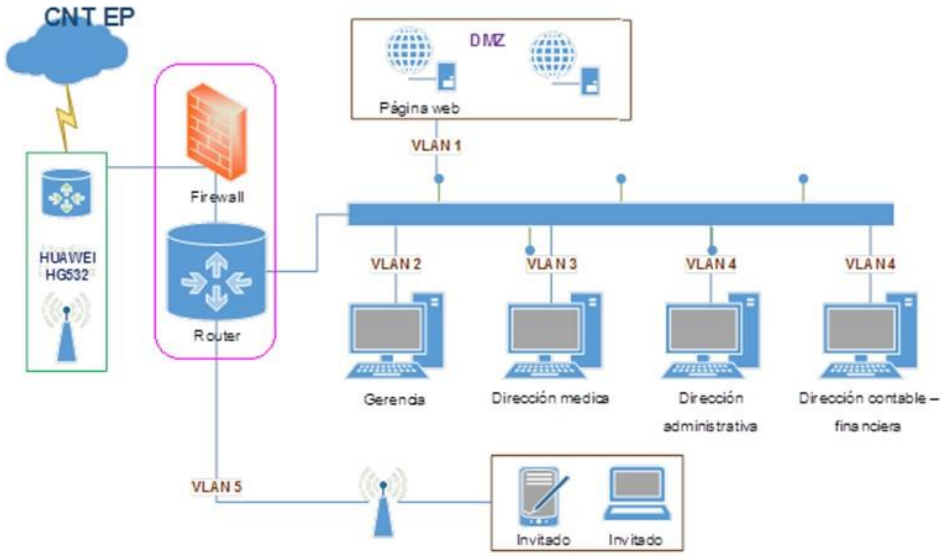


Figura 18 Topología de Red recomendada para la Clínica Médica Fértil

Fuente: Elaborado por el autor

Responsable: Gerencia de la Clínica y responsable de Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Amenazas a mitigar: A5, A6, A7, A8 y A9.

4.6.1.4 Implementación de sistema de helpdesk y tratamiento de incidencias de tecnologías de la información y comunicaciones.

Dominios afectados: Políticas de seguridad, aspectos organizativos de la seguridad de la información, seguridad ligada a los recursos humanos, gestión de activos, control de acceso, seguridad de las operaciones, Seguridad de las comunicaciones, gestión de los incidentes, gestión de la continuidad del negocio y cumplimiento.

Objetivo: Implementar un sistema Helpdesk o de tratamiento de incidencias y peticiones de servicio para la Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Descripción: Es necesario implementar un sistema que permita hacer un tratamiento correcto de las incidencias y peticiones de servicio de los empleados y pacientes de la Clínica Médica Fértil. Acorde a un estudio realizado por (Cloudsmallbusinessservice.com, 2018) ubica a OTRS Community Edition entre los 10 mejores software de asistencia de Mesa de Ayuda código abierto del año 2018.

OTRS (Open-source Ticket Request System), es un software para gestión de solicitudes mediante el mecanismo de tickets, el cual permite a los usuarios tener un único canal de comunicación para todas las solicitudes, y a los agentes responder a un alto volumen de casos de clientes de forma rápida, competente y, sobre todo, transparente. La aplicación permite gestionar solicitudes tanto vía web como mediante correo electrónico, e inclusive desde dispositivos móviles. Entre las principales características de OTRS están:

- Fácil manejo con un navegador Web.
- Soporte para varios lenguajes.
- Una interfaz Web para manejar las peticiones del cliente por parte de los empleados / agentes a través de la Web se integra.
- Soporte para archivos adjuntos de correo.
- Correos de notificaciones para los agentes sobre nuevos tickets, así como el seguimiento de los tickets abiertos.
- Definición del control de acceso para los tickets.
- Cambiar y fijar prioridades de un ticket.
- Control y seguimiento sobre todas las incidencias de cada ticket (cambios de estados, respuestas, notas, etc.)
- OTRS se ejecuta sobre cualquier sistema operativo (Linux, Solaris, FreeBSD, OpenBSD, Mac OS 10.x, Windows).
- Autenticación de clientes por medio de la base de datos.
- Soporte para diferentes bases de datos, por ejemplo, MySQL, PostgreSQL, Oracle.

De igual manera, existe herramientas que pueden complementarse con OTRS como es OCS Inventory (Open Computer and Software Inventory Next Generation), que es un software libre que permite a los administradores de TI gestionar el inventario de sus activos de TI. La integración entre las dos herramientas permitiría tener un inventario de hardware y software totalmente actualizado y automático de la Clínica Médica Fertil. El Inventario de OCS puede utilizarse para alimentar la base de datos de OTRS y obtener una potente solución de gestión de activos de TI.

Responsable: Gerencia de la Clínica y responsable de Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Amenazas a mitigar: A5, A6, A7, A8 y A9.

4.6.1.5 Implementación de un sistema de gestión eventos e información de seguridad la información

Dominios afectados: Gestión de activos, control de acceso, seguridad de las operaciones, Seguridad de las comunicaciones, gestión de los incidentes, gestión de la continuidad del negocio y cumplimiento.

Objetivo: Implementar un sistema de gestión eventos e información de seguridad la información que permita el monitoreo general de la infraestructura, obtener reportes en tiempo real de lo que está sucediendo en la red de datos de la Clínica Médica Fértil, para analizar las anomalías y ayuden al responsable de la Unidad de TIC en la toma de decisiones en el campo dela seguridad de la información y realizar correcciones oportunas.

Descripción: La seguridad informática necesita de una herramienta que ayude al responsable de la unidad de TIC, en la toma de decisiones oportunas en la información y servicios críticos que favorecen el desarrollo de la Clínica y su buen funcionamiento.

Un sistema de gestión eventos e información de seguridad (SIEM) es una tecnología que “proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware, software y en general por cualquier dispositivo de red” (AlienVault.Inc, 2018). Dado que el proyecto se centra en herramientas de código abierto y que se ajuste a la norma ISO/IEC27001:2013. En la Figura 20 se muestra un estudio realizado por la consultora Gartner, que ofrece una comparación de los productos SIEM más importantes que ofrece el mercado tanto del denominado código abierto como propietarios.

Figura 19 Cuadrante Magico Gartner SIEM

Fuente: Tomado de (Gartner, 2018)

Conforme la Figura 20, se observa que entre los productos analizados por la consulta Gartner destaca el único producto de código abierto OSSIM de AlienVAult.

OSSIM, es un acrónimo para Open Source Security Information Management, en español podría traducirse como: Herramienta de Código Abierto para la Gestión de Seguridad de la Información. OSSIM se entiende que como un conjunto de herramientas unidas en un solo programa que facilita el análisis, visualización y la gestión de manera centralizada de los eventos que ocurren en los diferentes componentes de la infraestructura tecnológica de la organización, obteniendo de esta forma mayor efectividad a la hora del monitoreo y de encontrar errores u vulnerabilidades en la seguridad de la red. Las principales funcionalidades de OSSIM son: Descubrimiento de activos e inventario, Gestión de vulnerabilidades, Detección de intrusiones, Monitorización del comportamiento de la red, presenta informes ejecutivos y técnicos, es gratuito.

Responsable: Gerencia de la Clínica y responsable de Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Amenazas a mitigar: A5, A6, A7, A8 y A9.

4.6.1.6 Implementación de una herramienta integrada de monitoreo de redes

Dominios afectados: Seguridad de las operaciones, seguridad de las comunicaciones, gestión de los incidentes, gestión de la continuidad del negocio y cumplimiento.

Objetivo: Implementar un sistema de monitoreo de red que permita observar el comportamiento de la infraestructura de comunicaciones de la Clínica Médica Fértil garantizando la detección inmediata de incidentes con el fin de mantener la conectividad y servicios informáticos.

Descripción: Multi Router Traffic Grapher (MRTG) es una herramienta, escrita en C y Perl por Tobias Oetiker y Dave Rand, que “se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera los resultados en archivos HTML con gráficos, que proveen una representación visual de este tráfico” (Oetiker, 2018)

MRTG utiliza SNMP (Simple Network Management Protocol) o protocolo simple de administración de red para recolectar los datos de tráfico de un determinado dispositivo (dispositivos encaminamiento o servidores), por tanto, es requisito contar con al menos un sistema a supervisar con SNMP funcionando y con dicho servicio correctamente configurado, conforme los proyectos propuestos involucra la implementación de un firewall/router el cual habilita realizar este tipo de monitoreo.

La aplicación de MRTG consiste es una serie de scripts escritos en lenguaje PERL que usan el protocolo de red SNMP (Simple Network Management Protocol) para leer los contadores de tráfico que están ubicados en los conmutadores (switch)

o los encaminadotes (routers) y mediante sencillos y rápidos programas escritos en lenguaje C, crea imágenes en formato PNG que representa el estado del tráfico de nuestra red. Estos gráficos los inserta en una página web que se puede consultar mediante cualquier navegador, entre las principales funcionalidades de MRTG se tiene:

- Monitoreo de Equipos con conexiones a redes IP
- Notificación de Alarmas y umbrales vía SMTP y SMS
- Monitoreo de Servicios de TI
- Lectura de comunidades SNMP
- Acceso a la información de monitoreo vía Web
- Soporta servidores Web con Apache e Microsoft IIS
- Flexibilidad en la configuración del portal con desarrollo ASP y PSP
- Capacidad de almacenamiento de los log para históricos

Responsable: Gerencia de la Clínica y responsable de Unidad de Gestión de Tecnologías de la Información y Comunicaciones.

Amenazas a mitigar: A5, A6, A7, A8 y A9.

