UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

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

TEMA:

DISEÑO DE UN SGSI BASADO EN EL ESTÁNDAR ISO 27001 PARA LA EMPRESA INVIMEDIC S.A.

AUTORES:

MARIANO ENRIQUE ÁLAVA CUADRA
HUGO ABRAHAM CHOEZ SALAZAR

DIRECTOR:

MIGUEL ÁNGEL QUIROZ MARTÍNEZ

CUENCA – ECUADOR
2023

Autores:

Mariano Enrique Álava Cuadra
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
malavac@est.ups.edu.ec

Hugo Abraham Choez Salazar
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
hchoez@est.ups.edu.ec

Dirigido por:

Miguel Ángel Quiroz Martínez
Ingeniero en Sistemas.
Máster en Ingeniería con especialidad en Sistemas de Calidad y Producción.
mquiroz@ups.edu.ec

DEDICATORIA

Dedico este trabajo de tesis de maestría a mis familiares, esencial a mis madres Maggi y Anita, cuya inquebrantable muestra de amor y apoyo constante han iluminado mi camino a lo largo de mi travesía académica. Agradezco profundamente su confianza en mí y su sacrificio incondicional para permitir que persiga mis aspiraciones.

A mi mentor y guía, Ing. Miguel Quiroz, quien me ha proporcionado dirección experta, paciencia incansable y sabiduría durante todo el proceso de investigación. La influencia y compromiso que has demostrado han sido elementos cruciales en mi desarrollo tanto como estudiante como individuo.

A mis amigos y seres queridos que han estado a mi lado en los momentos felices y desafiantes, su aliento y afecto han sido la fuente que me ha impulsado hasta este punto.

A todos aquellos que, de diversas maneras, han contribuido a mi formación académica, dedico este logro. Este trabajo de tesis ejemplifica la relevancia de la colaboración y el apoyo mutuo en la búsqueda del conocimiento y el desarrollo personal.

En última instancia, dedico esta tesis a mí mismo, como un recordatorio de que la perseverancia y el esfuerzo sostenido pueden hacer realidad los sueños. Este logro representa un paso más en mi continuo camino hacia el aprendizaje y la consecución de mis metas.

Agradezco a todos por ser parte esencial de esta extraordinaria travesía.

Mariano Enrique Alava Cuadra

AGRADECIMIENTO

A Dios, ante todo, por brindarme la sabiduría y la esperanza. A mi familia, especial a mis madres, padre, hermanas, tíos por el amor infinito y el constante soporte en cada tapa y proyecto de mi visa que he llevado a cabo.

A mi hermano Hugo Abraham, por compartir este sueño, por su entrañable cariño

A mis amigos y seres queridos, gracias por su apoyo constante.

Este logro es un testimonio de su apoyo y de mi compromiso personal con el aprendizaje continuo.

Mariano Enrique Alava Cuadra

DEDICATORIA

Dedico este trabajo de tesis de maestría a las personas que han iluminado mi camino con su amor, apoyo y sabiduría. A mi madre Rosa Salazar, un faro de fortaleza y cariño, cuya dedicación inquebrantable ha sido mi inspiración. A mi padre Angel Choez, que, aunque se encuentra en el cielo, su presencia sigue siendo un guía constante en mi vida, y sé que estaría orgulloso de los logros obtenidos.

A mis hermanos, quienes han compartido conmigo risas y desafíos, su amistad y respaldo han sido un pilar fundamental. A mis familiares cercanos, cuyo aliento y confianza me han impulsado a alcanzar esta meta.

A mis amigos cercanos, quienes han sido mi refugio en los momentos difíciles y mis compañeros en los triunfos. Su apoyo inquebrantable ha sido un tesoro invaluable.

A mi tutor de tesis Ing. Miguel Quiroz, un mentor cuya paciencia y orientación han sido fundamentales para este logro. Tu conocimiento y compromiso han sido una fuente constante de aprendizaje.

Este trabajo es el resultado de un esfuerzo colectivo y el amor de quienes me rodean. A cada uno de ustedes, les dedico esta tesis. Sin su presencia y respaldo, este logro no habría sido posible.

Hugo Abraham Choez Salazar

AGRADECIMIENTO

Primero, agradezco a Dios por ser mi guía y mi fuerza en este camino, su gracia y dirección me han acompañado en los desafíos y en los momentos de incertidumbre.

A mi querida madre, Rosa Salazar, le dedico un agradecimiento especial. Tú has sido mi inspiración constante, mi roca en tiempos difíciles y mi mayor defensora. Tus sacrificios y amor incondicional son el motor que me impulsa a alcanzar mis metas.

A mi padre, Ángel Choez, quien está en el cielo, le rindo homenaje con gratitud profunda. Tu legado de integridad y trabajo duro sigue siendo mi modelo para seguir. Sé que estás observando desde arriba con orgullo.

A mi hermano y compañero de tesis, Mariano Alava, agradezco tu colaboración incansable y tu apoyo. Juntos hemos superado obstáculos y alcanzado este logro significativo.

A mis amigos, quienes han estado a mi lado durante esta travesía, les agradezco por su amistad sincera, sus ánimos y su paciencia en los momentos de estrés. Han sido un tesoro invaluable en mi vida.

Durante mi trayecto académico, he contado con un apoyo inquebrantable de quienes me han acompañado en cada paso.

Este logro no es solo mío, sino que se debe al amor y apoyo de todos ustedes. Les agradezco profundamente y me siento honrado de tenerlos en mi vida.

Hugo Abraham Choez Salazar

Tabla de Contenido

Diseño de un SGSI basado en el estándar ISO 27001 para la empresa Invimedic S.A.

Autores:

Mariano Enrique Alava Cuadra
Hugo Abraham Choez Salazar

Resumen

La norma ISO 27001:2013 mantiene como requisitos el establecer, implementar, mantener y mejorar la personalización de la gestión de la seguridad de la información del sistema. Los errores en la elaboración del diseño de seguridad de la Empresa Invimedic, las falencias son los factores principales y críticos que generan dificultades significativas los mismos hace que tengan vulnerabilidad en el marco de seguridad de la información que se expone a los ataques externos tiene consecuencia e impacta de forma negativa la integridad de la información. El objetivo general de este trabajo es diseñar e implementar un SGSI basado en el estándar ISO 27001 para la empresa de INVIMEDIC S.A. Entre los resultados tenemos: un diagnóstico de la situación actual de seguridad de la información en INVIMEDIC, se diseñó un SGSI basado en ISO 27001, y se realizó una evaluación del SGSI implementado. Los requisitos esenciales para la aplicación de la implementación de un sistema de gestión de seguridad de la información permiten la administración de todos los procesos que gestione la empresa, las técnicas, la metodología en el uso de la norma ISO.

Palabras clave: ISO 27001, Norma ISO, Seguridad de la Información, Gestión en la seguridad

Abstract

The ISO 27001: 2013 standard maintains as requirements to establish, implement, maintain, and improve the customization of the information security management of the system. The errors in the elaboration of the design of security Company Invimedic, the shortcomings are the main and critical factors that generate significant difficulties the same makes them have vulnerability in the framework of security of the information that is exposed to the outside attacks has consequence and negatively impacts the integrity of the information. The general objective of this work is to design and implement an ISMS based on the ISO 27001 standard for the company INVIMEDIC S.A. Among the results we have: a diagnosis of the current information security situation in INVIMEDIC, an ISMS based on ISO 27001 was designed, and an evaluation of the implemented ISMS was carried out. The essential requirements for the implementation of an information security management system allow the administration of all processes managed by the company, techniques, methodology in the use of the ISO standard.

Keywords: ISO 27001, ISO Standard, Information Security, Security Management

1. Introducción

Antes de comenzar con este trabajo de investigación es necesario mencionar que el uso o la implementación de la tecnología de la información tiene una alta aceptación a nivel mundial; esta herramienta ISO 27001 define alto niveles de capacidad de generar respaldo, seguridad, políticas y estrategias; que son diseños de procesos que brindan confidencialidad, integridad y disponibilidad para aumentar la eficiencia, eficacia, y transparencia de los datos informáticos en las normas ISO/IEC 27001; con el objetivo de crear entornos participativos, innovadores que mejore la calidez y el alcance de salvaguardar la información de las entidades gubernamentales a nivel mundial que la utilización y la aplicación de las information and communication Technology (TIC) de los servicios al público; los objetivos es de cumplir los requerimientos que rigen las normas ISO 27001 en los diferentes niveles de aplicación y emplear estas normas de seguridad de la información (Institute of Electrical and Electronics Engineers, n.d.-a).

Otra de las clasificaciones del ISO 27001 es la gestión de controles para la seguridad física y sofisticada para garantizar la protección aplicada en varios niveles de parámetros de seguridad y según la clasificación del esquema de la información; que se debe de desarrollar para el monitoreo de la seguridad que debe de gestionar tanto para la política, seguridad y privacidad de cada informe; las operaciones de seguridad deben de incluir procesos que establezcan responsabilidad, protección contra los malwares, y técnicas para auditorias de vulnerabilidades en consideración; se conoce los controles en estas áreas sean importantes que otros priorizados y dependientes de su clasificación de activos y dentro de la infraestructura del sistema de información (Monev, 2022).

En el gobierno de Indonesia la policía nacional en el año 2018 implemento la tecnología ISO/IEC 27001:2013 en COBIT, en el año 2019 era de uso dominio en el que fue un modelo de selección en base para el diseño para evaluar, formular recomendaciones que debe de considerar resultados por medio del uso de la evaluación por lo que ese modelo posee una estructura organizativa, recursos que deben aplicar para el gobierno de Indonesia para que gestione la seguridad de la información; este trabajo contribuye y sustenta el desarrollo de esta tesis (Institute of Electrical and Electronics Engineers, n.d.-a).

Estos recursos informáticos permiten gestionar grandes recursos de información para los entes, es decir, personas y empresas; medianas, grandes dicha documentación contiene información importante, sensible este es a nivel empresarial es a la vez competitivo, en el que se evidencia su vulnerabilidad; ISO 27001:2013 una de sus cualidades es de brindar seguridad a esta documentación, por eso se propone la norma ISO 27001:2013, que uno de los requisitos es establecer, implementar, mantener y mejorar la personalización de la gestión de la seguridad de la información del sistema; esta norma posee importantes formas de aplicar en diferentes áreas; su singularidad es la aplicación de controles en el que brinda en la seguridad y privacidad de los informes relacionadas en empresas (Lopez-Leyva et al., 2020a).

Una de las características de las normas ISO/IEC 27001 en el uso de las information and communication Technology (TIC) se basa en el apoyo para la policía nacional de Indonesia; el desarrollo de estrategias políticas del e-gobierno que afirma el uso de la comunicación y la tecnología de la información dentro del proceso de gobernanza y aumentar la eficacia, eficiencia y la transparencia en la rendición de cuentas por parte de la administración. En el gobierno de Indonesia también regula la tecnología de la información en la utilización de crear un entorno abierto participativo, innovador; el gobierno debe de mejorar la calidad y el alcance del servicio público de la comunidad (Institute of Electrical and Electronics Engineers, n.d.-a).

Una de las definiciones de la norma ISO/IEC 27001:2013 se puede citar la seguridad estándar para todas las empresas que administran y gestionan información con una documentación muy importante a la vez es sensible y vulnerable; sin embargo, existen más estándares específicos para la seguridad en diferentes sectores empresariales e industriales; en el que se cita un ejemplo; el pago de un proveedor en el que requiere un método estándar de seguridad de datos de la industria con tarjetas de pago (PCI DSS), que se menciona que es adecuado y se tiene un mayor control sobre el sistema de pagos en línea; aún más en el sector de salud puede implementarse el seguro de salud ley de portabilidad y responsabilidad (HIPAA) para los pacientes y protección de registros médico (Chaiwut & Rueangsirarak, 2022).

Se puede mencionar otras de sus características de las normas ISO 9001:2015 en una de sus definiciones que lo caracterizan la calidad sistema de gestión (SGC) e ISO 27001:2013 dentro del marco de una excelente gestión para la seguridad de los activos (SGSI); son elegidos y crear diseños, recomendaciones el sistema gestión, calidad (SGC); es un sistema usado por las organizaciones que permite dirigir y controlar la calidad. La implementación del SGSI evita amenazas a la información; que la información, sistema de gestión tiene el objetivo desarrollar, implementar, operar, supervisar, mantener y aumentar la seguridad de la información de una organización (Institute of Electrical and Electronics Engineers, n.d.-b).

Las siglas de ISO organización internacional de normalización, comisión electrónica internacional IEC de manera conjunta se publicó una norma llamada ISO/IEC 27001 que es transferencia de la información y técnicas de seguridad revisado en 2013; se usa la ISO27001 que se refiere la versión ISO/IEC 27001:2013, el ISO es un estándar internacional sobre la manera de gestionar la información que esta certificada para cumplir con la ISO/IEC 27001; esta investigación tiene una finalidad con el ayudar a una organización para mejorar su seguridad a nivel empresarial por medio del desarrollo de la norma ISO/IEC 27001 estándar y ejecutar todos los requisitos sistemáticos; dicha documentación es una colección de datos tangibles e intangibles que son activos valiosos importantes para esta organización; que

necesita administrar de manera adecuada en la seguridad de su información es de practicar la prevención al acceso denegado, divulgación, alteración o destrucción de dicha información en la organización (Guo et al., 2021).

Para lograr un alto rendimiento en la gestión de la seguridad de información las empresas u organizaciones que se dedican en la tecnología de la información en esta era digital 4.0; las políticas de privacidad y seguridad en las organizaciones que se inician cumplen con las normas para la implementación de un sistema para gestionar la seguridad de la información en base a las normas internacionales de la seguridad de la información IS0/IEC 27001:2013; ISO 27001 no tiene mucha aceptación por parte de las organizaciones o empresas por lo que se requiere aplicar la minería web que permita explorar la adopción de las ISO/IEC 27001 mediante 2664 que son más de 900000 empresas europeas de un conjunto de datos de Mannheim Enterprise Panel que son los estándares para sitios web (Mirtsch et al., 2021).

Se puede evidenciar que los ciberataques son alteraciones, costosos cada vez más perturbadores a empresas, gobiernos las preocupaciones de seguridad cibernética; en el mundo For Económico (FEM) lanzo su primer informe global; informe que tiene una perspectiva en la seguridad cibernética que identifica y las futuras tendencias y los retos del delito cibernético que se asimila en el mundo de la digitalización que aumenta el 125% en ciberataques con evidencia en el año 2022 (Malatji, 2023).

Además, es importante tener en cuenta que la utilización, la implementación de las tecnologías de la información en las organizaciones o empresas tanto privada y gubernamentales las medidas de seguridad de la información deben de estar equilibradas que permita salvaguardar los activos de la empresa con los principios que tiene las normas ISO 27001; se puede mencionar que cada vez que las organizaciones implementen para gestionar la seguridad de la información en administrar los controles de acceso e instalar los firewalls que evolucionan las políticas y evalúan la información con alto riesgo de vulnerabilidad en el riesgo de

la seguridad; en la formulación durante la desarrollo de las políticas se deben de basarse en los altos riesgos para poder llevar a cabo los estándares establecidos en las normas ISO/IEC 27001; las organizaciones públicas son los responsables de ejecutar todas las tareas dentro del campo de la comunicación y la informática en una ciudad o distrito basados en la programación en Java; por otro lado se puede mencionar que las organizaciones son las encargadas de llevar a cabo la seguridad y la evaluación del respaldo de los datos informáticos, el uso tecnológico por falta de evaluación en que se gestiona en la seguridad de los datos informáticos que busca minimizar posibles problemas y ataques cibernéticos en las organizaciones públicas (Wicaksono et al., 2022).

La implementación de la tecnología de la información ha generado un gran reto a todas las organizaciones que gestionen los activos de la comunicación digital; la radicación de la transformación digital de la información es por medio del uso de un ordenador que procesa, recolecta, clasifica e interpreta un gran flujo de información y su uso en la edad digital estos datos se convierten en lo más preciado para los ataques cibernéticos en que las ISO/IEC 27001:2013; especifica y establece e implementa en la mejora continua de la información en los sistemas de gestión de seguridad de la información en las organizaciones; además, de la creciente conectividad nos conlleva a grandes riesgos en el flujo de los datos son las brechas de la seguridad de la información logren reducir el riesgo de parte de los infractores que las organizaciones deben de tomar decisiones con las adecuadas medidas de salvaguardar y proteger sus información que garantice al personal de los negocios de las organizaciones o empresas que se dedican al flujo de la información dentro de las redes y la web 3.0 (Mirtsch et al., 2021).

En algunas empresa u organizaciones el área de la seguridad de la información, y los que están a cargo del departamento de telecomunicación se interpreta acciones que deben tomar y prevenir la pérdida de archivos de información que contenga la empresa; la esencia de la seguridad y ser un esfuerzo del área de telecomunicación para medir la seguridad y garantizar para la continuidad de la empresa que minimice los riesgos que afecten a la empresa de esta manera aumente las oportunidades de

una empresa; esta información debe de ser considerada confidencial y ser autorizada por un agente de control para que solo las partes autorizadas puedan acceder a estos activos (Wicaksono et al., 2022).

En una organización la implementación del uso de las normas ISO/IEC 27001 uno de los grandes estándares que se usa y son aceptados por las organizaciones por el resguardo o la seguridad de la información en el mundo; año 2022 se publicó la tercera edición de esta norma internacional de SGSI, las ISO/IEC 27001:2022 para que aborde con la ciberseguridad global que es un reto o desafío mejorar la confianza digital; los autores en esta investigación busca encontrar, comparar, contrastar ISO/IEC 27001:2022 e ISO/IEC 27001:2013 por medio del lente del Instituto Nacional de Normalización and Technology (NIST) en el Marco de Seguridad Cibernética (CF); para la protección e infraestructura de la norma estándar de seguridad de la información las ISO 27001 se debe a la gestión de los controles de seguridad a los que toma una referencia en los anexos; las ISO/IEC 27001:2022 para mejorar los sistemas información, aspectos de la gestión de la seguridad de la información a nivel empresarial que aborda la protección de los servicios en salvaguardar por medio de la nube o cloud u otra aplicación informático de sistemas que se usen para la gestión de seguridad que toda empresa han adoptado en el manejo de la tecnología de la información (Malatji, 2023).