Como proyectos complementarios los propuestos, se debe considerar dos proyectos adicionales el primero está relacionado con la adquisición e implementación de un antivirus, sin embargo, debido a los parámetros planteados en el ítem 4.6.1 sobre elegir herramientas que sean de código abierto esta elección estará a consideración del responsable de la unidad de Tecnologías de la información. Puesto que analizar el mejor antivirus de código abierto aplicable al proyecto no se encuentra dentro del alcance del trabajo de titulación. Como un segundo proyecto a considerar se encuentra el relacionado con la gestión de usuarios y equipos conectados a la red de la clínica, la herramienta debe contener un sistema centralizado y estandarizado que automatice la gestión de red, esto es: información de usuarios, seguridad y distribución de recursos; Sin embargo, considerando el número reducido de computadoras de escritorio y de portátiles

conforme al inventario realizado en la tabla 11. Se Prioriza la implementación de los proyectos descritos anteriormente que permita brindar confidencialidad, integridad y disponibilidad a la información de los empleados y pacientes de la Clínica.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El Ecuador cuenta con un amplio marco legal y normativo relacionado al derecho a la salud y confidencialidad de la información, siendo la Constitución de la República del año 2008 uno de los principales instrumentos legales para garantizar la confidencialidad de la información de los pacientes que se generen a través de la utilización de los diferentes tipos de servicios de salud del país.

- Mediante la investigación se logró realizar una revisión bibliográfica de carácter analítico sobre leyes y regulaciones de confidencialidad de la información para el sector Salud del Ecuador y las normas ISO 27799:2008, ISO/IEC 27002:2015 e ISO/IEC 27005:2013; a través del cual permitió establecer los lineamientos adecuados para el desarrollo del modelo de Sistema de Gestión de Seguridad de la Información para la Clínica Médica Fértil.

- El uso de las Tecnologías de la Información dentro de las organizaciones del sector salud ha proporcionado grandes beneficios para el sector; sin embargo, esto también ha generado nuevos desafíos. Uno de estos desafíos, está relacionado con proteger la información personal sobre la salud. Es por esto que, para reducir las amenazas hasta un nivel de riesgo asumible por la organización, se implementan programas integrales de Seguridad de la Información basados en estándares y buenas prácticas como las normas ISO/IEC 27000 para la Gestión de Seguridad de la Información.

- Por su naturaleza, las organizaciones de salud operan en un entorno donde los trabajadores, pacientes, visitantes y público en general transitan a través de los activos de información y áreas operativas. Por lo cual la utilización de la norma ISO 27799:2008 que contiene un conjunto de controles específicos

para la gestión de la Seguridad de la Información en organizaciones del sector salud, garantiza un nivel mínimo de seguridad acorde a las circunstancias de la organización y manteniendo la confidencialidad, integridad y disponibilidad de la información de los pacientes.

- El Sistema de Gestión de Seguridad de la Información propuesto al tomar como referencia las normas ISO/IEC 27000, se convierte en una guía para las instituciones del sector salud, que tengan interés en realizar el proceso de certificación.

- El uso de estándares, modelos y buenas prácticas enfocados a la seguridad de la información, permitió diseñar un modelo de Gestión de Seguridad para la Clínica Médica Fértil que garanticen la confidencialidad, integridad y disponibilidad de la información de los pacientes.

- Dentro del levantamiento de información de la Clínica Médica Fértil, se identificó que la inexistencia de políticas, procedimientos y herramientas informáticas no permitía tener un inventario actualizado de activos de información, sobre el cual realizar el análisis de riesgos.

- A través de la investigación se logró realizar el levantamiento de información de la situación actual de la Clínica Médica Fértil, que permitieron identificar los escenarios de riesgos lógicos, físicos y de índole ambiental que comprometan la seguridad de la información mediante la metodología de la norma ISO/IEC 27005:2008, a través del cual se pudo constatar la inexistencia de controles de seguridad de la información.

- La validación del modelo de Sistema de Gestión de Seguridad de la Información en la Clínica Médica Fértil permitió identificar los activos de información de la clínica, así como también realizar una evaluación de riesgos, para finalmente proponer proyectos de seguridad de la información que proporcione confidencialidad, integridad y disponibilidad a la información de los pacientes y empleados.

- Dentro del proceso de análisis de riesgos realizado en la Clínica Médica Fértil mediante la aplicación de la norma ISO/IEC 27005:2008 se pudo evidenciar que los activos de información que mayor riesgo de pérdida de confidencialidad, integridad y disponibilidad tienen son los servicios médicos y procesos de negocio, información y datos, hardware y personas.

- Los proyectos propuestos de seguridad informática realizada en el presente trabajo, establecen un avance en cuanto a la gestión de seguridad de la información de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones de la Clínica Médica Fértil, debido que permitirá realizar una reducción de riesgos y vulnerabilidades sobre los activos e información.

5.2 RECOMENDACIONES

- Se recomienda realizar la implementación de los controles y políticas de seguridad de la información en la Clínica Médica Fértil propuestas en la presente investigación, para brindar confidencialidad, integridad y disponibilidad a la información de los pacientes.

- Es de vital importancia que se defina formalmente un comité de Seguridad de la Información dentro de la Clínica Médica Fértil, órgano que debería encargarse del proyecto de implementación del SGSI y que deberá contar con el apoyo de la Gerencia de modo que se facilite el acceso a la información de todas las áreas pertinentes.

- Se recomienda que el equipo designado para la implantación del Sistema de Gestión de Seguridad de la Información posea un amplio conocimiento en las normas ISO/IEC 27001:2013, ISO/IEC 27005:2008, ISO/IEC 27002:2013 e ISO 27799:2008 o en su defecto realizar un proceso de capacitación continua al personal de la clínica para facilitar el entendimiento y la familiarización de las normas utilizadas.

- De manera complementaria a la implementación del SGSI en la Clínica Médica Fértil se recomienda que la institución realice la implementación de un Sistema de Gestión de Continuidad de Negocios, enfocado en establecer planes a seguir durante un escenario que afecte la operativa de la Clínica. Este sistema de gestión y el SGSI permitirán tener un mayor nivel de protección no sólo sobre la información si no sobre los procesos críticos de la Clínica, contando con planes de contingencia que aseguren su recuperación luego de ser afectados por un escenario de desastre o incidente interno.

- Para la certificación formal de una Institución del sector salud sea Pública o Privada en la Normas ISO 27000 se debe tomar en cuenta la norma ISO/IEC 27006, puesto que en esta norma se encuentran los requisitos para la acreditación de entidades y certificación de sistemas de gestión de la seguridad de la información.

- Posterior a la implementación del Sistema de Gestión de Seguridad de la Información en el caso de estudio, se debe realizar una auditoría de las políticas de seguridad para verificar el grado de cumplimiento y así establecer el grado de reducción de riesgos y vulnerabilidades.

BIBLIOGRAFIA

ESET Smart Security. (2016). *the state of cybersecurity in healthcare organizations in 2016.* Recuperado el 13 de Diciembre de 2018, de https://cdn2.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf

HIPAA Journal. (2018). *Largest Healthcare Data Breaches of 2017*. Recuperado el 25 de Enero de 2018, de https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/

AlienVault.Inc. (2018). *Unified Security for Threat Detection*. Obtenido de https://www.alienvault.com/

Areitio, J. (2008). *Seguridad de la información. Redes, Informática y Sistemas de Información.* Paraninfo.

Bacula.org. (15 de Julio de 2018). *The Bacula Open Source Network Backup Solution*. Obtenido de http://blog.bacula.org/

Bell , G., & Ebert , M. (2015). *Health care and cyber security. Volumen 1.* (Vol. 1st). Recuperado el 02 de Octubre de 2016, de https://www.kpmg.com/LU/en/IssuesAndInsights/Articlespublications/Documents/cyber-health-care-survey-kpmg-2015.pdf

Calderón, M. (2017). *ISO/IEC 27001*. Recuperado el 10 de Enero de 2018, de https://archivoshistoriapatrimonio.blogspot.com/2017/12/isoiec-27001.html

Camelo, L. (10 de Marzo de 2018). *Seguridad de la Informacion en Colombia*. Obtenido de http://seguridadinformacioncolombia.blogspot.com/2010/08/alineando-cobit-41-itil-v3-e-iso-27002.html

Clínica Médica Fértil. (2013). *Clínica Médica Fértil - Especialidades Clínico Quirúrgicas y Biología de la Reproducción*. Recuperado el 05 de Enero de 2018, de http://www.clinicamedicafertil.com.ec/

Cloudsmallbusinessservice.com. (08 de Febrero de 2018). *Top 14 Best Free and Open Source Help Desk Software 2018*. Obtenido de https://cloudsmallbusinessservice.com/blog/top-14-best-free-and-open-source-help-desk-software.html

Código Orgánico Integral Penal. (2014). Cuenca: Editorial Jurídica del Arco Ediciones. Recuperado el 19 de Marzo de 2018, de https://oig.cepal.org/sites/default/files/2014_ecu_codpenal.pdf

Congreso Nacional. (2004). *Ley Orgánica de Transparencia y Acceso a la Información Pública.* Ecuador. Recuperado el 17 de Noviembre de 2016, de http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/04/ley_organica_de_transparencia_y_acceso_a_la_informacion_publica.pdf

Congreso Nacional. (2006). *ley orgánica de salud.* Recuperado el 10 de Noviembre de 2017, de http://www.ambiente.gob.ec/wp-content/uploads/downloads/2012/09/salud.pdf

Constitución de la República del Ecuador. (2008). Recuperado el 07 de Octubre de 2017, de http://www.pucesi.edu.ec/web/wp-content/uploads/2016/04/Constituci%C3%B3n-de-la-Rep%C3%BAblica-2008.pdf

El comercio. (2017). *Los ciberataques a la salud se incrementaron en un 600%*. Recuperado el 12 de Diciembre de 2018, de http://www.elcomercio.com/guaifai/ciberataques-hospitales-informacion-seguridad-datospersonales.html

Flores Ma. & Castillo A. (8 de Mayo de 2012). Una mirada desde la sociedad civil a la Gobernanza del Sistema Nacional de Salud. *Esfera Publica, 4*, 6. Recuperado el 2016 de Noviembre de 2016, de http://www.grupofaro.org/content/una-mirada-desde-la-sociedad-civil-la-gobernanza-del-sistema-nacional-de-salud

Gartner, I. (2018). *Reviews for Security Information and Event Management (SIEM)*. Obtenido de https://www.gartner.com/reviews/market/security-information-event-management

Gómez, L., & Fernández, P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.* Madrid: AENOR.

Healthcare IT News. (2017). *The biggest healthcare breaches of 2017*. Recuperado el 12 de Enero de 2018, de http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=2

HealthITSecurity. (2017). *Healthcare Ransomware Attacks Contribute to 2017 Top Data Breaches*. Recuperado el 13 de Enero de 2018, de https://healthitsecurity.com/news/healthcare-ransomware-attacks-contribute-to-2017-top-data-breaches

ISACA. (2012). *COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa* (ISBN 978-1-60420-282-3 ed.). Estados Unidos de America.

ISO. (2008). *27799 - Health informatics - Information security management in health using ISO/IEC 27002* (1st ed.).

ISO 27000.ES. (2005). *ISO27000.ES*. Recuperado el 17 de Noviembre de 2017, de http://www.iso27000.es/sgsi.html

ISO/IEC. (2005). *27001 Information Technology - Security Techniques - Information Security Management Systems – Requirements.*

ISO/IEC. (2008). *27005 Information technology - Security techniques - Information security risk management.*

ISO/IEC. (2013). *27001 Information Technology - Security Techniques - Information Security Management Systems – Requirements.*

ISO/IEC. (2013). *27002 - Técnicas de Seguridad de las Tecnologías de la Información: Código de Prácticas para la Gestión de la Seguridad de la Información.*

iso27000.es. (2012). *El portal de ISO 27001 en Español*. Recuperado el 24 de Enero de 2018, de http://www.iso27000.es/certificacion.html

IT Training Zone. (2016). *ITSM Zone*. Recuperado el 20 de Diciembre de 2017, de https://www.robh.eu/wp-content/uploads/2013/02/ITILonapage.pdf

Linuxtechi. (28 de Febrero de 2018). *Top 12 Open Source Backup Tools for Linux Systems*. Obtenido de https://www.linuxtechi.com/top-12-open-source-backup-tools-linux-systems/

Ministerio de Salud Pública. (2006). *Ley de Derechos y Amparo al Paciente.* Ecuador. Recuperado el 16 de Noviembre de 2016, de http://www.salud.gob.ec/wp-content/uploads/downloads/2014/09/Normativa-Ley-de-Derechos-y-Amparo-del-Paciente.pdf

Ministerio de Salud Pública. (2012). Ley Orgánica del Sistema Nacional de Salud. Recuperado el 07 de Octubre de 2016, de http://www.salud.gob.ec/wp-content/uploads/downloads/2014/09/Reglamento-a-la-Ley-Org%C3%A1nica-de-Salud.pdf

Ministerio de Salud Pública. (2015). *Reglamento de Información Confidencial en el Sistema Nacional de Salud.* Quito.

Oetiker, T. (2018). *The Multi Router Traffic Grapher*. Obtenido de https://oss.oetiker.ch/mrtg/

open source. (6 de Febrero de 2018). *Top Three Open Source Data Backup Tools*. Obtenido de https://opensourceforu.com/2018/02/top-three-open-source-data-backup-tools/

Organización Internacional de Normalización. (2017). *ISO Survey of certifications to management system standards - Full results*. Recuperado el 25 de Enero de 2018, de https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

Secretaría Nacional de la Administración Pública. (2013). Esquema Gubernamental de Seguridad de la Información.

Secretaría Nacional de la Administración Pública. (En línea). *La Secretaría*. Recuperado el 23 de Diciembre de 2016, de http://www.administracionpublica.gob.ec/la-secretaria/

Servicio de Acreditación Ecuatoriano. (2018). *Acreditación*. Obtenido de http://www.acreditacion.gob.ec/

Tripwire. (2018). *Another Indiana Hospital Hit by Ransomware Attack*. Recuperado el 20 de Enero de 2018, de https://www.tripwire.com/state-of-security/latest-security-news/another-indiana-hospital-hit-ransomware-attack/

UNIT- Instituto Uruguayo de Normas Técnicas. (2015). *Normas Técnicas*. Recuperado el 15 de Noviembre de 2017, de http://www.unit.org.uy/normalizacion/sistema/27000/

Van Bon, J., & Van Der Veen, A. (2011). *Fundamentos de ITIL - Volumen 3.* Amersfoort: Haren Publishing.

ANEXOS

Anexo 1. Recolección de información “Grupo focal”

Moderador: Alexandra Enríquez.

Objetivo: Conformar un cuadro de la situación actual de la Clínica Médica Fértil permitiendo obtener un diagnóstico preciso para tomar decisiones acordes con los objetivos y políticas de la seguridad de la información.

Preguntas

1. ¿Para la implementación de proyectos informáticos dentro de la Clínica Médica Fértil existe apoyo de la alta dirección?
2. A su consideración, ¿existe trabajo en equipo entre las diferentes áreas de la Clínica para la realización de proyectos?
3. Por parte del personal de la Unidad de TIC, ¿existe disponibilidad para auto capacitación?
4. A su consideración, ¿el soporte técnico y tiempo de respuesta por la Unidad de TIC es satisfactorio?
5. ¿Existe un uso correcto de los recursos informáticos por parte del personal de la Clínica?
6. Considera usted que obtener una certificación NTE INEN - ISO/IEC 27001:2013 para la Clínica Médica Fértil, ¿mejoraría la confidencialidad, integridad y disponibilidad de la información de los pacientes y el personal?
7. ¿Existe documentación sobre solución a incidentes relacionados con seguridad de la información de la Clínica Médica Fértil?
8. ¿Considera usted importante la existencia de políticas y procedimientos sobre seguridad de la información para resguardar la información de la clínica?
9. ¿Tiene conocimiento sobre el impacto en las instituciones del sector salud al sufrir ataques o infiltraciones de seguridad de la información?

Resultado:

Fortalezas	**Oportunidades**
• Apoyo de la Alta Dirección. • Posibilidad de trabajo en equipo con las diferentes áreas de la Clínica para la realización de proyectos. • Disponibilidad para auto capacitación del personal de la Unidad de TIC. • Centralización de las actividades de la Unidad de TIC, permitiendo que el soporte técnico y tiempo de respuesta sea más eficaz. • Uso correcto de los recursos informáticos por parte del personal de la Clínica	• Obtener la certificación NTE INEN - ISO/IEC 27001:2013. • Alinear la tecnología de información con el modelo del negocio de la Clínica. • Mejorar la imagen de la Clínica con los Clientes, en temas relacionados al manejo, confidencialidad y disponibilidad de la información.
Debilidades	**Amenazas**
• Procesos internos de la Clínica no posee documentación, sobre solución a incidentes relacionados con seguridad de la información. • Recursos humanos de la clínica tiene desconocimiento sobre los beneficios de implementar políticas y procedimientos de seguridad de la información. •Inexistencia de políticas y procedimientos sobre seguridad de la información para resguardar la información de la clínica. • Considerar a la Unidad de TIC como un servicio general de la clínica. •Costos elevados al aplicar los controles y herramientas de seguridad apropiados.	• Dificultad al aplicar los controles o mecanismos de seguridad apropiados por parte de los clientes. • Insatisfacción de los clientes respecto a los nuevos controles y herramientas de seguridad de la información. • La Clínica sea objeto de ataques o infiltraciones de seguridad de la información.

Ing. Jason Cervantes	Ing. Yomaira Guerrón	Dra. Sara Navarro
DEP. TIC	DEP. ADMIN-FINANC	GERENTE

clínica médica fértil
IMBACLINIC CIA. LTDA.
RUC. 1091747762001

Anexo 2. Lista de amenazas comunes

La siguiente tabla presenta ejemplos de amenazas comunes conforme la Norma ISO/IEC 27005:2008. Ellas pueden ser deliberadas, accidentales o ambientales (naturales) y pueden dar como resultado, por ejemplo, daño o pérdida de los servicios esenciales. Para cada uno de los tipos de amenazas, la siguiente lista indica los casos en que D (deliberadas), A (accidentales) y E (ambientales) son pertinentes. La letra D se utiliza para todas las acciones deliberadas que tienen como objetivo los activos de la información, A se utiliza para las acciones humanas que pueden dañar accidentalmente los activos de información y E se utiliza para todos los incidentes que no se basa en las acciones humanas. Los grupos de amenazas no están en orden de prioridad.

TIPO	**AMENAZA**	**ORIGEN**
Daño fisico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha subrepticia	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D

	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Se recomienda poner atención particular a las fuentes de amenazas humanas. Éstas se desglosan específicamente en la siguiente Tabla:

Fuente de amenaza	**Motivación**	**Acciones amenazantes**
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería social • Intrusión, accesos forzados al sistema • Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador (por ejemplo, espionaje cibernético) • Acto fraudulento (por ejemplo, repetición, personificación, interceptación) • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los	• Bomba/terrorismo • Guerra* (warfare) de información • Ataques contra el sistema (por ejemplo, negación distribuida del servicio)

	medios de comunicación	• Penetración en el sistema • Manipulación del sistema
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja Política • Explotación económica • Hurto de información • Intrusión en la privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
trusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (por ejemplo, error en el ingreso de los datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información de propietario • Abuso del computador • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malintencionado (por ejemplo, virus, bomba lógica, caballo troyano) • Venta de información personal • Errores* (bugs) en el sistema • Sabotaje del sistema • Acceso no autorizado al sistema

Anexo 3. Lista de vulnerabilidades

Conforme a la Norma ISO/IEC 27005:2008, la siguiente Tabla presenta tipos de vulnerabilidades en diversas áreas de seguridad, e incluye ejemplos de amenazas pueden explotar estas vulnerabilidades la lista puede brindar ayuda durante la evaluación de las amenazas y vulnerabilidades, con el fin de determinar los escenarios pertinentes de incidente.