La empresa Invimedic es una empresa que gestiona una extensa información por varios canales de la red y que son vulnerables antes las posibles amenazas existentes en la actualidad; por lo que, se debe de gestionar un diseño de seguridad de la información bajo los requisitos de las normas ISO/IEC 27001 que les permita salvaguardar su información tanto del personal médico y de sus pacientes (Putra et al., 2021).

1.2. Determinación del Problema

La presente investigación surge a la necesidad de conocer y aprender de los avances que tiene la seguridad información y que tanto ha influido a nivel de empresas o industrias; tanto que ha sido los avances tecnológicos a nivel mundial en el que toda información está al alcance de cualquier usuario; por lo que, cabe mencionar importancia el resguardo información a nivel organizacional.

Es fundamental abordar de manera integral el empleo y la integración de medidas de seguridad de la información, no solo en el ámbito industrial y empresarial, sino también en diversas esferas.

Esta investigación busca poner a disposición la información en base de los avances que se tienen en el control de información mediante la implementación de la seguridad información a nivel mundial; dado que la información se encuentra vulnerable a los ataques cibernéticos en la era de la web 3.0, cualquier dato o información es susceptible de ser difundido en el vasto entorno de las redes o la propia web.

Con el progreso tecnológico, este estudio destaca la responsabilidad de los estudiantes de ingeniería en sistemas en la gestión y diseño de modelos o esquemas de seguridad. Además, resalta la influencia de la seguridad informática en la sociedad, impulsando su implementación en empresas e industrias; acuerdo a las interrogantes se deben de realizar estudios de las posibles vulnerabilidades de la información que se generen en las organizaciones o empresas, sean estas del ámbito de la salud.

En este apartado se puede demostrar que es importante que las organizaciones o empresas puedan gestionar dichas normas de la seguridad de datos; y estas no sean tan vulnerables de posibles ataques cibernéticos o informático.

1.2. 1 Descripción del problema

Hoy en día se identifican las falencias en el desarrollo, estructuras de la seguridad de información de la Empresa Invimedic; los factores principales es la falta de resguardo de la información que garantice recursos la gestión de información; con el método de la observación que para tener acceso a los archivos que se realizan, las amenazas y vulnerabilidades tienen una brecha abierta a los archivos que afecta las principales normas de seguridad integridad, confidencialidad, la disponibilidad, asistencia de comunicación e información; están en el diseño del sistema de gestión de la seguridad y configuración en la estructura de equipos que se crean vulnerabilidades o amenazas que impactan de manera negativa con respecto de la seguridad dentro de la red; cabe mencionar que la garantía en las normas de seguridad es firme y eficiente en la información de la empresa.

El uso de la tecnología en la actualidad por medio de pruebas que permita replicar en los diferentes escenarios en el que proporciona la oportunidad de reflexionar y tener argumentos sobre los impactos positivos que tendría una mejoría y la ejecución del diseño gestión de seguridad de la información base de normas ISO/IEC 27001; metodología que usa la organización respecto a la información tiene que presentar óptimos resultados precisen y puedan guiar a los agentes encargados del área de telecomunicación debido a la aplicación de estas normas de seguridad a largo plazo; este argumento le permita a la Empresa Invimedic elaborar y tener un manual en dos secciones la sección teórica, la sección práctica que ejecuta el uso e implementación diseño de seguridad la información; que asegura una eficiencia por el uso de los instrumentos de evaluación y pruebas que se consideran herramientas que apoyan en la toma de decisiones de los altos directivos para desarrollar una planificación y ejecutar los proyectos para la aplicación del SGSI y las ISO 27001.

La ausencia de estudios y análisis exhaustivo en la operatividad gestión de la seguridad de la información en la Empresa Invimedic; Analizar las causas fundamentales de problemas significativos que se enfoca en la seguridad de la

ejecución de manera ininterrumpido del SGSI; se puede mencionar que no hubo la debida atención, La falta de verificación de las vulnerabilidades en el sistema de seguridad y la ausencia de detección de amenazas son motivo de inquietud. Esta preocupación se fundamenta en que las brechas de seguridad resultan de una gestión deficiente y falta de seguridad en la información que son una amenaza significativa que involucra la integridad, la confidencialidad y la disponibilidad de transferencia la información disponible de los servicios de la red; es fundamental que lleve a cabo la implementación, hacer pruebas necesarias que complemente la operatividad del sistema de gestión de seguridad de la información y las normas ISO/IEC 27001; tomar las medidas precisas proactivas que aborden cualquier debilidad en la seguridad ; que ofrezca la garantía de la operación esta sea confiable y segura la fluidez de la información en todo momento.

1. 2. 2 Justificación del problema

Los errores en la elaboración del diseño de seguridad Empresa Invimedic; las falencias son los factores principales y críticos que generan dificultades significativos los mismos hace que tengan vulnerabilidad en el marco de seguridad de la información que se expone a los ataques externos tiene consecuencia e impacta de forma negativa la integridad de la información; es importante para la toma de decisiones y las debidas medidas que aborden los problemas de seguridad de la información y su diseño del sistema de gestión de seguridad de la información; garantizar una gestión eficaz y segura en el trato de la información genera una protección a la información y su confidencialidad de los mismos que administre la empresa; de tal manera asegura la disponibilidad de los servicios de comunicación, la intercomunicación mejora y contribuya con un óptimo rendimiento en el trato de la información gestiona la organización o empresa de forma general.

1. 2. 3 Delimitación del problema

El objetivo de este trabajo es abordar los posibles problemas de seguridad en el marco del diseño de seguridad que permite identificar la tecnología de la información de la Empresa Invimedic; propone un proyecto para implementar un

nuevo y mejorado diseño en el sistema de gestión de seguridad de la información en el que presenta una configuración adecuada al manejo de información basadas en una seguridad especifica en el control de la seguridad, en prevenir el acceso no autorizado de terceros a la información reservada de la Empresa Invimedic y el uso de estas medidas de seguridad fortalezca la integridad, la confidencialidad y la disponibilidad de los servicios que ofrecen el área de intercomunicación de datos por parte de la empresa; este nuevo diseño de seguridad en la tecnología de la información se evalúa por medio de pruebas o test a los sistemas de seguridad que garanticen la eficacia antes de la implementación en producción del sistema de seguridad de la información; el objetivo de esta iniciativa es de buscar mejorar la gestión de seguridad de la información de la Empresa Invimedic; proteja la información sensible y asegurar la persistencia de los servicios críticos que ofrece la empresa.

1. 3 Objetivos

El objetivo general de este trabajo es diseñar e implementar un SGSI basado en el estándar ISO 27001 para la empresa de INVIMEDIC S.A

1. 3.1 Objetivos Específicos

- Realizar un diagnóstico de la situación actual de seguridad de la información en la empresa.
- Diseñar e implementar un SGSI basado en ISO 27001.
- Realizar una evaluación de la efectividad del SGSI implementado.

2. Marco teórico referencial

En la documentación que registra esta investigación se menciona que se puede evidenciar; después de la pandemia COVID-19 se destacaron los robos informáticos

y la información personal, tanto en personas naturales y jurídicas, es decir en la banca financiera, el sector gubernamental han sido víctimas de robos de información; ejecutados por los hackers en el año 2018, le sucedió al gobierno de Indonesia que se registró su ataque en el mismo año; y también ha sido a nivel mundial estos ataques de cibernéticos; dicho ataques pueden ser phishing, Spears phishing, whaling y malware; por lo que conlleva a la realización de esta investigación para el respaldo de la información es implementar el uso de la tecnología para la seguridad de la información (Institute of Electrical and Electronics Engineers, n.d.-b).

Uno de los objetivos es realizar un diseño e implementar un SGSI basado en el estándar ISO 27001; para respaldar la información de la empresa se gestiona una colección de datos tangibles e intangibles muy valiosos en la organización que dicha información necesita estar de manera adecuada protegida y respaldada; esta seguridad trata de prevenir accesos no permitidos, divulgación, uso, alteración o destrucción de la información; sistema de gestión se seguridad de la información (SGSI) permite a la organización identificar varios riesgos y el comportamiento de dichos riesgos que son los datos o información y activos (Guo et al., 2021).

Por los estudios realizados e indagaciones en el que se evidencia lo importante en la implementación de la norma ISO 27001 para el respaldo de la información en la organización; por lo tanto, en esta investigación uno de sus objetivos específicos es realizar un diagnóstico de la interacción que se gestiona la información de una empresa (Lopez-Leyva et al., 2020b).

También es diseñar un SGSI basado en ISO 27001 en el que se pueda implementar encuestas de evaluación para crear el diseño de la implementación de esta tecnología; en el que el sistema de gestión de la seguridad de la información (SGSI) son los más usados en el marco de diseñar recomendaciones y hoja de ruta para el gobierno de Indonesia para evitar amenazas a la información; seguridad de la información tiende a gestionar el objetivo de desarrollar, implementar, mantener y aumentar la seguridad en la organización por medio de la tabla comparativa en las

cláusulas en ISO 9001:2015 e ISO 27001:2013, en el que se puede mencionar, que son el mismo y relevante produce un diseño de sistema en gestión a la calidad en base de las cláusulas de la seguridad de la información (Institute of Electrical and Electronics Engineers, n.d.-a).

A nivel mundial los estados gubernamentales deben de proporcionar todos los recursos necesarios para operar sistema de seguridad de la información (SGSI), el objetivo es evaluar todos los riesgos asociados con los datos o información de la organización; se puede mencionar que, se debe de tener un alto nivel de calidad y un personal adecuado y capacitado que sean claves en gestionar y el sector técnico en todos los dominios de lo que es la seguridad de la información tales el: riesgo gestión, pruebas de seguridad, auditoria, seguridad y arquitectura y seguridad física; este programa de capacitación con respecto a la seguridad es el mínimo básico en dirección a todo tipo de roles; en las políticas se detallan para la comunicación de información que deben asegurar las oportunidades en mejoras y destrezas que distribuyan en los entes autorizados, normas políticas y seguridad, métodos técnicos y en caso de emergencia de cualquier vulnerabilidad o ataque cibernético (Monev, 2022).

Estos estados gubernamentales a nivel mundial han adquiridos equipos de última generación, en el que han precedido por evaluaciones de sistema relevantes y sus productos de sistema de seguridad de la información; que deben determinar las posibles soluciones con respecto a la seguridad puedan cumplir el objetivo específico de los criterios de seguridad; este software o sistema de seguridad en el que se despliegue y periódicamente para ser probados en líneas de la base de seguridad y dichos sistemas deben de ser aprobados de manera única y ser verificados los requisitos de dicha seguridad; dada que la infraestructura de componentes proporcionados por los proveedores es necesario crear una base de seguridad y así de tratar posibles riesgos externos (Malatji, 2023).

En la presente investigación examina la implementación de un modelo SGSI de mano con las normas ISO/IEC 27001:2013; permite proteger los datos públicos

comprueba y predice los fenómenos que genera por medio de pruebas de teorías y aplicaciones en base con la recolección de datos con los instrumentos necesarios para la evaluación que permite demostrar su fiabilidad; limita de manera voluntario la información precisa a la medición de las variables de estudio, se lleva a cabo la recopilación de datos mediante una revisión de documentos utilizados para extraer información valiosa que poseen las organizaciones. Este proceso facilita una comprensión más profunda de las normas estándar ISO/IEC 27001.: 2013 para un buen funcionamiento de las organizaciones que sus datos son exigentes tener una mayor protección; en esta nueva era digital de la tecnología de la información en la necesidad de implementar un sistema de gestión de la seguridad de la información bajo las normas internacionales de las ISO 27001 que aseguran a los datos de los sectores públicos (Tintin & Hidalgo, 2023).

En esta sección, destaca la importancia de la formación y la experiencia práctica en seguridad de la información, resaltando puntos observados en diversas empresas, organizaciones e incluso en industrias:

- ✓ Ampliar la familiarización con las normas ISO 27001 y las directrices de auditoría por las organizaciones de ISACA con lineamientos y normas de la seguridad;
- ✓ Tener un amplio conocimiento teórico y prácticos con la experiencia en diseños e implementación de la información métricas de la seguridad, implementar y operar el SGSI, el diseño y realización de evaluaciones.

Mediante el uso de los instrumentos de evaluación es la madurez que puede iniciar un agente que participe en las operaciones del SGSI; este instrumento respalda la información de gestión de la seguridad para la organización también así mismo del talento humano, la tecnología de la información se basa en la garantía de la calidad y seguridad física de los equipos tecnológicos con su información digital inmersa a la conectividad (Tekhnicheski universitet--Sofiia et al., n.d.).

En este apartado tiene la meta de proponer un alto nivel en la gestión para el diseño e implementación de las normas ISO/IEC 27001 para los controles de seguridad con

los lineamientos que sustentan la operación de la infraestructura del manejo de la información; las organizaciones gubernamentales son las únicas responsables de cumplir con los requisitos que rige las normas ISO 27001 a optar las directrices en el apoyo del diseño especifico de seguridad señala que las ISO 27001 y el sistema de gestión de seguridad de la información SGSI; varios enfoques en la aplicación sean posibles de asegurar la infraestructura del sistema de la gestión de seguridad de la información de cualquier organización gubernamental, empresa privada o pública (Monev, 2022).

Las normas ISO/IEC 27001 se fundamenta con la minería de datos en el que los autores determinan que la minería web es un complemento este importante y necesario para la metodología y el tratamiento de la información en la web 3.0; ofrece varias doctrinas innovadoras que busca una manera de actualizarlas que no se encuentran u obtienen fácilmente de otras fuentes que plantea críticas de obtener la información de datos de los sitios web un requerimiento difícil debido a la precaución al generar valores dentro de la web; dentro de la web 3.0 la información se relacionan con la tecnología estos sitios web son auto informados, esto quiere decir que las organizaciones no publican ningún tipo de información actualizada en sus páginas web o sitios web; son técnicas que se usan para generar palabras claves que son las industrias de las aeronáutica, espacial y defensa que su información se basa en la nanotecnología que se basan en los contextos del uso de la tecnología de la información que se gestiona con la normas ISO/IEC 27001 y el sistema de gestión de seguridad de la información (Mirtsch et al., 2021).

En la seguridad de la información se pueden identificar las amenazas y vulnerabilidades a los archivos que se llevan a cabo en una organización que será revisada y entrevistadas en base semiestructuradas; así se puede identificar que serían las causas de posibles daños potenciales a estos archivos, por lo que, se sugiere y se fundamenta hacer una lista de amenazas que existen en cada dominio de la web 3.0 y dentro de la organización estos son:

- Arquitectura de la aplicación: Ataques de virus, aplicaciones piratas informáticos invadan a la información, falla del sistema, la violación de datos
- Arquitectura de infraestructura: los servidores son vulnerables a los ataques por virus o malware, la capacidad del servidor, la sobrecarga del usuario, la energía eléctrica inestable, interferencias en la red, falla de la conectividad LAN, pérdidas de conectividad, pérdidas de dispositivos
- Datos y arquitectura de la información: pérdidas de datos, no se elabora una copia de seguridad a la información, hurto y falsificación de datos, datos no encontrados o dañados.

En esta fase de la elaboración de las posibles amenazas debe ser la responsabilidad de gestionar el área de telecomunicación, con los ingenieros en sistemas encargados de las normas de seguridad de la transferencia de la información e implementar las ISO/IEC 27001 y la SGSI; así de esta manera, se puede resguardar la información de una organización y evitar estas amenazas que existen en el día a día para dicha organización (Wicaksono et al., 2022).

En estos casos las normas ISO/IEC 27001 especifican los requisitos y se mencionó en líneas anteriores; de establecer, implementar, mantener, monitorear, revisar y mejorar en constante los sistemas de gestión de seguridad de la información (SGSI) es esencial tener una estructura que debe de contener la debida práctica con los métodos adecuados y procesos que se deba de gestionar la seguridad de los informes; las normas ISO 27001 están ancladas en siete requisitos del SGSI que es la certificación de las ISO 27001, las cláusulas que se implementa al sistema de gestión de seguridad de la información son:

1. Contexto de la organización en la administración de los sistemas de seguridad y prevenir las posibles amenazas.
2. Liderazgo en tener al personal capacitado a la gestión de los controles de la seguridad y con los agentes calificados para los certificados de entrada y salida de información
3. Planificar la gestión de la seguridad en base con las normas ISO 27001

4. Apoyo contar con los agentes y personal capacitado y profesionales en las áreas de telecomunicación y de seguridad digital
5. Operación en gestionar de manera correcta toda la infraestructura de los sistemas de datos y la arquitectura de software y de hardware para que no haya daños en los sistemas ni pérdidas de información
6. Evaluación del desempeño en el comportamiento de la tecnología de la información dentro de las redes o dentro de sitios web
7. Mejora en la implementación de la gestión de la seguridad de la información y el ajuste necesario a la aplicación de las normas ISO/IEC 27001 dentro de las empresa u organizaciones que gestionen el sistema de información

Las normas ISO/IEC 27001 no perciben de manera formal los controles de seguridad; ya que establecen con más detalle en las normas ISO/IEC 27001 toma referencia a los controles de seguridad; la organización debe de optar en implementar dichos controles para la seguridad de la información que deban de cumplir de manera oportuna y eficaz para proporcionar los requisitos que se mención en la lista anterior las directrices al implementar estos controles en las normas ISO 27001; así se gestiona una mejor práctica en la utilización de los controles de la seguridad de la información que existe lineamientos para un análisis sistemático con un enfoque general de los riesgos de ataques informáticos en las arquitecturas de la aplicación que gestione y suministre la información digital en el que esta puede ser vulnerada en cualquier sector de la industria u organización; para lograr un óptimo resultado en ciberseguridad debe de basarse en actividades y ser organizados en función de los lineamientos y requisitos que exige la ISO/IEC 27001 (Malatji, 2023).