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Falta de pruebas de auditoría	Abuso de los derechos

	Distribución errada de los derechos de acceso	Abuso de los derechos
	Software de distribución amplia	Corrupción de datos
	Utilización de los programas de aplicación a los datos errados en términos de tiempo	Corrupción de datos
	Interfase de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
Software	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Falta de control eficaz del cambio	Mal funcionamiento del software
	Descarga y uso no controlados de software	Mal funcionamiento del software
	Falta de copias de respaldo	Mal funcionamiento del software
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo

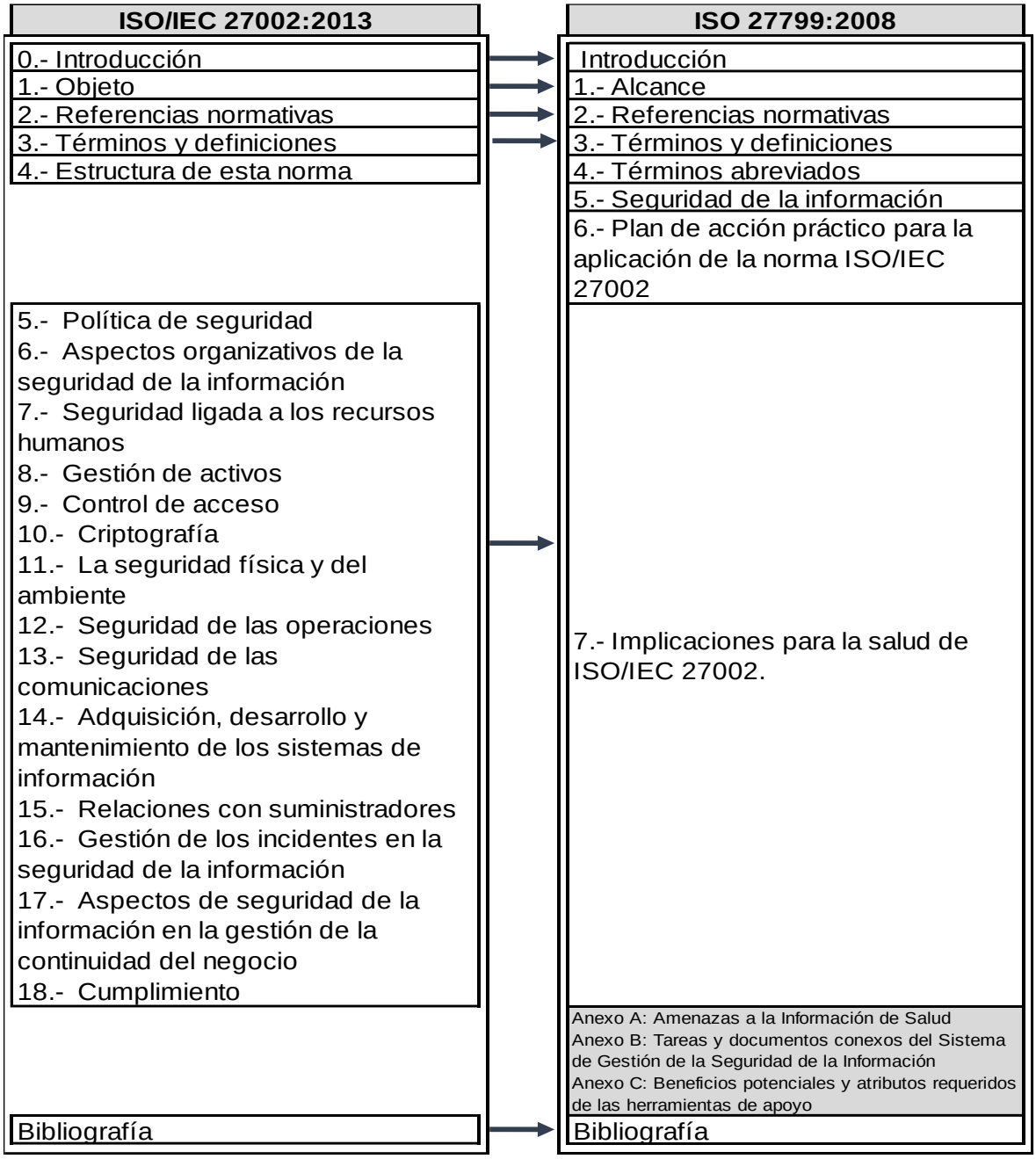
Red	Falta de prueba del envío o la recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha subrepticia
	Tráfico sensible sin protección	Escucha subrepticia
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Falta de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas autorizadas	Espionaje remoto
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos

	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo
Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos
	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos
	Falta de auditorías (supervisiones) regulares	Abuso de los derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de los derechos
	Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Abuso de los derechos

	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento del sistema de información
	Falta de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Falta de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Falta de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Falta de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Falta de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Falta de planes de continuidad	Falla del equipo
	Falta de políticas sobre el uso del correo electrónico	Error en el uso
	Falta de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Falta de registros en las bitácoras *(logs) de administrador y operario.	Error en el uso
	Falta de procedimientos para el manejo de información clasificada	Error en el uso
	Falta de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso

	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo

Anexo 4. Mapeo entre las normas ISO 27799:2008 e ISO/IEC 27002:2013



Anexo 5.

Nivel de cumplimiento de los dominios de la norma ISO/IEC 27002:2013

El presente documento describe el estado de la Seguridad de la Información (SI) en la Clínica Médica Fértil hasta la fecha de elaboración del presente trabajo de titulación. El diagnóstico de la SI en la organización es de los primeros pasos para la implementación del SGSI, de forma que se evalúa el cumplimiento de cada uno de los dominios descritos por la norma ISO/IEC 27002:2013.

1. Evaluación inicial

La evaluación permite establecer el nivel de cumplimiento de los 14 dominios de la norma ISO/IEC 27001:2013 en su anexo A o su equivalente y con mayor grado de detalle la norma ISO/IEC 27002:2013. Por lo tanto, las respuestas posibles para la encuesta aplicada son: NC, CP, CS. De acuerdo a la información que se presenta en la siguiente Tabla:

Sigla	Estado de Evaluación	Descripción
NC	No cumple	No existe y/o no se está haciendo
CP	Cumple parcialmente	Lo que la norma requiere (ISO/IEC 27002 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona.
CS	Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO/IEC 27002 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI cumple 100%

A continuación se presenta la encuesta aplicada en la Clínica Médica Fértil al Ing. Jason Cervantes responsable de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones (TIC). Con la encuesta se evalúan 114 ítems que hacen referencia a los controles de los 14 dominios de: Políticas de seguridad de la información, organización de la seguridad de la información, seguridad ligada a los recursos humanos, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, seguridad de las operaciones, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento de sistemas de información, relaciones con los proveedores, gestión de incidentes de seguridad de

la información, aspectos de seguridad de la información de la gestión de continuidad de negocio y cumplimiento.

1.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Control en la Normativa	Sección	Control	Evaluación
5.	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
5.1	DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN		
5.1.1	Políticas de seguridad de la información	Debería definirse un conjunto de políticas de seguridad de la información, ser aprobadas por la dirección, publicadas y comunicadas a los empleados y a las partes externas relevantes.	CP
5.1.2	Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información deberían revisarse a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continúa.	NC

1.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Control en la Normativa	Sección	Control	Evaluación
6.	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
6.1	ORGANIZACIÓN INTERNA		
6.1.1	Funciones y responsabilidades de la seguridad de la información	Deberían definirse y asignarse todas las responsabilidades de seguridad de la información.	NC

6.1.2	Separación de funciones	Las funciones en conflicto y las áreas de responsabilidad deberían separarse para reducir las oportunidades de modificación no autorizada o accidental o el mal uso de los activos de la organización.	NC
6.1.3	Contacto con autoridades	Deberían mantenerse los contactos apropiados con las autoridades relevantes.	CP
6.1.4	Contacto con grupos de interés especial	Deberían mantenerse contactos apropiados con los grupos de interés especial u otros foros especializados en seguridad y con asociaciones profesionales.	CP
6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información debería tratarse en la gestión de proyectos, independientemente del tipo de proyectos.	NC
6.2	DISPOSITIVOS MÓVILES Y TELETRABAJO		
6.2.1	Política para dispositivos móviles	Debería adoptarse una política y apoyo a las medidas de seguridad para gestionar los riesgos introducidos por el uso de dispositivos móviles.	CP
6.2.2	Teletrabajo	Se deberían 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.	NC

1.3 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Control en la Normativa	Sección	Control	Evaluación
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
7.1	ANTES DE ASUMIR EL EMPLEO		
7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían 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.	CP
7 .1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	NC
7.2	DURANTE LA EJECUCIÓN DEL EMPLEO		
7.2.1	Responsabilidades de la dirección	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	CP
7.2.2	Concientización, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	NC

7.2.3	Proceso disciplinario	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	CP
7.3	TERMINACIÓN O CAMBIO DE EMPLEO		
7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	NC