2. 1. Sistema de seguridad de la información (SGSI)

Se puede mencionar que la definición del SGSI (sistema de seguridad de la información) es de prevenir o evitar posibles amenazas a la información, en el que le permite a la organización poder identificar los riesgos y la conducta del

tratamiento de los datos de alta vulnerabilidad con valiosos activos de la organización; la gestión de la seguridad de la información está asociada con las normas ISO/IEC 27001 que facilita unos lineamientos a seguir en el que establece que la seguridad de la información tiene el objetivo desarrollar, implementar, operar, supervisar, mantener y aumentar la seguridad de la información en la empresa u organización; que de esta manera se mejora constante el sistema de seguridad de la información se debe de cumplir con el estándar de la ISO/IEC 27001 así de establecer parámetros de protección de seguridad a la información sistemática (Guo et al., 2021).

Esta documentación tiene un objetivo de evidenciar y la definición del SGSI el uso y la implementación de un sistema de seguridad de la información sistema de gestión (SGSI) basado en las normas ISO/IEC 27001:2013; para la seguridad de la información pública este modelo hace referencia que se ha implementado en el registro de la propiedad de Pedro Moncayo Cantón (PRPMC), Provincia de Pichincha en Ecuador en la operatividad de la gestión de datos públicos; en consecuencia con el sello internacional de la ISO con respecto a la información Security, por lo tanto, referenciado en las buenas prácticas en Ecuador a nivel nacional; se usa esta metodología cuantitativa que usa el diseño del SGSI adoptado por PRPMC con la norma ISO/IEC 27001:2013 de integrar alguna normas nacionales que emitan los diferentes órganos de control pertinentes (Tintin & Hidalgo, 2023).

Se puede mencionar que otro concepto del sistema de seguridad de la información se gestiona en los ámbitos de la mejora y prevención la información de cada departamento que gestione dicha documentación; recopile, identifique, analice el potencial que se relaciona con la administración del flujo de la información de la empresa u organización para que mejore cada situación de vulnerabilidad planificar planes de mejora e implementarlos; para luego examinar y verificar la calidad, la eficacia de las medidas de mejoras en la prevención de aplicabilidad que con el fin de diseñar un SGSI; que cumpla con las normas ISO/IEC 27001 en base a los requisitos que se aplican dentro de las normas ISO 27001 (Guo et al., 2021).

2.2 ISO 27001

Se puede mencionar de lo que es la Organización Internacional de Normalización (ISO), es una norma internacional que gestiona un sistema para la seguridad de la información (SGSI); en el que existe un marco sirve de guía para el auditor y administrador de sistemas para cumplir con los estándares de gestión de seguridad de la información esta norma permite ayudar a algunos países u organizaciones para construir y mantener la seguridad de la información; asimismo, se resguarda contra los riesgos de seguridad de la información con el objetivo de aumentar la autenticidad y la confianza de las partes involucradas; en la actualidad estos estándares de la seguridad de la información han sido implementadas, así también, en Indonesia la ISO/IEC 27001 incremento para la utilización de dicho estándar en el área cibernético (Putra et al., 2021).

Dentro del ámbito de la ciberseguridad, se hace referencia al marco e ISO 27001, esta norma se conceptualiza a una de las metodologías sólidas con respecto a la ciberseguridad de la información que previenen las amenazas o infracciones de toda probabilidad relacionado con la realidad; se puede implementar una de estas metodologías para alcanzar resultados destacados, se asegura mediante la gestión de controles en la seguridad. tres pilares que son confidencialidad, integridad y disponibilidad; el ISO 27001 el NIST CFS facilitan los lineamientos políticas y procedimientos a construir un diseño para el sistema de gestión de seguridad de la información de manera estructurada SGSI, con directrices de los controles de seguridad, directrices de riesgos, implementación de controles, métricas y gestión de riesgos (CALDER & WATKINS, 2019).

Se define otra conceptualización de la norma ISO 27001 es la verificación del SGSI dentro de la organización que debe de cumplir con la ISO/IEC 27001:2013; se debe pasar por un procedimiento válido por la credencial autorizada de la organización; por la simplicidad para optar esta norma la organización debe de seleccionar los organismos de certificación registrados (RCB) para hacer un test parcial del análisis

de brechas de información; los auditores o RCB proceden a examinar, entrevistar, en base de un listado de verificación de todos los documentos relacionados luego evidenciar los informes acorde a los resultados obtenidos por la organización; esta metodología mejora la práctica en las evaluaciones de las normas ISO/IEC 27001:2013 que garanticen la presentación de los informes o documentos y examine los niveles de seguridad estándar (Chaiwut & Rueangsirarak, 2022).

2.3 Uso del ISO 27001

El uso de la norma ISO ante la implementación de estructura de seguridad de la información a nivel mundial; uno de los requisitos para el uso de la ISO es, para configurar, actualizar, monitorear, progresar de forma continua en el sistema de gestión de la información; está planeado que las organizaciones lo usen referente para seleccionar los controles dentro del método de actualización continua en el sistema de SGSI en base del ISO/IEC 27001; que se realiza un informe directo a organizaciones que se ejecuta información comúnmente que se reconocen con el uso de los controles de seguridad; se proporcionan reglas que ayuda a los instrumentos de evaluación de los datos en ejecución de la seguridad y la viabilidad en un SGSI en arreglo de la satisfacción en la verificación, examen y evaluación que es uno de los requisitos principales que indica en las normas ISO/IEC 27001 (Putra et al., 2021).

En este documento evidencia que uno de los principales uso de las normas ISO 27001 se pasa en primer plano con respecto al marco de la seguridad cibernética de NIST es utilizado adecuada por varias organizaciones que pretende hacer frente a las ciber amenazas y brechas de información vulnerable; esta norma es adecuada para las empresas que usan tecnología para envíos de información hace énfasis a los controles tecnológicos debido a las necesidades de las empresas que tenían conflictos en la seguridad cibernética; posee una configuración que simplifica su aplicación en organizaciones a nivel empresarial, siendo considerado de fácil utilización y simplificación especialmente para la alta dirección empresarial; en el

que se divide en cinco dominios identificar, proteger, detectar, responder y recuperar; una forma sistemática de categorizar la seguridad por medio de la implementación de recursos con la administración de controles tecnológicos (CALDER & WATKINS, 2019).

En la actualidad existen varios países que usan ISO/IEC 27001; es la voluntaria estándar de la seguridad de la información en el que aplica un alto rendimiento en seguridad de la información en los sectores públicos y privados, además en varios países Australia, India, Italia, Luxemburgo, México, Noruega, Polonia, Suecia, Lituano e Indonesia; muchos países estipulan el uso de esta norma ISO/IEC 27001 es una obligatoriedad la utilización de dicha norma; Alemania es uno de tantos países que requieren y usan la ISO/IEC 27001 en las comunicaciones de la información, el sector multimedia, así mismo, el sector energético, el Reino Unido también recomienda las regulaciones basadas en las ISO/IEC 27001 que indican uno de los requisitos de la administración de la información; para la gestión de la información en las ISO/IEC 27001 se debe de tener al personal capacitado para el manejo de los controles de la seguridad (Putra et al., 2021).

2.4 Invimedic S. A.

2.4.1 Visión

Ser reconocidos la mejor opción en la distribución de productos y servicios médicos para nuestros clientes, basados en procesos de calidad y un servicio de excelencia generados por nuestro equipo de trabajo.

2.4.2 Misión

Contribuir en el desarrollo de cambios positivos en la salud de los pacientes, que ofrecen productos y servicios médicos de calidad, superar continuamente las expectativas de nuestros clientes y colaboradores.

2.4.3 Producto y/o Servicio

En Invimedic tecnología y terapia somos un equipo motivado por lograr cambios positivos en la vida de los pacientes porque creemos en un mejor vivir para ellos. Desde hace 29 años nos hemos dedicado a aliviar dolencias en columna, cráneo, osteosíntesis y trastornos neurológicos.

2.4.4 Diseño Organizacional

La empresa Invimedic cuenta con su propio diseño organizacional, el cual se segmenta en distintos aspectos o áreas. Esta estructura organizativa se detalla en el siguiente mapa mental que representa las diversas áreas de la empresa Invimedic Véase en la figura 1

Figura 1. Organigrama

3. Materiales y metodología

En este apartado se evalúa la seguridad de la información de la empresa Invimedic S.A. fue en base del uso de la observación para explicar, comprobar y predecir los posibles fenómenos de amenazas; este proceso permite realizar y seguir una diversidad de acciones con una serie de pasos necesarios que lleve a cabo el debido análisis adecuado para la gestión de seguridad de la información, con los estándares e instrumentos de autentificación que demuestre su fiabilidad (Tintin & Hidalgo, 2023).

En esta sección permite distinguir, precisar los altos riesgos de amenazas que explique la utilización de un sistema de gestión de seguridad de la información para la protección de los activos; y este estudio se enfoca en la progresión de estimación al exponer una lista de todos los activos de la empresa.

El primer paso a la aplicación en la metodología es identificar la recopilación de los datos que se pudo extraer la información necesaria para llevar a cabo un estudio exhaustivo que permite crear una lista de elementos críticos de la infraestructura técnica; la debida protección y la seguridad de la información se apoya en analizar la adopción de un sistema de seguridad y protección de la información se necesita la respectiva evaluación a medida de la necesidad del manejo de la información y operación de la empresa.

De acuerdo con la situación del uso de la tecnología de la información se ejecuta en precisar una valoración equivalente y métrica que pueda confrontar los resultados de los análisis efectuados de modo independiente; estos resultados ejecutados son una parte de todos los activos que ofrece la empresa Invimedic S.A, se hallan actividades vinculadas con la administración de la información y semejante; el uso de la metodología de esta tesis de maestría los autores van a usar una tabla de comparación reducida para establecer y lograr un análisis por medio de los recursos que se cuentan en la actualidad.

Para el primer paso es usar esta tabla en el que demuestra la valoración equivalente y métrica que explique los valores numéricos y su correspondencia nominal por la utilización y basada en la metodología Magerit; esta ayuda permite a evaluar los daños que pueda padecer la empresa si sus activos se extravíen en su totalidad; el impacto de la pérdida sufrida por la empresa está directamente relacionada con los valores que se muestran en la tabla; a medida que los valores de la escala incremente también lo harán los daños que causen a los activos de la empresa Invimedic S.A. Ver en la tabla 1.

VALOR DE LOS ACTIVOS				
VALORACIÓN CUANTITATIVA		VALORACIÓN CUANTITATIVA		
MA	MUY ALTO	10	EXTREMO	DAÑO EXTRA GRAVE
A	ALTO	9	MUY ALTO	DAÑO MUY GRAVE
M	MEDIO	6 – 8	ALTO	DAÑO GRAVE
B	BAJO	3 – 5	MEDIO	DAÑO IMPORTANTE
MB	MUY BAJO	1 – 2	BAJO	DAÑO MENOR
		0	DESPRECIABLE	IRRELEVANTE

Tabla 1. Valoración métrica de los activos

En la tabla 1 se observa el valor los activos de la empresa en base de una metodología llamada Magerit en el que demuestra más detallada el valor correspondiente de los daños generados por cada impacto, valoración y degradación; se puede visualizar en la tabla los activos tienen un valor que son cualitativo y cuantitativo y cada valor enlista el tipo de daño que pueden sufrir los activos con su respectivo índice de impacto, degradación cuantitativa y valoración cualitativa.

La información detallada sobre los activos del manejo de la seguridad se recopila por medio del uso de un diagrama de sistema de gestión la información proporcionada por la metodología Magerit durante el proceso del registro de información de activos estas pestañas muestran toda la información disponible

sobre el activo que posee la empresa Invimedic, ver en la figura 2. Diagrama de gestión Magerit

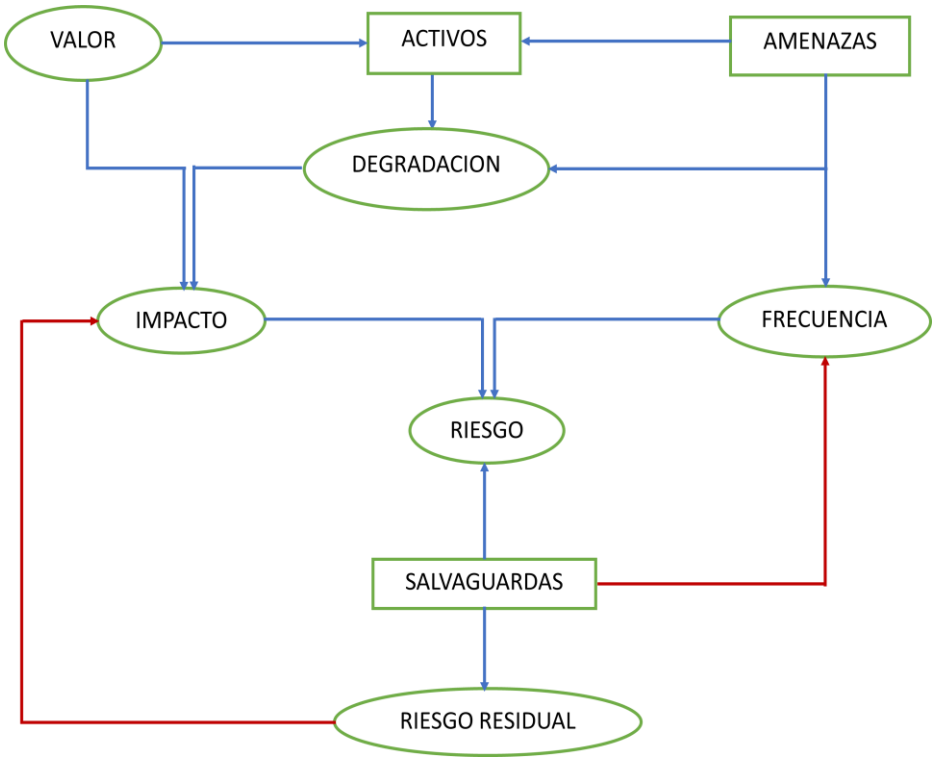

Figura 2. Diagrama de gestión - Magerit

En la figura 2 se observa que el valor mide el interés de los activos y pueden estimar el impacto; mientras tanto que las amenazas se materializan sobre los activos que pueden sufrir y causan una cierta degradación, estas amenazas ocurren con una cierta frecuencia y permiten estimar el riesgo; se puede mencionar la figura ilustra cómo los salvaguardias actúan para mitigar el riesgo. el riesgo también suaviza y limitan el riesgo a un valor del riesgo residual; y salvaguardas limitan el perjuicio de forma correctiva y la ocurrencia de forma preventiva.

Esto incluye las descripciones en los propietarios, las partes responsables (área de telecomunicación e intercomunicación y seguridad), las calificaciones de servicios, sus dimensionales y posibles dependencias con otros activos; para sintetizar y conectar un gráfico con la información de todos los activos a las dependencias con su respectiva valoración de servicios y dimensiones de los activos para que pueda generar un archivo de respaldo para cada activo; a continuación se presenta un

formato de ejemplo de la ficha de activos que se incluye en el siguiente organigrama. Ver en la figura 3. La gestión de los servicios.

Figura 3. La gestión de los servicios - dimensiones de los activos

El segundo paso es de comparar en una tabla comparativa con posibles amenazas, la degradación de los activos y tener en cuenta las probabilidades de la aplicación de las normas ISO 27001 en la actualidad con otras normas o metodologías con respecto a la aplicación de la gestión de la seguridad de la información, que se muestra en la siguiente tabla 2.

VALORACIÓN DE AMENAZAS						
DEGRADACIÓN						
PROBABILIDAD						
MA	MUY ALTO	Casi seguro	MA	100	Muy frecuente	A diario
A	ALTO	Muy alto	A	10	Frecuente	Mensualmente
M	MEDIO	Posible	M	1	Normal	Una vez al año
B	BAJO	Poco probable	B	1/10	Poco frecuente	Cada varios años
MB	MUY BAJO	Muy raro	MB	1/100	Muy poco frecuente	Siglos

Tabla 2. Valoración de amenazas - degradación y probabilidad de riesgo

En la tabla 2 que se muestra se puede describir que, las valoraciones de las amenazas de los impactos, su probabilidad en dañar la desaparición de los activos de la empresa se clasifica en escalas equivalentes en forma cualitativa, modo, cuantitativa, frecuencias, por tiempo; indica que la degradación representa el valor en materializarse el daño a los activos y la probabilidad indica que puede ser probable o no que se ejecute la degradación o en otras palabras se materialice la amenaza.