1.4 GESTIÓN DE ACTIVOS

Control en la Normativa	Sección	Control	Evaluación
8.	GESTIÓN DE ACTIVOS		
8.1	RESPONSABILIDAD SOBRE LOS ACTIVOS		
8.1.1	Inventario de activos	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	CP
8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deberían tener un propietario.	CP
8.1.3	Uso aceptable de los activos	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	NC
8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al	NC

		terminar su empleo, contrato o acuerdo.	
8.2	CLASIFICACIÓN DE LA INFORMACIÓN		
8.2.1	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	NC
8.2.2	Etiquetado de la información	Se debería 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.	NC
8.2.3	Manejo de activos	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	NC
8.3	MANEJO DE LOS MEDIOS		
8.3.1	Gestión de medios removibles	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	NC
8.3.2	Disposición de los medios	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	NC
8.3.3	Transferencia de medios físicos	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	NC

1.5 CONTROL DE ACCESO

Control en la Normativa	Sección	Control	Evaluación
9.	CONTROL DE ACCESO		
9.1	REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO		
9.1.1	Política de control de acceso	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	CP
9.1.2	Acceso a redes y a servicios en red	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	CP
9.2	GESTIÓN DEL ACCESO DE USUARIOS		
9.2.1	Registro y cancelación del registro de usuarios	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	NC
9.2.2	Suministro de acceso de usuarios	Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	NC
9.2.3	Gestión de derechos de acceso privilegiado	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	NC
9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debería controlar por medio de un proceso de gestión formal.	NC
9.2.5	Revisión de los derechos de	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	CP

	acceso de usuarios		
9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	CP
9.3	RESPONSABILIDADES DE LOS USUARIOS		
9.3.1	Uso de información de autenticación secreta	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	NC
9.4	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES		
9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	CP
9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	NC
9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	NC
9.4.4	Uso de programas utilitarios privilegiados	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	NC
9.4.5	Control de acceso a códigos fuente de programas	Se debería restringir el acceso a los códigos fuente de los programas.	NC

1.6 CRIPTOGRAFÍA

Control en la Normativa	Sección	Control	Evaluación
10.	CRIPTOGRAFÍA		
10.1	CONTROLES CRIPTOGRÁFICOS		
10.1.1	Política sobre el uso de controles criptográficos	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	CP
10.1.2	Gestión de llaves	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	NC

1.7 SEGURIDAD FÍSICA Y DEL ENTORNO

Control en la Normativa	Sección	Control	Evaluación
11.	SEGURIDAD FÍSICA Y DEL ENTORNO		
11.1	ÁREAS SEGURAS		
11.1.1	Perímetro de seguridad física	Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	CP
11.1.2	Controles físicos de entrada	Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	CP
11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	NC

11.1.4	Protección contra amenazas externas y ambientales	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	NC
11.1.5	Trabajo en áreas seguras	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	NC
11.1.6	Áreas de despacho y carga	Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	NC
11.2	EQUIPAMIENTO		
11.2.1	Ubicación y protección de los equipos	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	CP
11.2.2	Servicios de suministro	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	NC
11.2.3	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	NC
11.2.4	Mantenimiento de equipos	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	NC
11.2.5	Retiro de activos	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	NC

11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deberían 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.	NC
11.2.7	Disposición segura o reutilización de equipos	Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	NC
11.2.8	Equipos de usuario desatendidos	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	NC
11.2.9	Política de escritorio limpio y pantalla limpia	Se debería 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.	CP

1.8 SEGURIDAD DE LAS OPERACIONES

Control en la Normativa	Sección	Control	Evaluación
12.	SEGURIDAD DE LAS OPERACIONES		
12.1	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES		
12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	NC

12.1.2	Gestión de cambios	Se deberían 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.	NC
12.1.3	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	NC
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	CP
12.2	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS		
12.2.1	Controles contra códigos maliciosos	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	CP
12.3	COPIAS DE RESPALDO		
12.3.1	Respaldo de la información	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	CP
12.4	REGISTRO Y SEGUIMIENTO		
12.4.1	Registro de eventos	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	NC

12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	NC
12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	NC
12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	NC
12.5	CONTROL DE SOFTWARE EN LA PRODUCCIÓN		
12.5.1	Instalación de software en sistemas operativos	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	NC
12.6	GESTIÓN DE LA VULNERABILIDAD TÉCNICA		
12.6.1	Gestión de las vulnerabilidades técnicas	Se debería 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.	NC
12.6.2	Restricciones sobre la instalación de software	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	NC
12.7	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN		

12.7.1	Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	NC

1.9 SEGURIDAD DE LAS COMUNICACIONES

Control en la Normativa	Sección	Control	Evaluación
13.	SEGURIDAD DE LAS COMUNICACIONES		
13.1	GESTIÓN DE LA SEGURIDAD DE LAS REDES		
13.1.1	Controles de redes	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	NC
13.1.2	Seguridad de los servicios de red	Se deberían 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 servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	NC
13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	NC
13.2	TRANSFERENCIA DE INFORMACIÓN		
13.2.1	Políticas y procedimientos de transferencia de información	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	NC

13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	NC
13.2.3	Mensajería electrónica	Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	CP
13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deberían 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.	NC

1.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Control en la Normativa	Sección	Control	Evaluación
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
14.1	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN		
14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	NC
14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	NC

14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debería 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.	NC
14.2	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE		
14.2.1	Política de desarrollo seguro	Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	NC
14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	NC
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	NC
14.2.4	Restricciones en los cambios a los paquetes de software	Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	CP
14.2.5	Principios de construcción de sistemas seguros	Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	NC

14.2.6	Ambiente de desarrollo seguro	Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	NC
14.2.7	Desarrollo contratado externamente	La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	NC
14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.	CP
14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	NC
14.3	DATOS DE PRUEBA		
14.3.1	Protección de datos de prueba	Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.	NC

1.11 RELACIONES CON LOS PROVEEDORES

Control en la Normativa	Sección	Control	Evaluación
15.	RELACIONES CON LOS PROVEEDORES		
15.1	SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES		
15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar	CP

		con estos y se deberían documentar.	
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deberían 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.	NC
15.1 3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deberían 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.	NC
15.2	GESTIÓN DE LA ENTREGA DE SERVICIOS POR LOS PROVEEDORES		
15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	NC
15.2.2	Gestión de cambios en los servicios de los proveedores	Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	NC

1.12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Control en la Normativa	Sección	Control	Evaluación
16.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
16.1	GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN		
16.1.1	Responsabilidades y procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	NC
16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	NC
16.1.3	Reporte de debilidades de seguridad de la información	Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	NC
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.	NC
16.1.5	Respuesta a incidentes de seguridad de la información	Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	CP

16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	NC
16.1.7	Recolección de evidencia	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	NC

1.13 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

Control en la Normativa	Sección	Control	Evaluación
17.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO		
17.1	CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN		
17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debería 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.	NC
17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debería 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.	NC
17.1.3	Verificación, revisión y evaluación de la continuidad de la	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecida e	NC

	seguridad de la información	implementada, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	
17.2	REDUNDANCIAS		
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	NC

1.14 CUMPLIMIENTO

Control en la Normativa	Sección	Control	Evaluación
18.	CUMPLIMIENTO		
18.1	CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES		
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	CP
18.1.2	Derechos de propiedad intelectual	Se deberían 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.	NC
18.1.3	Protección de registros	Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	NC

18.1.4	Privacidad y protección de información de datos personales.	Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	CP
18.1.5	Reglamentación de controles criptográficos	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	NC
18.2	REVISIONES DE SEGURIDAD DE LA INFORMACIÓN		
18.2.1	Revisión independiente de la seguridad de la información	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 deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	NC
18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deberían 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.	NC
18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	NC

Anexo 6.

Selección de controles para el tratamiento del riesgo basado en la norma ISO/IEC 27002:2013

Ctrl	Sección	Tipo de Activos					
		Hardware	Información / Datos	Redes de comunicaciones	Servicios médicos y procesos del negocio	Software	Personas
5.	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN						
5.1	DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN						
5.1.1	Políticas de seguridad de la información	X	X	X	X	X	X
5.1.2	Revisión de las políticas de seguridad de la información	X	X	X	X	X	X
6.	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN						
6.1	ORGANIZACIÓN INTERNA						
6.1.1	Funciones y responsabilidades de la seguridad de la información	X	X	X	X	X	X
6.1.2	Separación de funciones	X	X	X	X	X	X
6.1.3	Contacto con autoridades				X		X
6.1.4	Contacto con grupos de interés especial	X	X	X	X	X	X
6.1.5	Seguridad de la información en la gestión de proyectos						
6.2	DISPOSITIVOS MÓVILES Y TELETRABAJO						
6.2.1	Política para dispositivos móviles	X		X			
6.2.2	Teletrabajo	X		X			
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS						
7.1	ANTES DE ASUMIR EL EMPLEO						
7.1.1	Selección						X

7 .1.2	Términos y condiciones del empleo						X
7.2	DURANTE LA EJECUCIÓN DEL EMPLEO						
7.2.1	Responsabilidades de la dirección						X
7.2.2	Concientización, educación y formación en la seguridad de la información						X
7.2.3	Proceso disciplinario						X
7.3	TERMINACIÓN O CAMBIO DE EMPLEO						
7.3.1	Terminación o cambio de responsabilidades de empleo						X
8.	GESTIÓN DE ACTIVOS						
8.1	RESPONSABILIDAD SOBRE LOS ACTIVOS						
8.1.1	Inventario de activos	X	X	X	X	X	X
8.1.2	Propiedad de los activos	X	X	X	X	X	X
8.1.3	Uso aceptable de los activos	X	X	X	X	X	X
8.1.4	Devolución de activos	X	X	X	X	X	X
8.2	CLASIFICACIÓN DE LA INFORMACIÓN						
8.2.1	Clasificación de la información		X				
8.2.2	Etiquetado de la información		X				
8.2.3	Manejo de activos		X				
8.3	MANEJO DE LOS MEDIOS						
8.3.1	Gestión de medios removibles	X	X				
8.3.2	Disposición de los medios	X	X				
8.3.3	Transferencia de medios físicos	X	X				
9.	CONTROL DE ACCESO						
9.1	REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO						
9.1.1	Política de control de acceso				X		X
9.1.2	Acceso a redes y a servicios en red			X			
9.2	GESTIÓN DEL ACCESO DE USUARIOS						
9.2.1	Registro y cancelación del registro de usuarios						X
9.2.2	Suministro de acceso de usuarios						X