El tercer paso es de realizar un breve análisis de acuerdo con los resultados de los que indican las salvaguardas de la prevención, la degradación y la consolidación en base del tipo de activo con su dimensión de amenaza, su nivel de riesgo en los activos de la empresa. A continuación, se mostrará los pasos que se describen en la metodología. Ver en la tabla 3

TIPOS DE SALVAGUARDAS		
EFECTO	**TIPO**	**VALOR %**
Preventivas: Reducen la probabilidad	**{PR}:** Preventivas **{DR}:** Disuasorias **{EL}:** Eliminatorias	**80 %** **15 %** **5 %**
Acotan: La degradación	**{IM}:** Minimizadoras **{CR}:** Correctivas **{RC}:** Recuperativas	**75 %** **20 %** **5 %**
Consolidan: El efecto de los demás	**{MN}:** De monitorización **{DC}:** De detección **{AW}:** De concienciación **{AD}:** Administrativas	**35 %** **25 %** **15 %** **25 %**

Tabla 3. Tipos de salvaguardas: Efecto y tipos

En la visualización de la tabla 3, se observa que salvaguardas son las dimensiones a proteger, los tipos de archivos, las amenazas, y reflejan dos categorías que son: el efecto y el tipo, por lo tanto, se detalla que el efecto son las dimensiones de protección para fortalecer con el objetivo de minimizar las posibles amenazas de cada activo; la categoría tipo indica las medidas de control y se base en el principio de la proporcionalidad que valoriza cada tipo es el caso de la preventiva, la disuasoria, eliminar que se encuentran en la categoría efecto de prevención en el que se reducen las probabilidades de amenazas; la minimización, la correctiva, recuperativa se encuentran en la categoría efecto de acotación porque el activo pierde una parte de su valor y el monitoreo, detección, concienciación, administrativa se encuentran en la categoría de consolidación se relaciona con las demás categoría con su respectivo nivel por cada tipo.

A continuación, se detalla el nivel de eficacia y madurez de las salvaguardas. Ver en la siguiente tabla 4.

EFICACIA Y MADUREZ DE LAS SALVAGUARDAS		
FACTOR	**NIVEL**	**SIGNIFICADO**
0 %	Level 0	Inexistente
5 %	Level 1	Inicial / ad hoc
25 %	Level 2	Reproducible – intuitivo
50 %	Level 3	Proceso definido
75 %	Level 4	Gestionado y medible
100 %	Level 5	Optimizado

Tabla 4. Eficacia - madurez salvaguardas

En la tabla 4 se demuestra la importancia de mantener las salvaguardas implementadas en la estructura de la seguridad de los activos proporciona, evidencia la eficacia y madurez de los controles de seguridad de las salvaguardas que se evidencia con sus respectivos factores, niveles y sus significados que detalla en que cada factor tiene su índice porcentual y con su respectivo significado.

El cuarto paso por seguir es el valor del impacto residual y puede aplicarse las salvaguardas ante las amenazas y las pérdidas de los activos; también se pueden observar dos enfoques relacionados con las salvaguardas frente a los impactos residuales.

En el que se podrá visualizar con los enfoques propuestos en la misma tabla. Ver en la tabla 5.

IMPACTO RESIDUAL
IMPLEMENTACIÓN DE LA SALVAGUARDA
- Se ha reducido el impacto desde un valor potencial a un valor residual
- El activo, su valor y sus dependencias no han cambiado
- Se ha reducido la magnitud de la degradación
IMPACTO RESIDUAL
- Acumulado sobre los activos inferiores
- Recuperado sobre los activos superiores

Tabla 5. Las salvaguardas - impacto residual

En la Tabla 5, se observa que la introducción de salvaguardias conlleva una mejora y reducción de los riesgos o amenazas a los activos. Dado que los valores y dependencias de dichos activos son inalterables, se logra disminuir los impactos residuales que podrían afectar a los activos superiores.

El quinto y último paso para seguir es el valor del riesgo residual que puede aplicarse las salvaguardas ante las amenazas y las pérdidas de los activos; también se pueden observar dos enfoques relacionados con las salvaguardas frente a los riesgos residuales. En el que se podrá visualizar en la siguiente tabla con los enfoques propuestos en la misma tabla. Ver en la tabla 6.

IMPACTO RESIDUAL
IMPLEMENTACIÓN DE LA SALVAGUARDA
- Se ha reducido el impacto desde un valor potencial a un valor residual
- El activo, su valor y sus dependencias no han cambiado
- Se ha reducido la magnitud de la degradación
IMPACTO RESIDUAL
- Acumulado sobre los activos inferiores
- Recuperado sobre los activos superiores

Tabla 6. Las salvaguardas - riesgo residual

En la tabla 6, se puede mencionar que la implementación de las salvaguardas mejora y minimiza los riesgos o las amenazas a los activos que sus valores y sus dependencias no pueden cambiar de esta manera, se logra reducir la incidencia de impactos residuales en los activos de nivel superior

4. Resultados y discusión

4.1 Situación inicial

Esta sección se menciona que la planificación se declara en la visión, misión de la empresa Invimedic que permite analizar la situación inicial interna y lo externo de ésta; establecer los objetivos generales que formulan los planes de la seguridad de la información para lograr los objetivos planteados; esta evaluación inicial que tiene la empresa Invimedic le permite identificar los planes de acción y las estrategias necesarias en salvaguardar sin aplicar las normas ISO 27001; la situación inicial de la empresa al no aplicar las ISO son métodos de trabajo en la seguridad con el fin de cumplir objetivos y metas a corto, mediano y largo plazo con la condición del medio que opera y gestiona la información de ésta empresa.

Por el análisis de la situación inicial de la empresa Invimedic se puede aplicar tres herramientas para un diagnóstico óptimo a la empresa.

El análisis PEST también conocida PESTEL permite identificar y evaluar los posibles cambios y características en el entorno que puede afectar el éxito de la empresa; es una herramienta que aprueba y evalúa los factores, las relaciones y éstas puedan afectar a la empresa tanto en el presente y en el futuro; el término PEST significa acrónimo que involucra los medios políticos, económico, social y tecnológico en el marco de un entorno que se desenvuelve la empresa; este análisis es usado para realizar una evaluación exhaustiva de los factores ya mencionados en relación con su razón social; estos análisis tienen el objetivo de analizar y examinar todas las oportunidades y posibles amenazas que afecten a partir de estos factores.

Al aplicar esta herramienta se puede obtener beneficios para realizar un óptimo análisis PEST sin aplicar las ISO 27001:

- ✓ Ayuda a detectar oportunidades y ofrece una alta advertencia de amenazas. significativas que afecten la información de la empresa Invimedic.
- ✓ Evita posibles fracasos luego no recuperar todos los activos de la empresa Invimedic.
- ✓ Proporciona una visión general de todas las influencias externas e internas en el marco del entorno de la empresa Invimedic.
- ✓ Apoya una mejor toma decisiones en base a la gestión y aplicar esta herramienta sin las ISO 27001.

En esta herramienta el análisis de PEST se describe los cuatro factores:

- ✓ Factores políticos.
- ✓ Factor económico.
- ✓ Factor social-cultural.
- ✓ Factores tecnológicos.

En la clasificación de los factores descritos, describen las características de cada factor descritos en el diagrama 1 de PEST; en el factor **político** es determinar las medidas de que un gobierno influye en la economía de la empresa que se subdividen en las políticas fiscales, aranceles comerciales, entre otras características que pueden afectar a la empresa Invimedic; en el factor **económico** se desarrolla el aumento de la inversión que ayuda a generar mejores tomas decisiones y aumenta la utilidad de la empresa Invimedic; en otro ámbito el factor **social-cultural** son aquellos elementos que proceden de un entorno cercano la familia, amigos, compañeros de trabajo y los que impactan en el que ayuda con las tomas decisiones para la empresa Invimedic; el último factor **tecnológico** son todos los adelantos de todas las ciencias y los productos tecnológicos, dispositivos, plataformas digitales para verificar las acciones empresariales de la empresa mencionada y su crecimiento a nivel nacional Invimedic, se muestra en la figura 4.

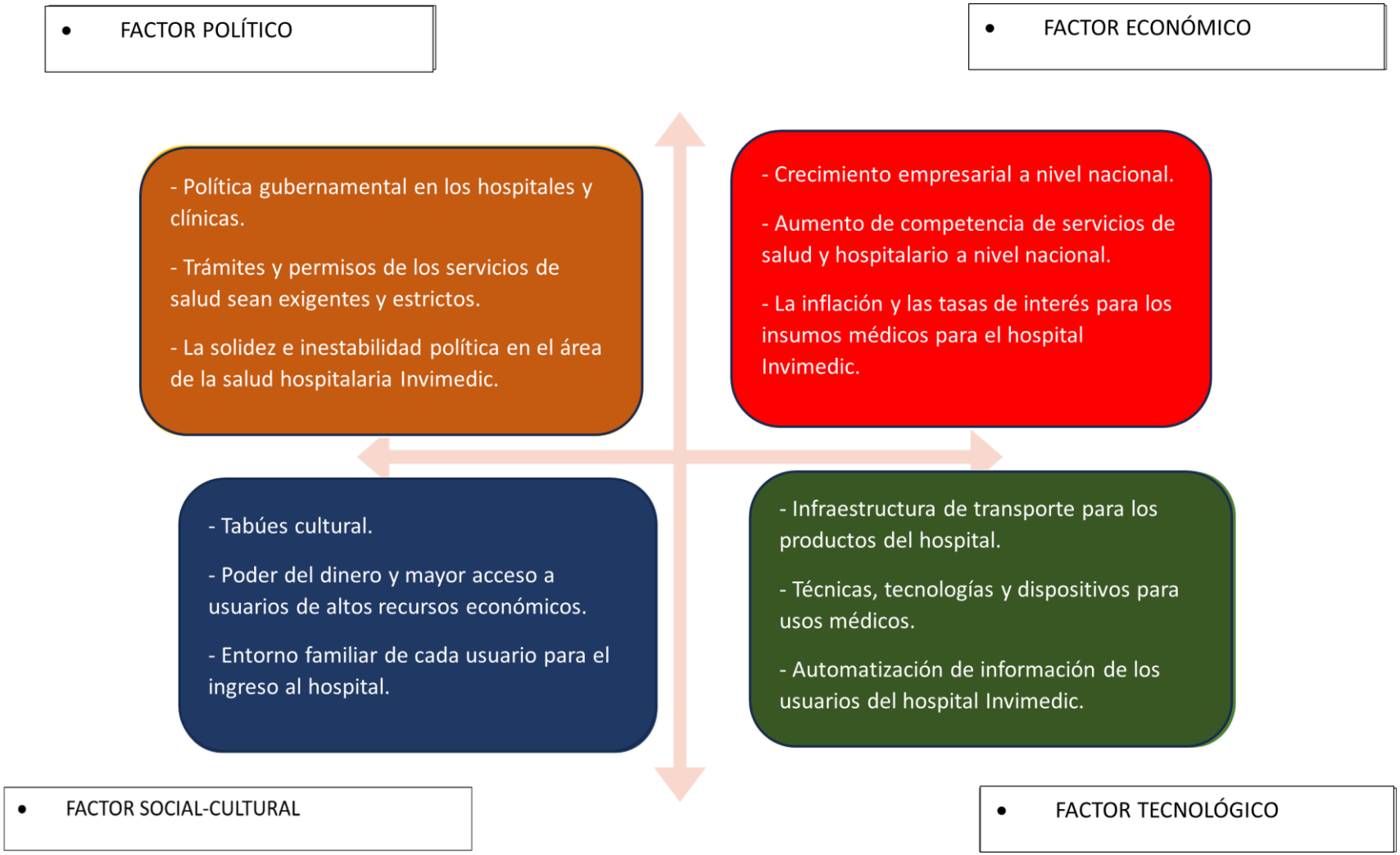

Figura 4. Factores de Pest – empresa Invimedic

Se puede mencionar otra de las herramientas aplicables sin implementar las ISO 27001; se tiene el estudio de las cinco fuerzas de PORTER esta herramienta identifica la influencia de la competencia en la toma de decisión empresarial con un modelo de estudio competitivo que analiza la negociación de los clientes, de los proveedores y la amenaza de productos que son representados el producto entrante; esta herramienta se analiza a nivel estratégico tiene un enfoque al análisis el potencial para la adquisición de clientes, proveedores y los nuevos competidores potenciales que puedan afectar toda la información sin ninguna norma de seguridad para sus activos; estos elementos ya mencionados (clientes, proveedores, productos, competidores potenciales y competencia), se puede mencionar que, el análisis de las cinco fuerzas de PORTER se puede determinar elementos para las cinco fuerzas de PORTER:

- ✓ Poder de negociación de los clientes.
- ✓ Poder de negociación de los proveedores.
- ✓ Amenazas de productos o servicios que oferta la empresa.
- ✓ Amenaza de entrada de los nuevos competidores para la empresa.
- ✓ Rivalidad y extravíos de los activos de la empresa.

La herramienta de PORTER, muestra las principales características que influyen en la empresa Invimedic; por lo que se menciona, que en cada característica la empresa Invimedic tiene el **poder del cliente** que tiene la libre libertad de negociar si este desea quedarse por los beneficios que oferta la empresa Invimedic; por otro lado se menciona el **poder de negociación de los proveedores** en esta característica se menciona que estos entes importan los productos o los insumos médicos para el hospital Invimedic es acotar que los precios suben por cada importación, por motivos de la derivación o ubicación de procedencia de los mismos; y por último la **competitividad del mercado**, dentro del marco de esta característica influye variedades de productos originales o genéricos, por lo que los genéricos tienen precios bajos y económicos y fácil adquisición que puede bajar los servicios hospitalarios de Invimedic, ver en la figura 5.

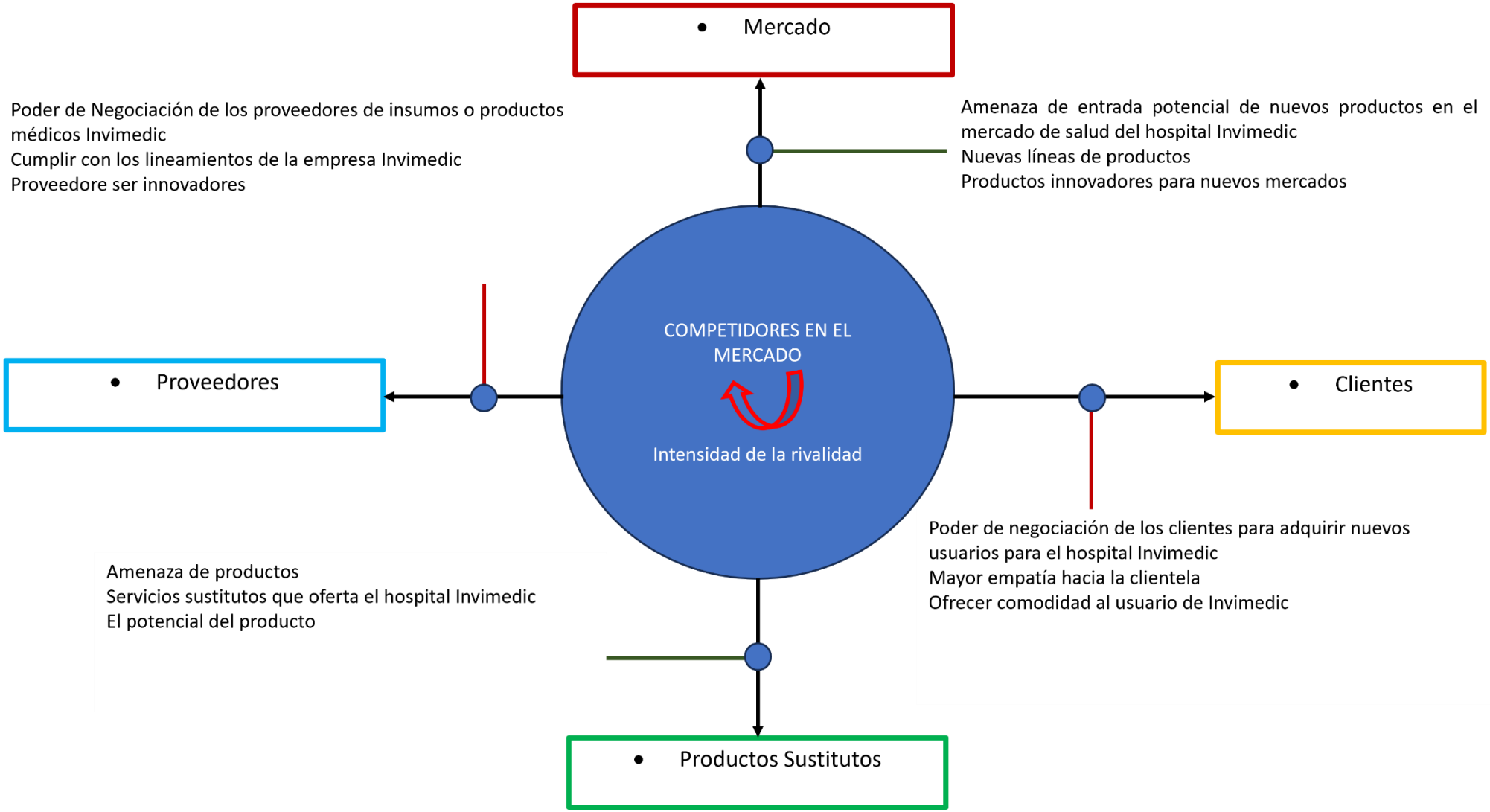

Figura 5. Los elementos de PORTER – empresa Invimedic

De acuerdo con Waterman Consultores existe una herramienta denominada el modelo de las 7 S (Siete eses) este instrumento de análisis permite enfrentar las diversas dificultades y problemas de desarrollo de la información que son capaces de diagnosticar y atajar rápidamente el origen del problema o la amenaza con el fin de implicar las siete partes de la empresa que se enfocan con el objetivo en común. (Consultores McKinsey, n.d.)

Este modelo de las siete S se identifica para tener una gestión eficaz con el cambio de su estructura, estrategia, personal, estilo, sistemas, valores y habilidades que enmarca de forma útil para la empresa que tiene diversas funciones; reconocer los aspectos del cambio organizativo identifiquen las áreas de oportunidad al usar este modelo implementado de manera efectiva.

El modelo proporciona un marco integral para la entrega de la información y los cambios que se genere a nivel empresarial desarrolle e implemente un plan que tendrá resultados favorables en el tratamiento de la seguridad de la información en base de las 7 S (Siete eses).

Así mismo, ayuda a gestionar y promover un alto nivel de confianza y viabilidad en los diferentes niveles de gestión de la empresa; existe el riesgo de resistencia a los nuevos cambios de la gestión de seguridad de la información las ISO 27001 que son normas para salvaguardar los diferentes activos de la empresa, los recursos humanos, personal médico y los pacientes; para garantizar una cultura en la organización empresarial y no afecte de manera negativa estos recursos sin el uso de las normas ISO 27001.

En este diagrama 3 de las 7 S (Siete eses) permite identificar todos los componentes de la empresa Invimedic que genere una gestión eficaz, calidez en la prestación de servicios hospitalarios y todos sus recursos se describen en la figura 6.

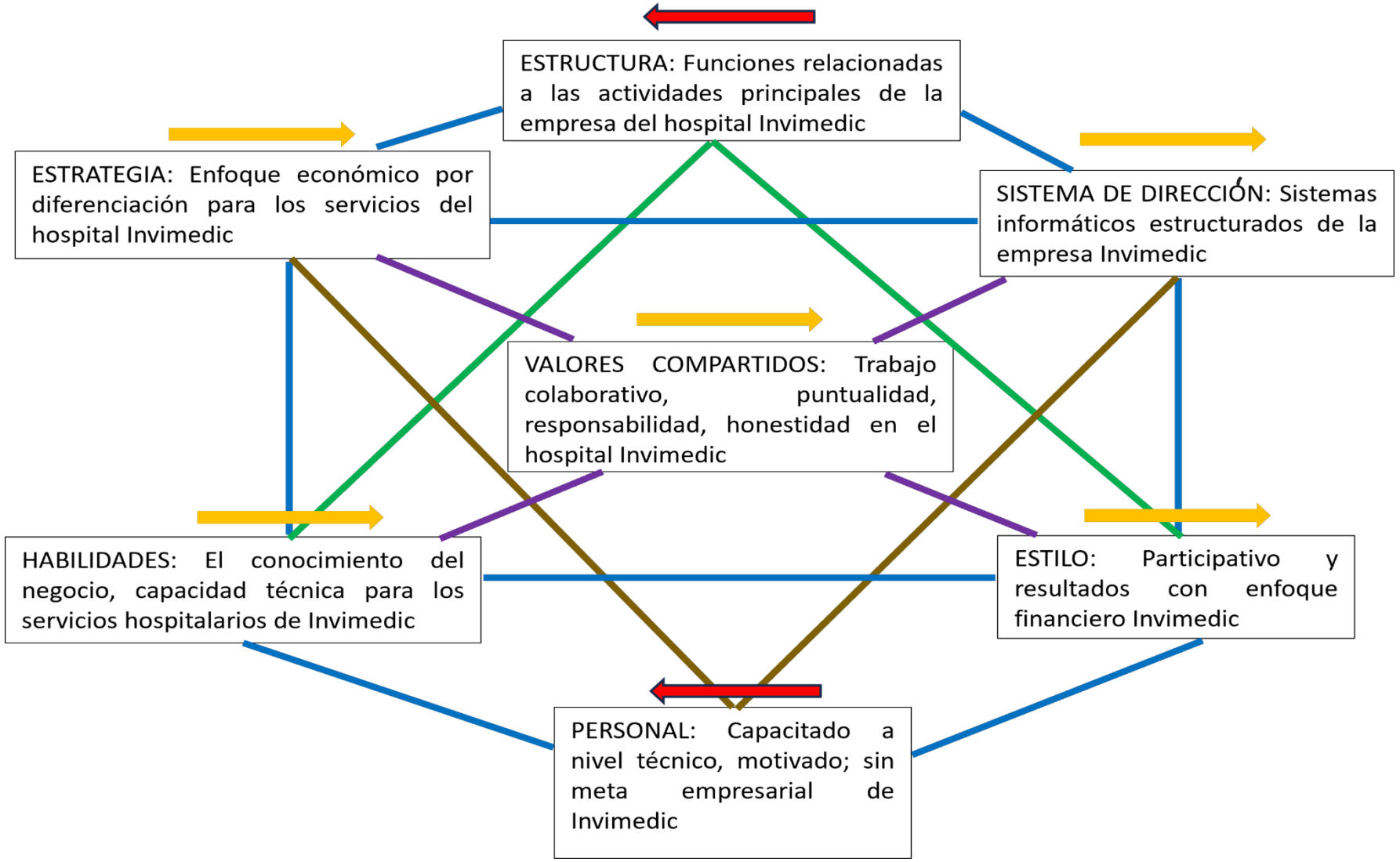

Figura 6. El método de las siete S – empresa Invimedic. Consultora McKinsey

4.2 Diseñar e implementar un SGSI en ISO 27001

En esta sección se describe que la empresa Invimedic propone un diseño para el sistema de gestión de seguridad de la información en base a las normas de seguridad estándar internacional las ISO 27001; se puede mencionar después de una revisión extensa de varios artículos relacionados a la implementación de las normas ISO 27001 son aceptadas a nivel mundial que se observa en la redacción de este proyecto; tiene la finalidad implementar un diseño elaborado para la seguridad de la información en base de una metodología llamada Magerit, Esta metodología se estructura en cinco pasos fundamentales, cuya importancia se destaca en la sección de materiales y metodología. Se utiliza esta guía como referencia para orientar la protección de los activos de la empresa Invimedic.

La documentación es experimental porque usa una metodología de diseño de seguridad de sistema de la información que propone en esta investigación.

Se puede mencionar que los resultados esperados se efectuaron por la realización de los debidos pasos y la revisión de la literatura propuesta en capítulos anteriores, el proyecto de la investigación son analizadas y respondidas en esta sección del documento; al realizar se explica el desarrollo de acuerdo los pasos mostrados en el capítulo anterior, después de un estudio exhaustivo y selección se obtuvieron 25 artículos, el desarrollo se refleja en la tabla 1, que se muestran con los valores de los activos que se centra en dos valores importantes que son la cualitativa y cuantitativa; estos valores representan los siguientes campos: Muy alto, alto, medio, bajo, muy bajo; en el valor cuantitativo se muestra los indicadores de valor por cada campo con su respectiva característica de daños.

A continuación, se muestran los resultados de los intervalos de la valoración métrica de los activos en base a la siguiente ilustración que ayuden a comprender las

descripciones en el siguiente gráfico que visualiza los resultados de la tabla 1 en la sección anterior.

Ver en la figura 7, se interpretan los valores altos son aquellos que representan una categoría mayor de daño con su respectivo indicador de daño al valor de los activos; puede mencionar que los resultados de los indicadores de campos del valor de los activos son los números de paso, que X1 (indicadores en la tabla 10) indica el número de pasos del resultado proporcionado, así mismo ver en la tabla 7.

RESULTADOS PROPORCIONADOS		
DESCRIPCIÓN	**PRE – TEST**	**POST – TEST**
Número de resultados proporcionados	10	0 – 1

Tabla 7. Resultados - logrados

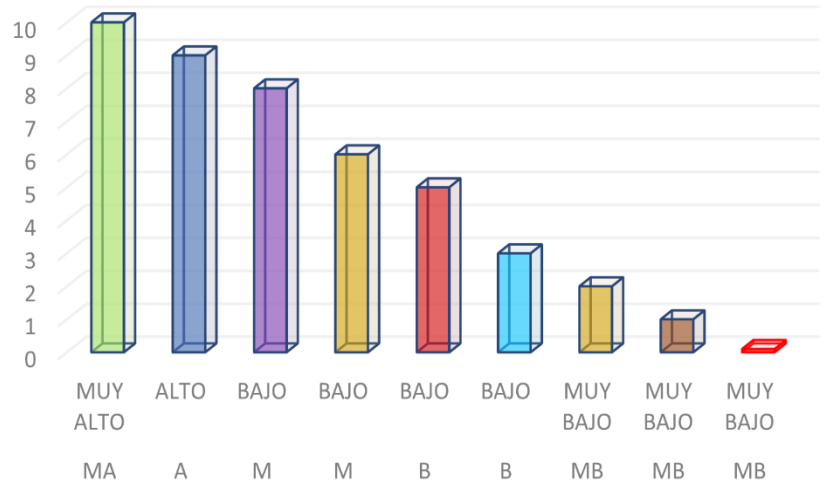

Figura 7. Indicador del valor de los activos

El número de resultados proporcionados en el **POST – TEST** se extrajo la cantidad de los resultados proporcionados que se tienen en base de la figura 7 hace referencia a la valoración métrica de los activos para la implementación de las normas ISO 27001; en los resultados de la representación gráfica son el resultado logrado de la investigación exhaustiva realizada y aplicada; el resultado del

indicador son los resultados proporcionados X1.1 (indicadores en la tabla 10), indica la entrega de resultados con respecto al argumento de la investigación. Ver en la tabla 8.

DIAGRAMAS DE PROCESOS		
DESCRIPCIÓN	**PRE – TEST**	**POST – TEST**
Número de diagrama de proceso	0	1

Tabla 8. Número de diagrama - Magerit

El número se resultados de la evaluación del diagrama en el **POST – TEST** se extrajo la cantidad de los procesos que se alcanzaron en la construcción del modelo de pasos a seguir para la implementación de las normas ISO 27001; en el resultado del indicador X2 del diagrama de proceso es el resultado esperado. Ver en la tabla 9.

GESTIÓN DE SERVICIOS		
DESCRIPCIÓN	**PRE – TEST**	**POST – TEST**
Número de categoría de la gestión de servicios	0	1

Tabla 9. Gestión servicios - descripción

El número se resultados de la evaluación del organigrama de la gestión de servicio en el **POST – TEST** se extrajo la cantidad de los procesos que se alcanzaron en la construcción de la gestión de seguridad en el modelo de pasos a seguir para la implementación de las normas ISO 27001; el resultado del indicador X2.1 (indicadores en la tabla 10) indica la descripción de cada paso de los resultados proporcionado en base de la gestión de servicios.

Se puede observar que las valoraciones de las amenazas tienen una mayor probabilidad de generar agravio a los activos de la empresa Invimedic y se muestra

en el gráfico; el resultado del estudio de la tabla 2 de la sección anterior es evidente que los indicadores para implementar las normas ISO 27001. Ver en la figura 8.

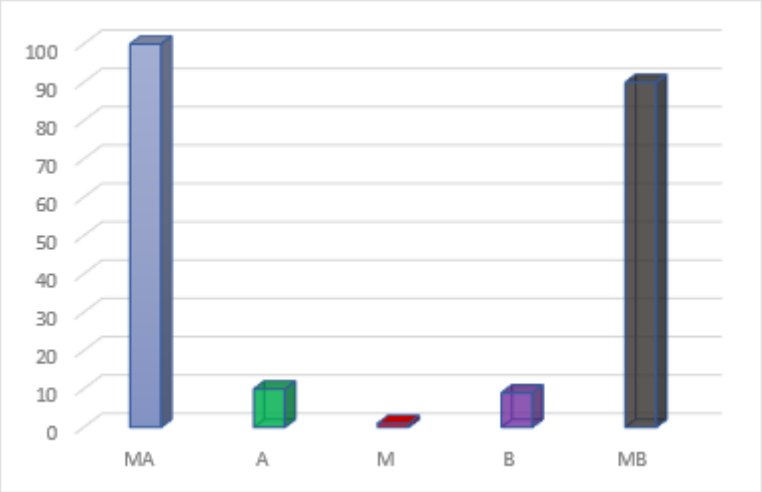

Figura 8. El valor amenazas – degradación, probabilidad

En la siguiente figura se observa que las salvaguardas genera una protección a medida sea alto el indicador del porcentaje en probabilidad de proteger los activos, los sistemas, los equipos tecnológicos, la arquitectura de los diseños de seguridad de la información en base de cada tipo con su respectivo efecto; el resultado se extrajo de acuerdo con la tabla 3 **Tipos de salvaguardas** propuesta en el capítulo 3 materiales y metodología es el resultado logrado que se espera para la implementación de las salvaguardas de los activos de la empresa Invimedic. Ver en la figura 9.

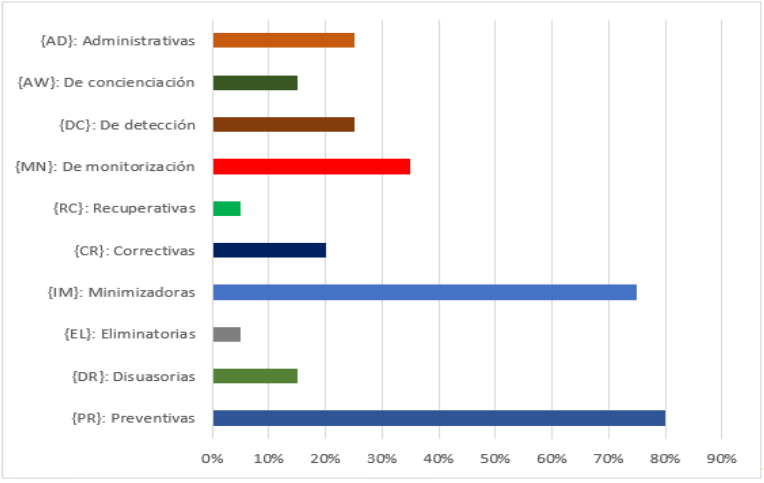

Figura 9. Las salvaguardas

En esta gráfica se observa a los indicadores para la aplicación de las salvaguardas a los sistemas de gestión de seguridad son aceptados por sus resultados obtenidos que indican, si están en el mayor valor del factor con su respectivo nivel de madurez, esto quiere decir, que son aplicables e implementar las salvaguardas en la empresa; el resultado se extrajo de los datos de la tabla 4 exhibido en la sección anterior. Ver en la figura 10.

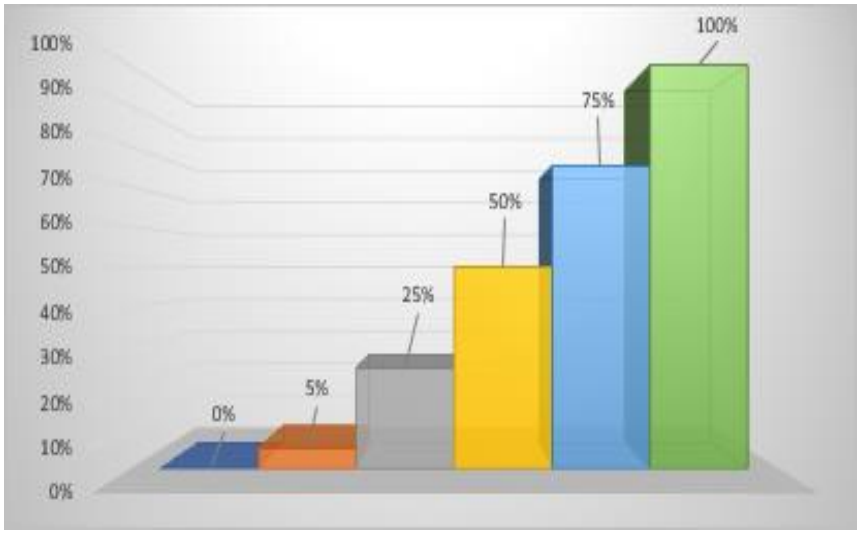

Figura 10. Eficacia - madurez salvaguardas

En esta sección el desarrollo del diseño de sistema de seguridad de la información para la implementación de las ISO 27001, adopte la metodología de Magerit se lo plantea en la tabla 4 **Eficacia y madurez de las salvaguardas** de la sección 3 materiales y metodología de este documento, por medio de los resultados obtenidos del gráfico propuesto de la figura 10, se puede ver que la realización de las normas ISO 27001 con el diseño de gestión de sistema de seguridad de la información; se mencionan los impactos residuales son las salvaguarda tiene sus fases aceptables; por lo tanto también existe el impacto residual que pueden afectar de manera negativa las posibles afectaciones a los activos que están en los niveles inferiores y se pueden repercutir los activos superiores; se da el análisis de que la aplicación de las normas ISO 27001 con las salvaguardas son aplicables para la gestión de seguridad de la información.

En resumen, el riesgo residual de la tabla 5 y la tabla 6; responden que la implementación de la salvaguarda es la reducción de los riesgos potenciales para un valor residual del activo con sus dependencias que no cambien y reduce la magnitud de la probabilidad de todos los posibles riesgos; así mismo los valores de los riesgos residuales son acumulados respecto a los activos inferiores y repercuten sobre todos los activos superiores; se muestra en la figura 11.

Figura 11. Riesgo residual

De acuerdo con lo documentado se puede decir que la implementación de las salvaguardas reduce los posibles riesgos potenciales a los sistemas de información de la empresa Invimedic; genera el debido respaldo con un alto índice de seguridad de los activos de la empresa.

En la sección de resultados identificamos los tipos de las variables y con su respectivo indicador de evaluación. Ver en la tabla 10 y la tabla 11.

VI: Diseño de un modelo SGSI con las normas de seguridad ISO.

VD: Implementación de las normas ISO 27001.

MEDIDA	INDICADORES
Pasos de procesos	X1: Número de pasos X1.1: Entrega de resultados
Procesos	X2: Número de estructura de pasos X2.1: Descripción de cada paso X2.2: Valor de porcentual de cada paso

Tabla 10. Indicadores de cada paso y proceso – diseño de SGSI

MEDIDA	INDICADORES DE PASO
Descripción de cada paso	Y1: Valores de las normas implementadas
Criterios o punto de vista	X2: Evaluación de criterios de la implementación

Tabla 11. Implementación de las normas ISO 27001

Se puede observar que las tablas muestran las distintas partes o pasos a seguir para generar un mayor uso y ejecución de un diseño de SGSI y las normas ISO 27001, para ser aplicada en la empresa Invimedic.