9.2.3	Gestión de derechos de acceso privilegiado						X
9.2.4	Gestión de información de autenticación secreta de usuarios						X
9.2.5	Revisión de los derechos de acceso de usuarios						X
9.2.6	Retiro o ajuste de los derechos de acceso						X
9.3	RESPONSABILIDADES DE LOS USUARIOS						
9.3.1	Uso de información de autenticación secreta						X
9.4	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES						
9.4.1	Restricción de acceso a la información					X	X
9.4.2	Procedimiento de ingreso seguro					X	X
9.4.3	Sistema de gestión de contraseñas					X	X
9.4.4	Uso de programas utilitarios privilegiados					X	X
9.4.5	Control de acceso a códigos fuente de programas					X	X
10.	CRIPTOGRAFÍA						
10.1	CONTROLES CRIPTOGRÁFICOS						
10.1.1	Política sobre el uso de controles criptográficos						
10.1.2	Gestión de llaves						
11.	SEGURIDAD FÍSICA Y DEL ENTORNO						
11.1	ÁREAS SEGURAS						
11.1.1	Perímetro de seguridad física				X		X
11.1.2	Controles físicos de entrada	X			X		X
11.1.3	Seguridad de oficinas, recintos e instalaciones						
11.1.4	Protección contra amenazas externas y ambientales						
11.1.5	Trabajo en áreas seguras		X				X
11.1.6	Áreas de despacho y carga						X
11.2	EQUIPAMIENTO						

11.2.1	Ubicación y protección de los equipos			X			
11.2.2	Servicios de suministro	X		X			
11.2.3	Seguridad del cableado	X		X			
11.2.4	Mantenimiento de equipos	X		X			
11.2.5	Retiro de activos	X		X			
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	X		X			
11.2.7	Disposición segura o reutilización de equipos	X		X			
11.2.8	Equipos de usuario desatendidos	X		X			
11.2.9	Política de escritorio limpio y pantalla limpia						X
12.	SEGURIDAD DE LAS OPERACIONES						
12.1	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES						
12.1.1	Procedimientos de operación documentados						
12.1.2	Gestión de cambios						
12.1.3	Gestión de capacidad						
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación						
12.2	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS						
12.2.1	Controles contra códigos maliciosos		X			X	
12.3	COPIAS DE RESPALDO						
12.3.1	Respaldo de la información		X			X	
12.4	REGISTRO Y SEGUIMIENTO						
12.4.1	Registro de eventos		X			X	X
12.4.2	Protección de la información de registro		X			X	
12.4.3	Registros del administrador y del operador		X			X	
12.4.4	Sincronización de relojes	X	X				
12.5	CONTROL DE SOFTWARE EN LA PRODUCCIÓN						
12.5.1	Instalación de software en sistemas operativos						

12.6	GESTIÓN DE LA VULNERABILIDAD TÉCNICA						
12.6.1	Gestión de las vulnerabilidades técnicas						
12.6.2	Restricciones sobre la instalación de software						
12.7	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN						
12.7.1	Controles sobre auditorías de sistemas de información						
13.	SEGURIDAD DE LAS COMUNICAIONES						
13.1	GESTIÓN DE LA SEGURIDAD DE LAS REDES						
13.1.1	Controles de redes			X			
13.1.2	Seguridad de los servicios de red			X			
13.1.3	Separación en las redes			X			
13.2	TRANSFERENCIA DE INFORMACIÓN						
13.2.1	Políticas y procedimientos de transferencia de información		X				X
13.2.2	Acuerdos sobre transferencia de información		X				X
13.2.3	Mensajería electrónica		X				X
13.2.4	Acuerdos de confidencialidad o de no divulgación		X				X
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN						
14.1	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN						
14.1.1	Análisis y especificación de requisitos de seguridad de la información						
14.1.2	Seguridad de servicios de las aplicaciones en redes públicas						
14.1.3	Protección de transacciones de los servicios de las aplicaciones						
14.2	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE						
14.2.1	Política de desarrollo seguro						
14.2.2	Procedimientos de control de cambios en sistemas						

14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación						
14.2.4	Restricciones en los cambios a los paquetes de software						
14.2.5	Principios de construcción de sistemas seguros						
14.2.6	Ambiente de desarrollo seguro						
14.2.7	Desarrollo contratado externamente						
14.2.8	Pruebas de seguridad de sistemas						
14.2.9	Prueba de aceptación de sistemas						
14.3	DATOS DE PRUEBA						
14.3.1	Protección de datos de prueba						
15.	RELACIONES CON LOS PROVEEDORES						
15.1	SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES						
15.1.1	Política de seguridad de la información para las relaciones con proveedores						
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores						
15.1 3	Cadena de suministro de tecnología de información y comunicación						
15.2	GESTIÓN DE LA ENTREGA DE SERVICIOS POR LOS PROVEEDORES						
15.2.1	Seguimiento y revisión de los servicios de los proveedores						
15.2.2	Gestión de cambios en los servicios de los proveedores						
16.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN						
16.1	GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN						
16.1.1	Responsabilidades y procedimientos		X				X
16.1.2	Reporte de eventos de seguridad de la información		X				X
16.1.3	Reporte de debilidades de seguridad de la información		X				X

16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		X				X
16.1.5	Respuesta a incidentes de seguridad de la información		X				X
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		X				X
16.1.7	Recolección de evidencia		X				X
17.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO						
17.1	CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN						
17.1.1	Planificación de la continuidad de la seguridad de la información				X		
17.1.2	Implementación de la continuidad de la seguridad de la información				X		
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información				X		
17.2	REDUNDANCIAS						
17.2.1	Disponibilidad de instalaciones de procesamiento de información.						
18.	CUMPLIMIENTO						
18.1	CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES						
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales				X		
18.1.2	Derechos de propiedad intelectual		X		X	X	
18.1.3	Protección de registros		X		X		X
18.1.4	Privacidad y protección de información de datos personales.		X				
18.1.5	Reglamentación de controles criptográficos		X			X	X
18.2	REVISIONES DE SEGURIDAD DE LA INFORMACIÓN						
18.2.1	Revisión independiente de la seguridad de la información	X	X		X		X
18.2.2	Cumplimiento con las políticas y normas de seguridad		X				X
18.2.3	Revisión del cumplimiento técnico	X	X				X

Anexo 7

Documentación de SGSI para la Clínica Médica Fértil

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Organización:

Clínica Médica Fértil

Objetivo:

Establecer que elementos de la Clínica Médica Fértil formaran parte del SGSI, a través de cual se permita brindar confidencialidad, integridad y disponibilidad a los servicios médicos y los sistemas de información existentes.

Descripción:

Por su naturaleza, las entidades prestadoras de servicios de salud realizan sus atenciones en ambientes en los cuales se dificulta el control sobre el público que accede entre los cuales se tiene pacientes, visitas, médicos, trabajadores y público en general, siendo difícil la segmentación de las personas que pertenecen a cada uno de estos grupos. Por tal motivo el Sistema de Gestión de Seguridad de la Información de la Clínica Médica Fértil abarca todas las áreas administrativas, servicios médicos e infraestructura tecnológica tanto a nivel interno como a nivel externo de la organización; La implementación del SGSI a través de los controles y documentación permitirá brindar confidencialidad, integridad y disponibilidad a los servicios médicos, información de los pacientes y los sistemas de información existentes.

El desarrollo del SGSI se centra en que el proyecto es teórico fundamentado en las experiencias de los trabajadores de la clínica y el responsable de la Unidad de TIC; Funcionarios que manifiestan los problemas en la red, infección de virus, acceso sin restricción a los diferentes equipos de cómputo, el manejo de sus correos personales para transferir información administrativa del clínica, falta de backups, etc.

Por otro lado se debe considerar que no es posible hacer pruebas con la

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

información real de los pacientes y sistemas informáticos relacionados, debido que por normas éticas y morales no se puede tener acceso a dicha información clasificada sin autorización de la Gerencia y los pacientes.

Las funciones de las áreas involucradas en el SGSI son las siguientes:

1. **Gerencia**:
   - Representar a la institución legalmente.
   - Autorizar el ingreso del personal necesario.
   - Establecer objetivos a corto y largo plazo.
   - Autorizar la compra de insumos para la institución.
   - Tomar decisiones respecto a sanciones al personal por incumplimiento de normas.
   - Desarrollar estrategias para mantener la buena imagen de la Clínica.
   - Identificar, analizar y resolver los problemas que se presenten en la institución.
   - Supervisar la contabilidad y cierres de caja.
   - Tomar decisiones en favor de la institución.

2. **Dirección Administrativa**

   2.1. Talento Humano:
   - Planear, organizar, dirigir y controlar los programas, estrategias y acciones a desarrollar para el óptimo aprovechamiento de las habilidades del personal.
   - Proponer medidas técnico administrativas para el mejor funcionamiento de los recursos existentes.
   - Supervisa y distribuye las actividades del personal.
   - Velar por el cumplimiento de las normas y procedimientos de higiene y seguridad, establecidos por la organización.

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

- Elaborar y controlar el proceso de reclutamiento, selección, ingreso e inducción del personal.
- Proyectar y coordinar programas de capacitación y entrenamiento para los empleados.
- Coordinar y controlar el proceso de desincorporación del personal.