Se puede mencionar que la gestión seguridad de la información y la aplicación de las normas ISO 27001 para salvaguardar los diversos activos de la empresa Invimedic; se puede visualizar una ilustración que se representa los pasos a seguir para la implementación de las normas ISO 27001; además se puede visualizar las evaluaciones que los sistemas de información deben de gestionar antes y después de realizar un estudio a todos los posibles casos de amenazas e implementar la seguridad de la información; tener la debida documentación para que la empresa pueda cumplir con los requisitos que implementa las ISO 27001; finalmente en la ilustración se visualiza el trabajo colaborativo de diferentes áreas de telecomunicación con los ingenieros y el personal capacitado para la gestión de los

controles técnicos y de seguridad que se debe de implementar las ISO 27001 en la empresa Invimedic. Ver en la figura 12.

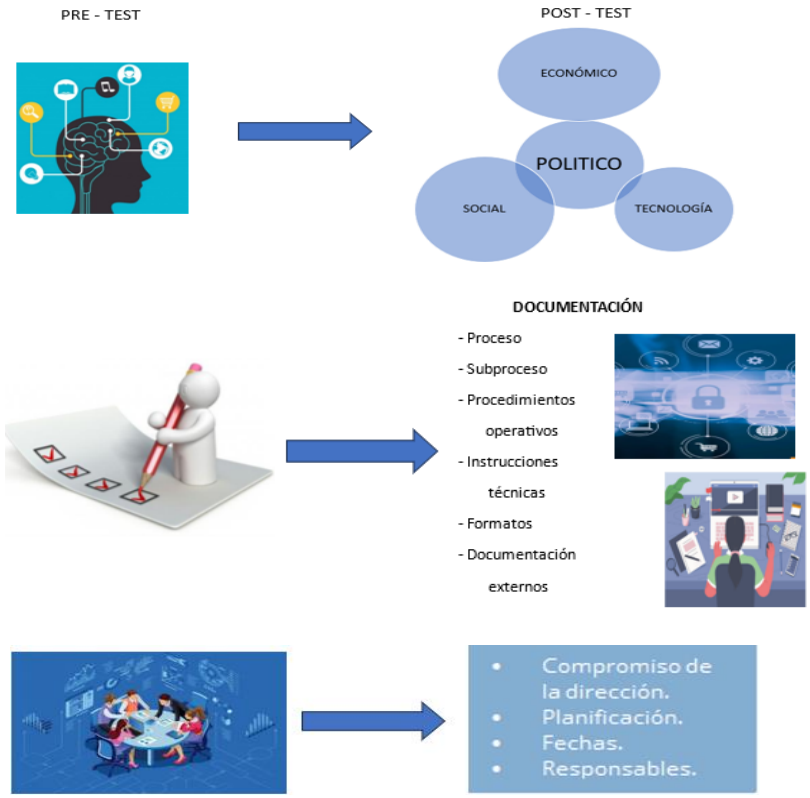

Figura 12. Pasos a implementar las ISO 27001

La implementación de las normas ISO 27001 se debe de elaborar una guía de un SGSI, debe de tener en cuenta las siguientes fases con sus respectivas derivaciones en implementar en el sistema de gestión de seguridad de la información para así generar la aplicación de esta SGSI junto de las normas ISO 27001, que se puede ver en la figura 13.

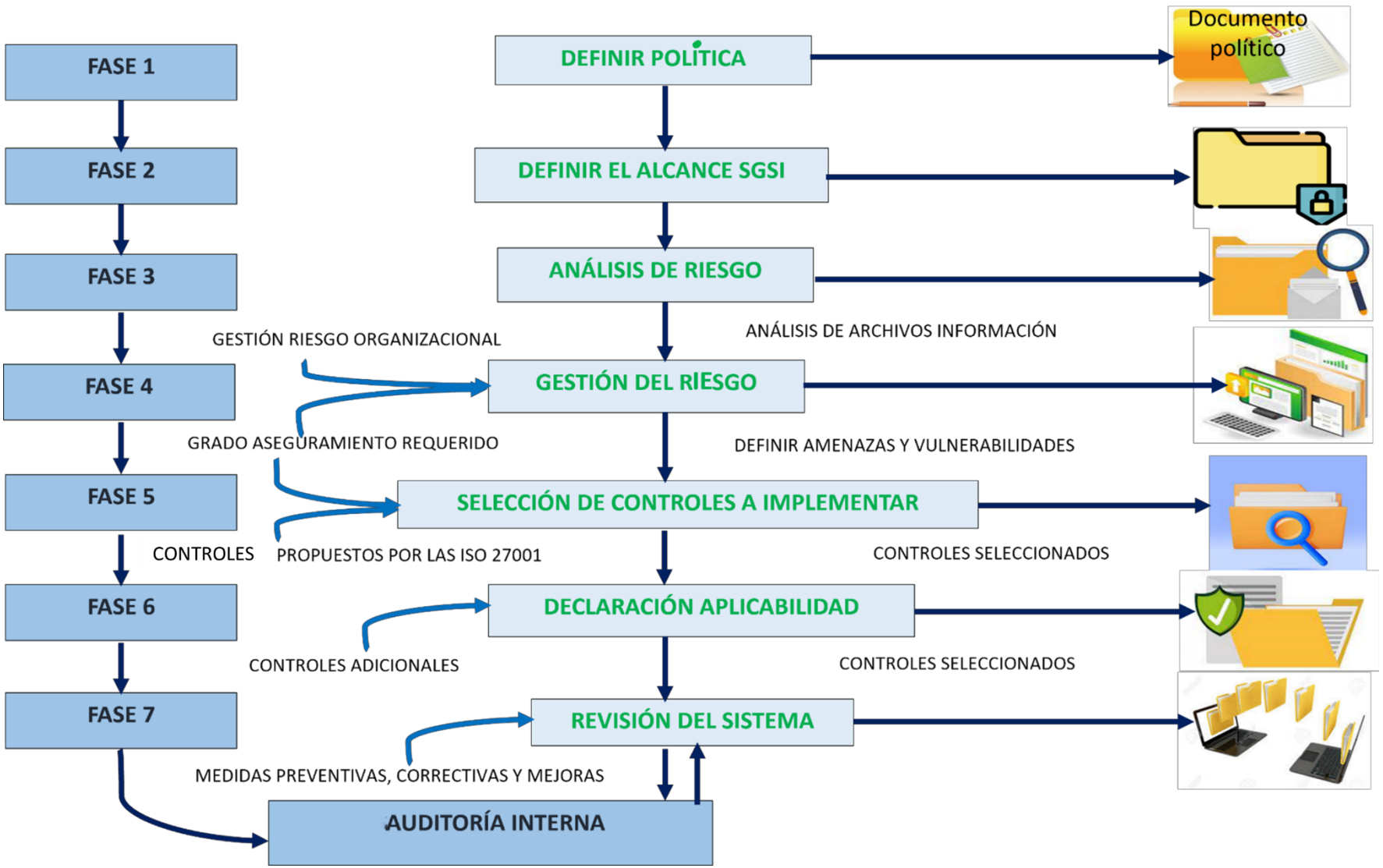

Figura 13. Implementación SGSI

En la figura 13 se observan los elementos o fases para la implementación de un SGSI:

- **FASE 1: Definir la política**

  La empresa Invimedic debe definir los siguientes parámetros:

  - ✓ En la hora de implementar un sistema de gestión de seguridad de la información (SGSI) en base a las normas ISO 27001 en la empresa Invimedic, se considera un eje central es la evaluación de riesgos de este sistema; permite a la gerencia empresarial es tener una visión precisa para definir el alcance de aplicación de las normas ISO 27001 con el SGSI; se tienen las políticas y las medidas en aplicar que es integrar una mejora continua en todas las normas ISO que beneficie a la empresa Invimedic.
  - ✓ Al implementar la política de seguridad de la información a nivel organizacional, permitir que estas normas de la política de seguridad de la información cumplan con los requisitos y llegar a ejecutar los principios de los objetivos internos y externos y la responsabilidad de al flujo de la información general del personal médico y de los pacientes y se define así:

    - Se deduce a la gestión de toda incidencia que deben de garantizar los que desarrollan los procesos adecuados para ejecutar dichas tareas necesarias en la empresa Invimedic.
    - Invimedic define a cada personal en colaborar con las necesidades de las incidencias como la comunicación y la seguridad de la información de cada cliente o paciente.

  - ✓ La evaluación continua se detalla de esta manera:

    1) Es identificar los activos de información que gestione la empresa Invimedic que todo activo tiene su valor dentro de la empresa,

incluido las estructuras físicas, intelectuales o informativas la marca y la reputación, que no afecten de manera negativa a la empresa Invimedic.

2) Es identificar las vulnerabilidades y debilidades de los activos, en que los activos no se vean afectados por ataques o daños que gestione la empresa Invimedic.
3) Estas evaluaciones identifican las posibles amenazas que son aquellas que pueden suceder y dañar los activos de la información, estos pueden ser desastres naturales o ataques cibernéticos en contra de la empresa Invimedic.
4) Esto permite que los requisitos legales y contractuales que la empresa Invimedic está obligada a cumplir con las necesidades de sus usuarios, socios y/o proveedores que se relacionen con la empresa Invimedic.
5) Además, permite identificar los riesgos es definir los activos y la probabilidad de las posibles amenazas o las vulnerabilidades propias de cada activo que puedan ser afectadas de manera parcial o en su totalidad en relación con la disponibilidad, confidencialidad e integridad de los activos que contienen la información en la empresa Invimedic.
6) Esta evaluación permite el cálculo del riesgo que realiza a partir de la probabilidad en ocurrencia y el impacto que tiene sobre la empresa, la ecuación que se aplica es **(riesgo = impacto * probabilidad de amenaza)**, con esta ecuación se puede determinar con exactitud los riesgos que deben ser controlados con prioridad de la empresa Invimedic.
7) Cabe mencionar que se tiene un plan de tratamiento del riesgo este punto la empresa Invimedic está preparada para definir la política de tratamiento de amenazas en referencias de los puntos anteriores propuestos o redactados en el documento que se defina por la alta

gerencia de la empresa, es aquí donde se selecciona los controles de seguridad en cada posible riesgo:

1) Asumir el riesgo.
2) Reducir el riesgo.
3) Eliminar el riesgo.
4) Transferir el riesgo.

La gestión de seguridad de la información son la clave en la prevención del fraude online, robo de identidad o daños a los sitios web, pérdida de datos personales que evita a la empresa exponga todos sus activos a amenazas informáticas.

Las normas ISO 27001 abarca con la seguridad de la información, ayuda a la empresa Invimedic a mejorar y minimiza los riesgos que puedan afectar a la información; en la actualidad la fluidez de la transferencia de la información es necesario implementar un sistema de seguridad de la información (SGSI), un enfoque sistemático e informático que permite gestionar la información de manera confidencial de la empresa aporta su seguridad de los mismos activos, así mismo, el personal calificado de la empresa Invimedic y sus procesos de los sistemas de tecnología de la información (TI).

El diseño de la implementación del SGSI e ISO/IEC 27001 otorga una alta confianza entre los clientes, los proveedores de la empresa Invimedic puede ofrecer la seguridad de la información dentro del marco empresarial; aplicar la técnica de procesos y afrontar las amenazas de la información con la alta gestión de seguridad de la información que administre la empresa Invimedic.

La empresa Invimedic aplica las ISO 27001 que propone dentro del contexto de la gestión de seguridad de toda la información de posea y administre la empresa Invimedic; esta información tiene mucho valor por los conocimientos y experiencia del personal que la tratan en sesiones de la alta

seguridad, el área de sistemas de telecomunicación que gestiona el sistema de seguridad SGSI y sus propios activos de la empresa Invimedic.

La implementación de un SGSI en la empresa Invimedic posibilita la identificación y gestión de los riesgos a los que la empresa podría enfrentarse. De este modo, se puede eliminar o aplicar las medidas necesarias para resguardar los activos de manera efectiva.

La reducción de los riesgos es por medio de los controles, los protocolos, las políticas y monitoreo de los procesos que minimice las amenazas de un modo notable; en el caso que presente una posible amenaza relacionada con los activos, la empresa está preparada para tomar las medidas necesarias y actuar de manera inmediata que minimice el impacto de posibles daños que puedan afectar a la empresa.

Se menciona **la reducción de costes** que optimiza todo el proceso de un test de esta manera detectar amenazas para eliminar aquellos procesos ineficaces, así conseguir mayor ahorro en costes de la seguridad de la información que beneficie la mayor inversión en gestionar la seguridad que beneficie a la empresa Invimedic.

La integración de la seguridad de la información en la empresa requiere de la implicación de todo el personal que esté relacionado en la administración y generar la información, cambio de mentalidad y todos los activos de la empresa para la seguridad de cada componente fundamental y beneficie al generar la empresa Invimedic en los servicios hospitalarios.

Cumplimiento de la normativa vigente en seguridad la empresa Invimedic tiene lineamientos que debe de cumplir con las leyes nacionales e internacionales para la protección de los activos y los datos que garanticen el respaldo en todos los niveles o áreas de la empresa.

Gestión de incidentes de seguridad la empresa Invimedic debe hacer un análisis de los riesgos no eliminados en su totalidad y las posibles vulnerabilidades residuales pueden existir incidencias en la seguridad de la información que no se puedan identificar; Invimedic implementará las medidas necesarias para estas incidencias con los siguientes requisitos:

- ✓ Detectar: es de informar y evaluar los incidentes de la seguridad de la información.
- ✓ Responder: con las medidas de seguridad para todas las incidencias que surjan en la información.
- ✓ Reportar: todas las vulnerabilidades, por ejemplo, brechas de datos o ciberataques.
- ✓ Aprender: a identificar todas las posibles incidencias en la política de seguridad de la información de la empresa Invimedic.

Incremento de la competitividad este sistema dispone de una certificación acta y calificada en las normas ISO con la seguridad para la competencia, los clientes tendrán una confianza y seguros de compartir sus datos personales, bancarios, gustos y similares al saber que la empresa usa las mejores prácticas en garantías de datos seguros que oferta la empresa Invimedic.

Educación y capacitación la empresa Invimedic está en constante capacitación para el personal encargado de bienestar y salud:

- ✓ La empresa de la competitividad del personal en la atención en la resolución de incidentes y mantener un plan de capacitación en el ámbito de la seguridad de la información.
- ✓ Tener los debidos procedimientos para la detección, análisis y elaboración de informes de incidentes en la seguridad de la información.
- ✓ Realizar procedimientos para tener una comunicación eficaz y precisa en la empresa Invimedic.

- **FASE 2: Definir el alcance SGSI**

Se define el alcance del sistema de gestión de seguridad de la información SGSI, son los límites de la implementación del SGSI en la empresa Invimedic que tiene el objetivo de realizar una toma de decisión de seleccionar los activos que desee proteger; estos activos que son la información que gestiona la empresa es protegida en forma independiente es almacenada, procesada o transferida interno o externo del sistema SGSI; la información está disponible y fuera del alcance no implica que no aplica las medidas de seguridad de los activos; la responsabilidad de gestionar el alcance del sistema del SGSI en la empresa Invimedic.

Entre estas características que se basa el alcance del SGSI son la integridad, la confidencialidad y la disponibilidad.

Integridad la información debe estar en forma exacta e inmutable en su utilización; al momento que los activos de la empresa pueden ser modificadas sin la debida autentificación de credenciales que provenga del personal encargado de la seguridad de los activos de la empresa, de tal manera sean autenticados sin alguna justificación legal por parte de la empresa Invimedic.

Confidencialidad en este apartado los datos que gestione la empresa son confidenciales que no pueden ser patentizados a personal externa de la empresa o entidades; la información es el valor prioritario y de propiedad que usa de manera única y exclusiva por la empresa Invimedic.

Disponibilidad es una característica contraria a la confidencialidad; a pesar de ello, un SGSI hace referencia a la potencia a las oportunidades y necesidades de las personas, empresas o procesos que se autentifiquen y puedan tener paso a la información de la empresa Invimedic.

- **FASE 3: Análisis de riesgo**

En esta fase lo primero que debe analizar el impacto en la empresa con un fallo de la seguridad que implica la pérdida de las tres características mencionadas en la fase del alcance del SGSI que representa el activo de la información de la empresa Invimedic; evalúa de forma realista la probabilidad de ocurrencia de este fallo en seguridad se relaciona a las amenazas, vulnerabilidades o impactos en los activos que gestiona la empresa Invimedic.

Cabe mencionar que es necesario analizar las consecuencias potenciales de muchas y diferentes niveles de gravedad; en simple separación de los activos y la información de extravió o robo de datos importantes o secreto por parte de la empresa Invimedic.

La empresa Invimedic tiene que realizar una posible evaluación de riesgos comprendida en fases:

1) Recoger y preparación de la información.
2) Identificar, clasificar y valorar los grupos de activos.
3) Reconocer y clasificar las amenazas.
4) Identificar y estimar las vulnerabilidades.
5) Establecer y valorar los impactos: identificar, tipificar y valorar los impactos.
6) Evaluar y analizar el riesgo.

1) Recoger y preparación de la información

Se puede mencionar en este punto el sistema de gestión de seguridad de la información SGSI para la empresa Invimedic; la información es todo activo que gestione en el tratamiento y el proceso de la recopilación y preparación de la información son organizadas por parte de la empresa; de forma independiente que almacena o transmita el origen de la

elaboración de la respectiva documentación ser presentado por toda la empresa Invimedic.

Estas prácticas se basan en las normas ISO 27701 que describe los objetivos de controles recomendables en la gestión de seguridad de la información; estas normas ISO 27001 tienen 39 objetivos de control, 133 controles en 11 dominios.

Se puede mencionar que la preparación de datos es aquel que son preprocesamiento que consiste en limpiar y consolidar los datos sin antes de procesar, usar para el respectivo análisis de la empresa Invimedic; también es la preparación de todos los datos en forma minuciosa y es comprensible para el debido y correcto análisis de datos implementado por la empresa Invimedic; la realización de este proceso de validar, limpiar y que los datos aumenten sin ser procesados en la obtención precisos e importantes para la empresa, este análisis depende de la eficacia en la preparación de los datos en las etapas iniciales en la empresa Invimedic.