2.2. Servicios generales:

- Dar cumplimiento a las políticas y normas de seguridad e higiene emitidas.
- Mantenimiento de Equipos médicos.
- Limpieza y seguridad de las instalaciones.
- Mantener el orden e higiene de los materiales o enseres utilizados.
- Informar del deterioro de los equipos médicos e instalaciones de la Clínica.
- Brindar apoyo en las tareas administrativas de la Institución.
- Tratamiento de reciclaje de desechos infecciosos.
- Suministrar, controlar y conservar en buen estado físico y logístico interno de la Institución.

3. Dirección Contable – Financiera.

3.1. Contabilidad

- Realizar un listado de los insumos médicos y administrativos faltantes.
- Realizar las cotizaciones.
- Pago a proveedores.
- Facturación de servicios médicos.
- Control de inventario (Laboratorio, Farmacia, Emergencia, Consultorios).
- Preparar los registros para realizar las declaraciones.
- Recibir, examinar, clasificar y codificar los documentos contables.

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

- Archivar documentos contables
- Mantener actualizados los registros contables.

3.2. Presupuesto

- Registro de ingresos, gastos y control de inventarios.
- Pago a empleados de la institución.
- Realizar el cierre del ejercicio al finalizar el periodo.
- Verificar y consolidar saldos contables.
- Asesorar a gerencia en la toma de decisiones financieras.
- Llevar un adecuado control de los activos fijos de la Clínica y su respectiva depreciación.
- Elaborar de Conciliaciones Bancarias.
- Preparar y presentar informes acerca de la situación financiera a los accionistas.

4. **Consulta Externa:**
   - Brindar un servicio ambulatorio para pacientes con una cita asignada de los diferentes tipos de diagnósticos que posee la clínica: Medicina General, Otorrinolaringología, Ginecología – Infertilidad, Pediatría y Acupuntura.

5. **Servicios Médicos:**
   - Brindar a los pacientes un eficiente servicio médico de las diferentes atenciones que presta la clínica:
     - Hospitalización
     - Quirófano
     - Emergencia
     - Farmacia

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

- Servicios de diagnóstico (Imagenlogia)
- Laboratorio de Infertilidad

Se debe considerar que en organigrama estructural vigente la Unidad de TIC se encuentra como una unidad de Apoyo y es considerado como un servicio general; sin embargo las funciones de dicha unidad se encuentra descrita en el ítem 4.1.7.

Elaborado	Revisado y Aprobado	Aprobado y autorizado
Alexandra Enríquez	Ing. Jason Cervantes	Dra. Susana Navarro
ESTUDIANTE	DEP. TIC	GERENTE

clínica médica fértil IMBACLINIC CIA. LTDA. RUC. 1091747762001

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

POLÍTICA Y OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Organización:

Clínica Médica Fértil

Objetivo:

Describir y establecer la política y objetivos del sistema de gestión de seguridad de la información en la Clínica Médica Fértil, que permita especificar las condiciones, derechos y obligaciones de cada uno de los miembros de la organización con respecto a la utilización de los activos y sistemas informáticos.

Descripción:

La política y objetivos propuestos para el presente SGSI es la siguiente:

1. **Política del SGSI:**

La Clínica Médica Fértil enfocada en brindar un servicio de salud de calidad, orientado siempre a la satisfacción de los pacientes y en cumplimiento de la misión, visión y objetivos estratégicos, establece la función del Sistema de Gestión de Seguridad de la Información con el objetivo de:

- Cumplir con los requerimientos legales y reglamentarios aplicables a la Clínica Médica Fértil y al Sistema de Gestión de Seguridad de la Información.
- Entregar servicio de salud de calidad, con sentido de pertenencia, actitud proactiva y comunicación continua y oportuna.
- Gestionar los riesgos de la entidad a través de la aplicación de estándares y controles orientados a preservar la seguridad de nuestra información.
- Mantener buenas prácticas de seguridad de la información que garantizan la Disponibilidad, Integridad y Confidencialidad de la información, proporcionando confianza en nuestras partes interesadas.

Dirección: César Morales Granda 4-76 y Salvador Dalí, Urbanización Flota Imbabura, vía Urcuquí
Telef: (06) 2951 357 - 2600 064 - 2600 975 - 2608 011 - 0995 272 158 / **Ibarra - Ecuador**
www.clinicamedicafertil.com.ec

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

- Implementar el sistema de gestión de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores de la Clínica Médica Fértil.
- Garantizar la continuidad de los servicios y la seguridad de la información.
- Garantizar la Disponibilidad, Integridad y Confidencialidad de los datos personales y sensibles de sus pacientes en todo uso que a estos se les pueda dar, siguiendo los lineamientos otorgados por la ley y el uso ético de los mismos.
- Los colaboradores de la Clínica Médica Fértil deben comprometerse con el cumplimiento de lo establecido por el presente documento, así como con las políticas y procedimientos relacionados del SGSI – tanto los ya vigentes como los que se publiquen posteriormente.

Aplicabilidad de la Política del SGSI:

Esta política aplica a toda la Clínica Médica Fértil, sus colaboradores, proveedores, terceros y demás partes interesadas.

2. Objetivos del SGSI:

- Ofrecer un servicio médico de calidad a las pacientes, garantizando que se apliquen los controles necesarios para asegurar su información.
- Cumplir con los requerimientos legales en cuanto a la protección de la información de los pacientes.
- Establecer y monitorear un Sistema de Gestión de Seguridad de la Información que identifique los riesgos a los que se expone la información en la Clínica Médica Fértil y pueda definir controles para los mismos.
- Concienciar al personal sobre la importancia del SGSI, así como su

Dirección: César Morales Granda 4-76 y Salvador Dalí, Urbanización Flota Imbabura, vía Urcuquí
Telef: (06) 2951 357 - 2600 064 - 2600 975 - 2608 011 - 0995 272 158 / **Ibarra - Ecuador**
www.clinicamedicafertil.com.ec

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

responsabilidad sobre el cumplimiento de lo dispuesto por el SGSI.

- Garantizar el acceso a la información de la Clínica Médica Fértil de acuerdo con los niveles de la organización y criterios de seguridad que establezca la entidad, la normatividad aplicable y/o las partes interesadas.
- Mantener la Disponibilidad e Integridad de la información de la entidad, teniendo en cuenta los requisitos de seguridad aplicables y los resultados de la valoración y el tratamiento de los riesgos identificados.
- Asegurar que la información de la Clínica Médica Fértil esté disponible para los usuarios o procesos autorizados en el momento en que así lo requieran

Elaborado	Revisado y Aprobado	Aprobado y autorizado
ALEXANDRA ENRIQUEZ	ING. JASON CERVANTES	DRA. SARA NAVARRO
ESTUDIANTE	DER. Clínica médica fértil IMBACLINIC CIA. LTDA. RUC. 1091747762001	GERENTE

Dirección: César Morales Granda 4-76 y Salvador Dalí, Urbanización Flota Imbabura, vía Urcuquí
Telef: (06) 2951 357 - 2600 064 - 2600 975 - 2608 011 - 0995 272 158 / **Ibarra - Ecuador**
www.clinicamedicafertil.com.ec

3

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

INVENTARIO DE LOS ACTIVOS DE LA CLÍNICA MÉDICA FÉRTIL				
#	Nombre del activo	Descripción del activo	Tipo de activo	Propietario del activo
1	Servicios Médicos	Servicios clínicos especializados y de emergencia prestado a los pacientes	Servicios médicos y procesos del negocio	Responsable de Gerencia
2	Consulta Externa	Servicio ambulatorio para pacientes con una cita asignada previamente que acceden a atenciones médicas para diferentes tipos de diagnósticos.	Servicios médicos y procesos del negocio	Responsable de Gerencia
3	Historia Clínica	Documentación y registros informáticos que contiene datos, valoraciones e información generado en cada uno de los procesos asistenciales a un paciente	Información / Datos	Responsable de Dirección Medica
4	Informe de resultados de pruebas de laboratorio	Base de datos con resultados de exámenes de laboratorio específicos.	Información / Datos	Responsable de Servicios Médicos Especializados
5	Informe de tratamientos de fertilidad	Archivos donde se registra todo el proceso de fertilidad para fecundación de las pacientes.	Información / Datos	Responsable de Servicios Médicos Especializad

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

				os
6	Informe de pruebas de Endoscopia	Información que refleja los resultados de tomografías o ecografía	Información / Datos	Responsable de Servicios Médicos Especializados
7	Informe de resultados de Ecografías	Archivos físico y digital de las imágenes obtenidas de pacientes	Información / Datos	Responsable de Servicios Médicos Especializados
8	Torre de Endoscópica	Equipo para la realización técnica de exploración gastro-endoscópicas, contiene puerto USB para observar la imagen en la pantalla de un PC y almacena videos e imágenes en su memoria flash interna	Hardware	Responsable de Servicios Médicos Especializados
9	Monitor de signos vitales	Dispositivo que permite detectar, procesar y desplegar en forma continua los parámetros fisiológicos del paciente; Conexión USB o inalámbrica y memoria interna para mediciones de	Hardware	Responsable de Servicios Médicos Especializados

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

		los pacientes		
10	Ecógrafo	Aparato de diagnóstico electro médico utilizado para realizar ecografías o ultrasonidos; integra mini computador, lectograbadora de CD/DVD y puertos USB	Hardware	Responsable de Servicios Médicos Especializados
11	Impresora de placas radiográficas	Dispositivos que permite imprimir imágenes de resultados de ecografías, endoscopías, entre otros.	Hardware	Responsable de Servicios Médicos Especializados
12	Computador recepción	Computador que se utiliza para agendar citas médicas	Hardware	Responsable de Recepción
13	Computador Contabilidad	Computador donde se realizan actividades relacionadas a el área de contabilidad	Hardware	Responsable de Contabilidad
14	Computador Presupuesto	Computador donde se realizan actividades relacionadas a el área de Presupuestos	Hardware	Responsable de Presupuesto
15	Computador Laboratorio	Computador donde se ingresan los resultados de	Hardware	Responsable de Servicios

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

		exámenes de laboratorio		Médicos Especializados
16	Computador Consultorio Ginecología	Computador donde se lleva un registro del historial clínico de pacientes respecto a Ginecologia	Hardware	Responsable de Consulta externa
17	Portátil del área de Emergencia	Computador donde se lleva un registro de historial clínico de los pacientes en el área de emergencia	Hardware	Responsable de Servicios Médicos Especializados
18	Portátil del área de Farmacia	Computador donde se lleva un registro e inventario de los medicamentos.	Hardware	Responsable de Servicios Médicos Especializados
19	Portátil Consultorio de Otorrinolarin-gología	Computador donde se lleva un registro de historial clínico de pacientes respecto a Otorrinolaringología	Hardware	Responsable de Consulta externa
20	Portátil Consultorio de Pediatría	Computador donde se lleva un registro de historial de pacientes respecto a Pediatría	Hardware	Responsable de Consulta externa
21	Impresora del área de	Equipo conectado para el área de recepción y	Hardware	Responsable de

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

	recepción	contabilidad		Recepción
22	Impresora del área de laboratorio	Equipo conectado para imprimir resultados de exámenes de laboratorio	Hardware	Responsable de Servicios Médicos Especializados
23	Impresora del área de Pediatría / Ginecología	Equipo utilizado para imprimir información de pacientes respecto a Pediatría / ginecología	Hardware	Responsable de Consulta externa
24	Antivirus	Programa informático que protege a los equipos de cómputo de los virus	Software	Responsable de Servicios Generales
25	Recursos de Ofimática	Aplicación o paquete de aplicaciones que tiene funciones ofimáticas, es decir, que sirven para facilitar el trabajo en el ámbito de una oficina.	Software	Responsable de Servicios Generales
26	Grabador de vídeo digital	Equipo de gestión de vídeo para el control, la grabación y el archivo de vídeos que provienen de cámaras de video vigilancia	Hardware	Responsable de Servicios Generales
27	Cámara de video vigilancia	Equipo de monitoreo y grabación de imágenes de una área determinada.	Hardware	Responsable de Servicios Generales
28	Datáfono	Dispositivo que permite el	Hardware	Responsable

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

		pago de los servicios médicos a través de tarjeta de crédito o débito.		de Servicios Generales
29	Reloj Biométrico	Sistema de control de ingreso del personal	Hardware	Responsable de Servicios Generales
30	Central telefónica Analógica	Equipo telefónico que permite la comunicación entre el personal de la organización	Redes de comunicaciones	Responsable de Servicios Generales
31	Teléfono analógico	Equipo telefónico que permite la comunicación entre el personal de la organización	Redes de comunicaciones	Responsable de Servicios Generales
32	Red LAN	Red LAN usada por equipos móviles para acceder a los recursos de la red corporativa de la clínica	Redes de comunicaciones	Responsable de Servicios Generales
33	Red WAN	Red WAN usada por equipos móviles para acceder a los recursos de la red corporativa de la clínica	Redes de comunicaciones	Responsable de Servicios Generales
34	Módem	Equipo que permite ofrecer acceso a Internet por la línea telefónica a los computadores	Redes de comunicaciones	Responsable de Servicios Generales

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

35	Switch	Dispositivo de 8 puertos de interconexión de equipos en red	Redes de comunicaciones	Responsable de Servicios Generales
36	Registros Contables - Financieros	Documentación que contienen datos relacionados con las operaciones económicas y financieras de la clínica	Información / Datos	Responsable de Contabilidad
37	Registros de asistencia del personal	Documentación del control digital de entrada/salida del personal	Información / Datos	Responsable de Talento Humano
38	Base de datos talento humano	Información que dispone este departamento debidamente actualizada en donde incluye información completa del personal que labora como datos personales, cargo, salario, beneficios, horarios, cursos o actividades realizadas.	Información / Datos	Responsable de Talento Humano
39	Consultorios	Espacio físico en el cual un médico o varios médicos asociados atienden a sus pacientes	Sitio / Instalaciones	Responsable de Servicios Generales
40	Laboratorio	Espacio físico en el cual se encuentran equipamiento médico para realizar	Sitio / Instalaciones	Responsable de Servicios Generales

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

VALORIZACIÓN DE LOS ACTIVOS DE LA CLÍNICA MÉDICA FÉRTIL					
#	Nombre del activo	Confiden -cialidad	Integridad	Disponibilidad	Valoración
1	Servicios Médicos	3	3	3	3,00
2	Consulta Externa	3	3	3	3,00
3	Historia Clínica	3	3	3	3,00
4	Informe de resultados de pruebas de laboratorio	3	3	3	3,00
5	Informe de tratamientos de fertilidad	3	3	3	3,00
6	Informe de pruebas de Endoscopia	3	3	3	3,00
7	Informe de resultados de Ecografías	3	3	3	3,00
8	Torre de Endoscópica	3	3	2	2,67
9	Monitor de signos vitales	3	3	2	2,67
10	Ecógrafo	3	3	2	2,67
11	Impresora de placas radiográficas	3	3	2	2,67
12	Computador recepción	2	2	1	1,67
13	Computador Contabilidad	2	2	1	1,67
14	Computador Presupuesto	2	2	1	1,67

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

15	Computador Laboratorio	2	2	3	2,33
16	Computador Consultorio Ginecología	2	2	1	1,67
17	Portátil del área de Emergencia	3	3	3	3,00
18	Portátil del área de Farmacia	3	3	3	3,00
19	Portátil Consultorio de Otorrinolaringología	2	2	1	1,67
20	Portátil Consultorio de Pediatría	2	2	1	1,67
21	Impresora del área de recepción	2	2	1	1,67
22	Impresora del área de laboratorio	2	2	1	1,67
23	Impresora del área de Pediatría / Ginecología	2	2	1	1,67
24	Antivirus	2	2	2	2,00
25	Recursos de Ofimática	2	2	1	1,67
26	Grabador de vídeo digital	2	1	1	1,33
27	Cámara de video vigilancia	2	2	1	1,67

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

28	Datáfono	3	3	2	2,67
29	Reloj Biométrico	2	2	1	1,67
30	Central telefónica Analógica	2	1	1	1,33
31	Teléfono analógico	2	1	1	1,33
32	Red LAN	2	2	2	2,00
33	Red WAN	2	2	1	1,67
34	Módem	2	2	2	2,00
35	Switch	2	2	2	2,00
36	Registros Contables - Financieros	3	3	2	2,67
37	Registros de asistencia del personal	3	3	2	2,67
38	Base de datos talento humano	2	2	1	1,67
39	Consultorios	1	1	1	1,00
40	Laboratorio	2	1	1	1,33
41	Quirófano	2	2	3	2,33
42	Página WEB	2	2	2	2,00
43	Talento Humano	2	2	3	2,33

Elaborado	Revisado y Aprobado	Aprobado y autorizado
ALEXANDRA ENRIQUEZ	ING. JASON CERVANTES	DRA. SARA NAVARRO
ESTUDIANTE	DEP. TIC	GERENTE

clínica médica fértil IMBACLINIC CIA. LTDA. RUC. 1091747762001

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

NIVEL DE ESTIMACIÓN DEL RIESGO A LOS ACTIVOS DE LA CLÍNICA MÉDICA FÉRTIL					
#	Nombre del activo	Tipo de activo	Impacto en caso de materializarse la amenaza	Probabilidad de que la amenaza explote la vulnerabilidad	Estimación del riesgo
1	Servicios Médicos	Servicios médicos y procesos del negocio	2,77	2,50	6,93
2	Consulta Externa	Servicios médicos y procesos del negocio	2,77	2,50	6,93
3	Historia Clínica	Información / Datos	2,46	2,67	6,56
4	Informe de resultados de pruebas de laboratorio	Información / Datos	2,38	2,50	5,96
5	Informe de tratamientos de fertilidad	Información / Datos	2,38	2,50	5,96
6	Informe de pruebas de Endoscopia	Información / Datos	2,38	2,33	5,56
7	Informe de resultados de Ecografías	Información / Datos	2,38	2,33	5,56
8	Torre de Endoscópica	Hardware	2,23	2,00	4,46
9	Monitor de signos vitales	Hardware	2,23	1,83	4,09
10	Ecógrafo	Hardware	2,31	2,00	4,62
11	Impresora de placas	Hardware	2,31	2,00	4,62

Clínica médica fértil
ESPECIALIDADES CLÍNICO QUIRÚRGICAS Y BIOLOGÍA DE LA REPRODUCCIÓN

	radiográficas				
12	Computador Laboratorio	Hardware	2,38	2,50	5,96
13	Portátil del área de Emergencia	Hardware	2,38	2,50	5,96
14	Portátil del área de Farmacia	Hardware	2,38	2,50	5,96
15	Antivirus	Software	1,85	1,83	3,38
16	Datáfono	Hardware	2,54	2,17	5,50
17	Red LAN	Redes de comunicaciones	1,85	2,00	3,69
18	Módem	Redes de comunicaciones	2,08	1,67	3,46
19	Switch	Redes de comunicaciones	2,08	1,67	3,46
20	Registros Contables - Financieros	Información / Datos	1,92	2,00	3,85
21	Registros de asistencia del personal	Información / Datos	1,92	2,17	4,17
22	Quirófano	Sitio / Instalaciones	1,62	1,33	2,15
23	Página WEB	Software	2,15	2,00	4,31
24	Talento Humano	Personas	2,38	2,50	5,96

Elaborado	Revisado y Aprobado	Aprobado y autorizado
ALEXANDRA ENRIQUEZ	ING. JASON CERVANTES	DRA. SARA NAVARRO
ESTUDIANTE	DEP. TIC	GERENTE

clínica médica fértil IMBACLINIC CIA. LTDA. RUC. 1091747762001