La importancia de la preparación de los datos depende de las decisiones de la gerencia de la empresa; la preparación de datos debe ser cuidadosa, exhaustiva y garantice a los analistas sentirse seguros en la dicha preparación, una mayor comprensión que generen consultas con respecto a los datos ingresados y consten en el sistema de la empresa, este análisis proporciona análisis precisos e importantes de la empresa Invimedic.

Este proceso en la recopilación y preparación de la información en las siguientes descripciones:

a) **Adquisición de datos:** es la determinación de los datos que se necesitan para establecer un acceso consistente para hacer un test, analizar y ser confiables para el

tratamiento de la información que gestione la empresa Invimedic.

b) **Exploración de datos:** este punto hace referencia a la calidad de los activos, datos, la revisión de la distribución del análisis en la relación de cada variable y así comprender de una mejor forma en el desarrollo de los respectivos análisis propuesto en la empresa Invimedic.

c) **Limpieza de datos:** es la mejora de la calidad de la presentación de los datos, con su respectiva producción en la elaboración de los documentos, de tal forma, permanecer limpios en el momento de la implementación y el uso del sistema de gestión de seguridad de la información SGSI implementada por la empresa Invimedic.

d) **Transformación de datos:** en este punto cabe mencionar en darle formato, orientación, adición y enriquecer el conjunto de los activos en el tratamiento de la información y los datos usados para el análisis en la producción de los activos más significativos que represente a la empresa Invimedic.

2) Identificar, clasificar y valorar los grupos de activos

En este punto en identificar, clasificar y valorar de forma cuantitativa o cualitativo que pueda brindar un mejor trato y seguridad en función del interior de los procesos para cumplir y alcanzar los objetivos definidos por la empresa Invimedic.

Para identificar los grupos de activos permite en determinar los activos de la información que forman parte del inventario de la empresa; el responsable de seguridad de la información es orientar la adecuada

identificación de los mismos en conjunto con el personal encargado de seguridad de la información y el personal institucional son los encargados de coordinar aspectos importantes con los alcances ya definido en la planificación institucional de seguridad de la información en la empresa Invimedic.

En la fase de la clasificación se ingresan los procesos más importantes para la empresa sea este el medio de presentación en físico o digital; los tipos de la información son la estrategia, información de archivos personales, información del área administrativa, la información de los procesos legales de la empresa, entre otros aspectos que les represente un coste económico con el objetivo de que cumplan con las normativas legales.

3) Reconocer y clasificar las amenazas

Este punto hace referencia que el sistema de gestión de seguridad de la información SGSI basado en las normas ISO 27001 en identificar, analizar las principales amenazas para establecer la adecuada planificación y evaluación de dichos riesgos.

Las amenazas pueden interpretarse de algunos modos de ataques externos, infecciones malware, inundaciones, incendios o corte de fluido eléctrico; puede presentarse debido a las omisiones o están despistados por el personal encargada de la gestión de seguridad de la información de la empresa Invimedic.

Es recomendable de elaborar una adecuada coordinación en la gestión de riesgos que permita a la empresa conocer las principales vulnerabilidades o amenazas de los activos de la información, el debido proceso de identificar los riesgos implica lo siguiente:

a) **Identificar todos aquellos activos de la información:** son aquellas que dan valor a los activos de la empresa Invimedic.
b) **Asociar las amenazas relevantes con los activos**: son identificados por la empresa Invimedic.
c) **Determinar las vulnerabilidades:** es aprovechar dichas amenazas y convertirlas en oportunidades para la empresa Invimedic.

Se puede analizar el nivel de impacto en la empresa en base al fallo de la seguridad en la pérdida de la confidencialidad, la integridad o disponibilidad de los activos, con evaluaciones acuerdo a la probabilidad de ocurrencia en relación con las amenazas, vulnerabilidades e incluso los impactos en todos los activos que gestione la empresa Invimedic.

Además, se analizan las consecuencias potenciales que representan muchas y otros casos de gravedad en base a la dispersión o pérdida de la información o robo de datos importantes y confidenciales en el marco de la empresa Invimedic.

En estos elementos o fases del análisis de riesgo consiste en que la empresa Invimedic cumpla con uno de sus objetivos; es de aplicar las salvaguardas en los activos que gestione la empresa Invimedic; en la implementación de las normas ISO 27001 se ejerce el liderazgo del sistema de seguridad de la información en la empresa; establecer un plan de trabajo que se defina la división de las diferentes actividades que establecen la exactitud y tienen que hacer cada actividad o función para ser ejecutada por la empresa Invimedic.

Las normas ISO 27001 implementa la representación de dueño del riesgo que asocia en cada amenaza potencial; el personal se asegura que se cumplan las disposiciones de distintas actividades empleadas por la empresa Invimedic; el personal que está encargado de ejecutar la gestión de seguridad de la información no son los únicos que pueden realizarla, sino

también puede el personal que tenga la capacidad y este calificado para el manejo de los controles de seguridad de forma responsable y puedan cumplir con las disposiciones establecidas por la empresa Invimedic.

Es importante definir la estructura organizacional del SGSI, con la selección del personal adecuado e idóneo con la condición del tamaño de la empresa, el alcance que tenga la implementación y el alcance del SGSI se determina la cantidad del personal acorde a los perfiles profesional que integrarán parte del grupo de trabajo seguridad de la información de la empresa Invimedic.

Las normas ISO 27001 para la implementación del SGSI se implementa, automatiza y mantiene la plataforma Isotopos que facilita la debida automatización de las ISO 27001; tal forma cumple con los requisitos en base al ciclo planear – hacer – verificar – actuar (PHVA) que se usan para establecer, implementar, mantener y mejorar los sistemas de gestión de seguridad de la información complementa las mejoras en las prácticas y controles definidos y establecidos por las ISO 27001 implementadas en la empresa Invimedic.

Los estándares más empleados en las normativas ISO 27001 se encuentran detallados y definidos con el propósito de su clasificación:

a) **Disponibilidad:**

   Es la propiedad de sus recursos y su utilización en el momento que se lo requiera la empresa Invimedic.

b) **Confidencialidad:**

   Es la información que está disponible que no es divulgada a personas externas, entidades u organizaciones en procesos no autorizados por la empresa Invimedic.

c) **Integridad:**

La propiedad es de salvaguardar la veracidad de los activos de la empresa Invimedic.

d) **Seguridad de información:**

Es la preservación de la confidencialidad, integridad y disponibilidad de la información; pueden estar involucradas y otros aspectos la autenticidad, responsabilidad, y confiabilidad.

Cabe mencionar que en estas fases se aplica el PDCA:

a) **Planificar:**

En esta etapa se pueden establecer las respectivas políticas, los objetivos, procesos y los procedimientos importantes en la gestión del riesgo y mejorar la seguridad de los activos de la empresa; en el aspecto de la política se definen los lineamientos de la seguridad y los requerimientos legales relativos a la seguridad de la información; establecer los criterios al evaluar al riesgo y ser aprobada por la gerencia de la empresa Invimedic.

Además, en esta etapa se define la evaluación del riesgo adecuado para la implementación y los requerimientos de la empresa y establece los criterios de aprobación del riesgo debe especificar los niveles de riesgo apropiado para la empresa Invimedic.

b) **Hacer:**

Esta etapa se selecciona e implementan los controles que reduzcan el riesgo a los niveles considerados graves y peligrosos para la empresa; efectuar el cambio con las pruebas proyectadas según la toma de decisión y la planificación que se desarrolló en Invimedic.

c) **Verificar:**

Después de realizar todas las etapas ya mencionadas en líneas anteriores las acciones e implementación de los controles, se debe de verificar, evaluar y medir el desempeño de los procesos ejecutados frente a las normas políticas, los objetivos, experiencias prácticas y evidenciar los resultados para su respectiva revisión por parte de la gerencia de la empresa Invimedic.

d) **Actuar:**

Etapa es la toma de acciones correctivas y preventivas en base a los resultados demostrados por parte de la auditoría interna del SGSI, revisión general u otro activo importante de tal forma para mejorar la implementación del sistema de gestión SGSI en base de las normas ISO 27001 implementado por la empresa Invimedic.

4) Identificar y estimar las vulnerabilidades.

En esta etapa de la fase de la implementación del sistema de gestión del SGSI es identificar las principales vulnerabilidades que más se destacan en el sistema del SGSI:

a) Interfaz de usuario complicada:

Para estimar esta vulnerabilidad es identificar y tener un buen diseño en la interfaz, el usuario debe entender en completar en forma primordial para ejecutar con eficacia, la mejor práctica posible estar satisfecho al terminar todos los procesos que gestione la empresa Invimedic.

Estos ciclos del diseño de la interfaz tienen cuatro pasos principales:

1. **Recopila toda la información**: de los usuarios y las tareas a ejecutar.
2. **Realiza los diseños:** optativos y novedosos de la interfaz.
3. **Crea prototipos**: de los mejores diseños para probar y cumplir con las apariencias principales en la realización de las tareas.
4. **Evalúa**: la usabilidad y utilidad de la interfaz del usuario.

En esta vulnerabilidad de la interfaz y al recopilar la información debemos tratar de responder las siguientes preguntas: ¿Quiénes son los usuarios? ¿Por qué se ejecutan las tareas? ¿Cuáles son los problemas en los usuarios?; las respuestas a estas preguntas son la combinación en base de encuestas, foros, focos groups, entrevistas y observaciones directas de la gestión de las actividades o tareas a realizar en la implementación del sistema de gestión SGSI y la gestión del usuario en el sistema de seguridad SGSI y las normas ISO 27001 implementada en la empresa Invimedic.

b) Contraseñas predeterminadas no modificadas:

Las contraseñas predeterminadas por el sistema SGSI implica que la comunicación entre dispositivos los usuarios no tiene una debida importancia con la seguridad de las credenciales; los errores más frecuentes en la gestión de seguridad de las credenciales es de no cambiar las configuraciones y contraseñas por defecto que no trata de sistemas operativos o plataformas, sino que, con la llegada de la tecnología de la información (TI) que abre un abanico de opciones en los sistemas de gestión de seguridad de la información SGSI implementada ISO 27001 que puede generar un problema mayor en un futuro; los puntos más

críticos en esta etapa está ligado al uso del usuario con clave genérica que está ya predeterminada de fábrica en todos los dispositivos o en los equipos de telecomunicación; el usuario no procede en generar cambios de estas credenciales, es muy frecuente que expuestas a los ataques cibernéticos de forma remota a cualquier punto de dispositivos o equipos que están interconectadas entre sí en la empresa Invimedic.

La concurrencia de esta mala práctica genera un uso frecuente entre dispositivos o equipos de la empresa estos son el router con su credencial predeterminada que usa un valor predefinido con valores numéricos para emparejarse; estos dispositivos comparten una extensa información privada de los usuarios e incluso los valores predeterminados por el fabricante, por lo tanto, emplea la importancia de cuidar la seguridad en el manejo o la gestión de la seguridad de los activos o la información de la empresa Invimedic.

Sin embargo, es realizar la debida revisión de los cuestionarios básicos de la seguridad que debe ser lo primordial es el cambio de las credenciales de predeterminadas no modificadas antes de conectar con los sistemas de comunicación de la información que la absoluta funcionalidad y seguridad de la información de la empresa Invimedic.

Entre los dispositivos con más vulnerabilidad en generar claves predeterminadas y fácil acceso a los posibles ataques cibernéticos es el router, estos tienen puntos de acceso vulnerables que son de fácil ingreso por parte de los cibernéticos, que pueden causar posibles y graves daños a la pérdida de la información de la empresa Invimedic.

c) Sensibilidad del equipo a los cambios de voltaje:

La sensibilidad de los equipos con respecto a los cambios de voltaje son dependientes al tipo de carga de tensión eléctrico, los ajustes de los controles de su uso específico; no se puede identificar las características de los cambios de voltaje que afecten a los equipos característica más frecuentes son la magnitud de los voltajes, cambios de fase y desequilibrio, falta de voltaje, desequilibrio trifásico de voltaje. Estos cambios de voltaje se clasifican en:

a) **Equipo sensible a la magnitud de voltaje:**

Son aquellos equipos relevadores de baja tensión, controles de procesos, controles de arranque de motores.

b) **Equipo sensible a la magnitud y duración de la tensión de voltaje:**

Son todos los equipos que usen fuentes de poder o alimentación electrónicas; es importante mencionar que estos equipos duran con voltaje cuidado medio de la raíz (RMS), debajo del valor especificado e implementado en los equipos de la empresa Invimedic.

c) **Equipo sensible a otras características:**

Algunos equipos son afectados por otras características que es el desequilibrio de las fases durante los eventos de la tensión de voltaje u oscilación transitoria que ocurra durante el disturbio; son sutiles en la magnitud y la duración de sus impactos que son difíciles de detallar con alguna certeza; los índices de estos comportamientos es la variación de los RMS, son las características más

frecuentes entre la magnitud y la duración de la tensión de electricidad.

d) Inadecuada seguridad del cableado:

En las empresas corporativas tienen una mala gestión en lo que respecta a la seguridad del cableado de los equipos de telecomunicación por lo general, el personal encargado de esta seguridad no procede con la debida gestión en dar un seguimiento adecuado para el cableado de los equipos de la empresa Invimedic; cabe mencionar la importancia de la protección del cableado sea este de energía y de comunicaciones en los sistemas de información; evitar lo posible en que haya daños de las infraestructura con las diferentes interferencias que afecten a los datos de la empresa Invimedic. Por lo tanto, se rige con las debidas precauciones:

a) Los cables deben estar bajo tierra hasta el punto de acceso de la instalación.
b) Los cables de potencia deben de estar distanciados de los cables de comunicaciones para evitar interferencias.
c) Los accesos del cableado hacia los equipos deben de estar asegurados según corresponda los cables protegidos para cada función del cableado.
d) Tener en cuenta las medidas adicionales que puede realizar los técnicos en los cableados de comunicación para los equipos no autorizados que estén conectados por medio del cableado.
e) El cableado de las salas de servidores y centros de datos deben estar aislados de manera segura para evitar la conexión de equipos o dispositivos no autorizados.

f) Tener en cuenta siempre el acceso restringido y controlado a los paneles de conexión y de control.

e) Mantenimiento inadecuado:

El mantenimiento de los equipos a escala empresarial o corporativa no recibe el debido mantenimiento, por lo que genera, una gran pérdida de información en los equipos, e incluso daños en la infraestructura del cableado las salas que están los servidores. Por lo tanto, garantizar los equipos mantenerse de forma adecuada y segura para no deteriorarse y están de forma operativo. Por esta razón debe de seguir lo siguiente:

a) Las recomendaciones del fabricante para el mantenimiento de los equipos.
b) Solo el personal autorizado debe de dar mantenimiento a los equipos y de sus registros.
c) La información sensible debería ser eliminada de los equipos en su debido momento.
d) Cumplir con todos los requisitos de las pólizas de seguro de los equipos.

4) **Establecer y valorar los impactos: identificar, tipificar, y valorar los impactos.**

Para establecer los impactos de ISO 27001, debe realizarse una evaluación y el tratamiento de riesgos que consiste en:

a. **Identificar:** los activos, amenazas y vulnerabilidades que afecten la seguridad de la información de un SGSI.
b. Estimar: consiste en la probabilidad y el impacto de cada riesgo, que considere los criterios de la aprobación y normas establecidas por la empresa Invimedic.

c. **Determinar:** permite describir el nivel de riesgo y compararlo con el riesgo aceptable.
d. **Seleccionar:** son las opciones de tratamiento de riesgo más adecuadas, evitar, transferir, mitigar y aceptar el riesgo.
e. **Implementar:** las medidas de control necesarias para reducir o eliminar el riesgo.
f. **Revisar y monitorear:** en forma periódicamente el proceso de gestión de riesgos y los resultados obtenidos.

5) **Evaluar y analizar el riesgo.**

Su principal fundamento es identificar y analizar las importantes amenazas para poder evaluar dichos riesgos; es decir, es evaluar las consecuencias condicionales para poder evaluar su criticidad.

- **FASE 4: Gestión de riesgo**

En la empresa Invimedic la implementación de un sistema de gestión de seguridad de la información (SGSI), este sistema requiere un conocimiento en gestión de riesgo; después de precisar los riesgos existentes de la empresa, esto permite tomar las medidas correspondientes y adecuadas para afrontarlos.

Invimedic cuenta con un software llamado Risk Management, el cual se constituye como una herramienta fundamental para la gestión, reducción, transferencia o eliminación de todos los riesgos que puedan afectar a los activos de la empresa.

1) Consiste en descartar los activos que este asociado a los riesgos es costoso, por lo tanto, se suele buscar todas las posibles alternativas.
2) Transferir el riesgo son aquellos que se valoran la subcontratación del servicio externo o de un seguro que cubra cualquier incidencia dentro del centro de riesgo; es importante mencionar que la

subcontratación pueda aplicar debe de cumplir el requisito que los activos de la empresa sean mayores en relación del seguro.

3) Asumir el riesgo implica a la empresa Invimedic tomar decisiones con respecto a las medidas de seguridad a los riesgos; estas decisiones son aplicadas por la alta gerencia de la empresa factible en el caso de que la empresa gestione y controle por medio del monitoreo estos riesgos no aumenten.
4) Mitigar el riesgo es aquella acción que la empresa deba implementar todas las medidas posibles que actúen con las salvaguardas para los activos que se administren dentro del marco empresarial; estas medidas implementadas son documentadas y gestionadas por la empresa Invimedic.

Una vez aplicada las medidas y son adoptadas es para identificar estos riesgos, se realiza un análisis y se muestra el resultado parcial se obtiene el riesgo residual y el nivel de riesgo aceptable por la empresa Invimedic.

- **FASE 5: Selección de controles a implementar**

La implementación de las ISO 27001 en la empresa Invimedic se enfoca en las salvaguardas, la confidencialidad y la integridad de los activos, igual a los sistemas que se encargan de gestionar la seguridad de la información.

Las normas ISO 27001 tienen como objetivo proporcionar un modelo que facilite o administre el establecimiento, implementación, monitoreo, revisión y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI).

Las ISO 27001 tiene un enfoque en base a la seguridad de la información es fomentar que los usuarios enfaticen con la empresa Invimedic.

1) Entender los requerimientos de seguridad de la información de la empresa y su necesidad de establecer su política y sus objetivos.

2) Implementar y operar controles para manejar los riesgos de la seguridad de la información.
3) Monitorear y revisar el desempeño y la efectividad del SGSI.
4) Mejorar continuo en base a la medición del alcance del objetivo.

Entender los requisitos en la seguridad de la información, es considerar e implementar los controles para la seguridad para el uso en el sistema de gestión de seguridad de la información SGSI, las normas ISO/IEC 27001; esta norma tiene un enfoque a la gestión de los controles acorde a los atributos, la introducción de temas, la actualización de un conjunto de controles y las prácticas en la seguridad de la información en las ISO 27001 con el sistema de gestión de seguridad de la información SGSI.

Los usuarios que tienen acceso a la selección de los controles del sistema de seguridad en la empresa Invimedic tienen que estar capacitados para implementar, monitorear y gestionar todos los procesos que generen los activos de la empresa.

- **FASE 6: Declaración aplicabilidad**

La implementación de las ISO/ IEC 27001 y la aplicabilidad de un sistema de seguridad SGSI, es un documento formado por la organización empresarial en la gestión de los controles de seguridad de los activos y/o la información evaluable que están en los lineamientos y requerimientos de las normas ISO 27001 que tiene la empresa Invimedic.

La implementación de un SGSI en la organización empresarial de Invimedic con su respectiva descripción, motivos y su estado; hace referencia para esta ejecución de medidas de protección de los activos, la empresa Invimedic, agregar más controles de seguridad y sus objetivos para la gestión y aplicación de la seguridad necesaria para la empresa Invimedic.

Una vez realizado el respectivo análisis y la evaluación de la innovación que la empresa Invimedic adquiere; tiene que definir todas las posibilidades en el tratamiento de los riesgos y tomar la decisión de mitigarlos, una de las características para la aplicación del sistema de seguridad de la información; puede registrar el formato más conveniente para la empresa Invimedic, para su importancia y contenido en los controles de seguridad:

1) Los controles estándar.
2) Aplicar las justificaciones.
3) El estado de implementar.
4) Documentar los procedimientos, evidencias.
5) Todos los datos adicionales que se registren.

También se puede mencionar que, en la declaración de la aplicación del sistema de seguridad SGSI tiene una gran importancia para la organización empresarial de la empresa Invimedic y le permite:

- La declaración de aplicabilidad permite la relación entre los controles de las ISO 27001 y lo que desea la empresa Invimedic.
- Proporciona una visión amplia que realiza la empresa para salvaguardar su información, identificar, los registros acuerdo a las medidas de seguridad implementada.
- Permite justificar la inclusión o exclusión de cada uno de los controles de seguridad o apariencia que no incluyen dentro del informe de la evaluación de los controles de seguridad.
- La empresa Invimedic implementará y aplicará un SGSI para las normas ISO 27001 en el marco de la seguridad de la información de la empresa Invimedic.
- Documentar cada control de seguridad aplicable e indicar su implementación, ser una guía principal para todos los auditores de sistemas de seguridad empresarial tanto interno y externo; el auditor tiene acceso a la función de aplicabilidad, por lo

tanto, se desarrolla la auditoria y verificar el cumplimiento de los requisitos para la realización de SGSI y su aplicabilidad en las normas ISO/IEC 27001 para el beneficio de la empresa Invimedic.

Así mismo la empresa Invimedic realiza la debida y adecuada revisión con su respectiva actualización en los controles de seguridad en base a la declaración de la aplicabilidad de las normas ISO 27001 implementada en la empresa Invimedic y estas son:

1) La documentación es verificada y aprobada por el área encargada de aplicar la seguridad de la empresa y actualizar alguna presunción que apliquen nuevos controles para la seguridad y revisar las implementadas.
2) Generar internamente la información que generen los clientes, proveedores o alguien relacionado que cumplan la normativa de la seguridad de la empresa Invimedic.
3) La adquisición de los activos que gestione la información en los dispositivos móviles, software, proveedores, nuevas tecnologías de comunicación; que pueden suponer la visión de nuevas amenazas y/o vulnerabilidades hacia la empresa Invimedic.
4) Los proveedores o contratistas deben de cumplir con la seguridad de la información que posea la empresa, incluyen los cambios que genere la empresa o sus operaciones que estimen un cambio en la gestión de la información.
5) Verificar las necesidades o los requisitos de las partes interesadas que son la exigencia de contratos o cláusulas de confidencialidad, aparición de leyes o reglamentos, ampliación a nuevos mercados, nuevas amenazas de ciberseguridad para la empresa Invimedic.

El documento del anexo A de las ISO 27001 parte del 6.1 más amplio centrado en acciones para plantearlos riesgos y las oportunidades que se

presenten; de tal forma, este documento se debe entregar al auditor externo del SGSI se someta a las evaluaciones de la auditoría independiente, evidencia los debidos procesos de auditoría y la regulación de la seguridad de la información; la declaración de aplicabilidad tiene 14 dominios se denominan categorías que gestionan los controles de seguridad acorde a su necesidad y su función; en mención son la gestión de activos, la criptografía y la gestión de los incidentes de seguridad de la información que contenga la empresa Invimedic.

CONTROL	NOMBRE DEL CONTROL	DESCRIPCIÓN DEL CONTORL	APLICABLE	JUSTIFICACIÓN APLICABILIDAD / EXCLUSIÓN
5. 1	Política de seguridad de la información	Las políticas de seguridad de la información y las políticas específicas deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocido por el personal pertinente y las partes interesadas y revisadas por intervalos planificados que producen cambios significativos.	SI	Información documentada requerida
7. 10	Medios de almacenamiento	Los medios de almacenamiento se gestionarán a lo largo de su ciclo de vida de adquisición uso, transporte y eliminación de acuerdo con las normas de la empresa, esquema de clasificación y de manipulación	NO	No se manejan medios de almacenamiento

Tabla 12. Anexo A - Statement of Applicability – Los controles

		Objetivo de control / Control seleccionado	Razón de la selección	Objetivo de control / Control implementado	Justificación de exclusión	Referencia
Dominio	A. 12. Seguridad de las operaciones					
Objetivo de control	A. 12. 2. Protección contra Malware	SI	Resultado de la evaluación de riesgo	SI		
Control	A. 12. 2. 1. Controles contra Malware	SI	Resultado de la evaluación de riesgo	SI		DOC 010. Procedimiento para la instalación y configuración antivirus

Tabla 13. Anexo A Statement of Applicability - Los Dominios

Estos dominios o categorías se derivan en objetivos y controles que suman un total de 114 controles que definen la aplicabilidad a la empresa Invimedic con sus respectivas extensiones a implementar. Estas 14 categorías ISO 27001 en el anexo A son:

1) Las políticas de seguridad de la información.

2) Organización de la seguridad de la información.
3) Seguridad del talento humano.
4) Gestión de activos.
5) Control de acceso.
6) Criptografía.
7) Seguridad física y ambiental.
8) Seguridad operativa.
9) Seguridad de las comunicaciones.
10) Adquisición desarrollo y mantenimiento de sistemas.
11) Relaciones con proveedores.
12) Gestión de incidentes de seguridad de la información.
13) Aspectos de seguridad de la información de la gestión de la continuidad de la empresa Invimedic.
14) Conformidad.

Cabe mencionar que la declaración de aplicabilidad tiene ventajas en función de aplicabilidad para la empresa Invimedic; el principal beneficio de una declaración de aplicabilidad es proporcionar un extracto conciso en el proceso de gestión de riesgos; es más fácil de comprender el informe que se realizó la evaluación de riesgos puede ser extenso por lo que se dificulta la gestión en el uso operativo diario en la empresa Invimedic.

Permite revisar las políticas, procedimientos y otros documentos de los sistemas de seguridad de la información aplicada en el tratamiento de los riesgos identificados por los controles de seguridad.

La declaración de aplicabilidad es una guía de una hoja tipo ruta para el sistema de gestión de seguridad de la información que mantiene el enfoque y que cumple los requisitos de las normas ISO 27001 para su implementación y el SGSI en la empresa Invimedic.

En el proceso de la creación, desarrollo y análisis de la declaración de aplicabilidad que sea fácil su gestión debe guiarse por lo consiguiente:

1) **Identifica las brechas y las ideas en dirección correcta de llegar:**

La declaración de aplicabilidad trata de enlistar de diferentes controles o aspectos que considere la empresa con la finalidad de asegurar la información propia de los clientes o las partes interesadas en la gestión de la información; si se aplica los 114 aspectos se sabe qué hace falta para implementar y reforzar priorizar en fortalecer la seguridad de la información; que minimice los riesgos que se asocien y representen costos altos para la empresa Invimedic.

De manera similar, la declaración de aplicabilidad, conocida como "Statement of Applicability" en inglés, emplea controles que posibilitan la identificación de riesgos de seguridad. Esto es crucial para prevenir situaciones en las que el responsable de seguridad podría no haber detectado un acceso no autorizado a la información u otro incidente de pérdida de datos en la gestión de la seguridad de la información.

2) **Seleccionar la seguridad de la información en forma colectiva:**

La implementación del Statement of Applicability podría extenderse a lo largo de varios años, ya que implica la definición técnica y la aplicación de diversos recursos como talento humano, criptografía, vulnerabilidades técnicas, entre otros aspectos. No obstante, la empresa cuenta con diversas áreas que podrían acelerar este proceso, generando así un considerable valor tanto para los activos de Invimedic como para las partes interesadas en la empresa.

3) **Aplicar en forma incremental paso a paso:**

Para iniciar la realización se deben considerar los 114 controles y analizar que tiene la empresa en la actualidad para la implementación en forma parcial y estar pendiente que cumpla los lineamientos y así también los que no aplicará en el sistema de gestión; una vez identificada las brechas en la ejecución debe de iniciar en analizar cada uno de los controles de seguridad y priorizar a todos los controles ya evaluados, verificar la información en cada proceso si es simple en implementar en costo beneficio para la empresa Invimedic; de tal forma esperar los resultados de los controles evaluados para una buena toma de decisión; al seleccionar los controles se inicia la realización y presentar en un listado todas las actividades que la empresa debe de conllevar para su aplicabilidad e incluir los recursos que tiene la empresa no afecte el costo para la aplicación de cada uno de los controles en la empresa Invimedic.

4) **Declaración o evidencias del trabajo en el momento:**

Los resultados en la aplicabilidad de los controles de seguridad permiten ayudar a la empresa Invimedic; en mantener su información y sus activos de mayor valor bajo la supervisión de las salvaguardas, que genera un informe en un software utilitario Excel para descargar el informe detallado de todas las actividades y gestiones en la seguridad de la información de la empresa Invimedic.

- **FASE 7: Revisión del sistema**

En la revisión del sistema debe de incluir las evaluaciones realizadas a los controles de seguridad en un tiempo anual para obtener una eficaz en la aplicación y seguridad de la información con las normas ISO 27001.

La implementación de un sistema de gestión de seguridad de la información SGSI, es generar una adaptación para la revisión del sistema que la empresa

debe de incluir la evaluación de oportunidades en la mejora en base a la necesidad de realizar variaciones en el sistema del SGSI; también debe de incluir la revisión de política con la seguridad de la información de los objetivos que deba cumplir la seguridad de la información en el marco empresarial de la empresa Invimedic.

Se puede mencionar que la empresa Invimedic tiene el deber de mejorar en forma continua con la eficacia y el alcance del sistema de gestión de seguridad de la información (SGSI); al usar la política de seguridad de la información, los objetivos de la seguridad, los resultados obtenidos tras la auditoria por medio de los análisis con el tratamiento del estado del SGSI con el monitoreo y por las medidas correctivas o preventivas en la gestión de revisión.

Dentro de la implementación del sistema de gestión de seguridad de la información se debe de tomar decisiones y acciones necesarias que elimine todo riesgo o causas de algún daño en el sistema de la información; para prevenir que los posibles riesgos aparezcan en mantener y usar continua las acciones correctivas y preventivas en el sistema de gestión de seguridad de la información (SGSI), las ISO/I3C 27001 en la empresa Invimedic.

En la revisión del sistema es importante priorizar la acción preventiva que determina los resultados obtenido acuerdo al valor del riesgo; estas acciones se usan en forma adecuada en el momento del impacto que genere algún incidente o problemas en el sistema del SGSI y las ISO 27001 implementado por la empresa Invimedic.

En esta acción o medida se ejecuta un plan de mejora de una herramienta que se usará durante una continua mejora; es un documento con la finalidad de recopilar todas las acciones que están implicadas en el marco de mejora para el sistema de gestión de seguridad de la información SGSI y de los procesos que se encuentran los sistemas de seguridad de la información en la empresa Invimedic.

En este procedimiento se realiza el respectivo análisis de los datos para cada proceso que realiza la empresa que se definen en cada uno de los indicadores de análisis; que la empresa Invimedic debe de realizar el correspondiente seguimiento en cada cierto tiempo.

Este plan de mejora se constituye en las siguientes acciones que se detallan:

1) La fecha de apertura de la acción preventiva y correctiva.
2) Número de acción de mejora (se usa un número correlativo).
3) El origen de la acción (sugerencia, revisión de sistemas).
4) Llevar a cabo una planificación y seguimiento en el tiempo.
5) Descripción de la acción de mejora.
6) Planificación de la acción de mejora.
7) Detallar todas las acciones (pequeñas y detalladas).
8) Asignar plazos de ejecución y sus responsables.
9) El seguimiento se debe de realizar trimestralmente.
10) Realizar el seguimiento antes de la fecha prevista.
11) Personal encargado de determinar cada aspecto de la seguridad.

Estas acciones deben de ser aprobadas por la administración de la empresa Invimedic, este plan de mejor es anual que se lo desarrolla a manera que complete según las necesidades de la planificación si requiere alguna mejora; se ejecuta en el momento de realización de reuniones del comité de seguridad, si en la reunión existen inasistencias de ciertos miembros del comité sin excepción es importante que el jefe del comité de seguridad esté y ejecutará lo siguiente:

1) Las acciones de mejora propuestas por cualquier persona que asista a la reunión.
2) Asistentes de los responsables de todos los procesos que se realizan en la empresa Invimedic.
3) Sugerir propuestas por el personal de la empresa Invimedic.

4) Las acciones preventivas y correctivas que requieran una planificación y seguimiento en el tiempo previsto.

El personal que son responsables de diferentes procesos tiene la facilidad de detectar puntos frágiles que necesitan las mejoras pertinentes, documentarlas y presentarlas ante el jefe del comité de seguridad, después se presentará ante todo el comité en la próxima reunión, para debatir su aprobación o no; el jefe del comité de seguridad está en la obligación de realizar un mayor esfuerzo en una acción de mejora para toda la empresa Invimedic. El seguimiento de estas acciones preventivas y correctivas se basa a los acuerdos de los plazos establecidos por el jefe del comité de seguridad de la empresa Invimedic.

- **FASES: Auditoría Interna**

En esta fase o elemento, de la implementación del SGSI en la empresa Invimedic se relaciona con las normas ISO 27001; éstas normas internacional de seguridad están en la obligación de llevar auditorias planificadas en un intervalo de tiempo para presentar la debida información, en referencia del sistema de gestión de seguridad de la información; con el fin de observar que cumpla con los requisitos establecidos por la empresa, relacionado con los lineamientos con las normas internacional ISO 27001, que permita evidenciar que el sistema implementado por la empresa Invimedic.

La fase de la auditoría interna contempla la frecuencia de las fechas en ejecución, el alcance del mismo sistema SGSI, la metodología de la auditoría, la asignación de interlocutores para la realización de la planificación de la auditoría del sistema, la ejecución y la presentación de los informes de resultados; este plan de mejoría en la auditoría está comprendido y descrito por ubicaciones físicas, organización personal, actividades y procesos con fechas de inicio y fin ejecutada y planificada por la empresa Invimedic.

La auditoría interna del sistema es ejecutada por el personal apto y calificado en revisar el tratamiento de la implementación del SGSI, que asegura la objetividad y ser imparcial en el momento de la auditoria y la independencia de los auditores internos. La auditoría se realiza en forma anual y se entrega una certificación del seguimiento de los sistemas de seguridad aplicados; la implementación de la auditoría de las fases en el marco de las ISO 27001 se ejecuta para evaluar con eficacia la seguridad de los controles y permitir detectar las intrusiones de la seguridad de la empresa Invimedic.

Dentro del marco de la auditoria tiene un alcance que comprende un checklist completo al sistema de gestión, en base de las ISO/IEC 27001; la selección de los controles de seguridad de la implementación en la empresa Invimedic, en esta selección se necesitan los controles de seguridad acuerdo entre el auditor jefe y el responsable del SGSI, en referencia con la información de la declaración de aplicabilidad (Statement of applicability); asegurar lo auditado a todos los controles y los procesos de los objetivos de control y referencia (anexo A) de la norma ISO 27001 en un periodo de tres años implementado en la empresa Invimedic.

La auditoría en el momento de la aplicación o ejecución el auditor debe de realizar un informe previo y presentarlo al personal encargado de las áreas auditadas; al evaluar en forma interna entregar un documento para analizar luego ejecutar la auditoría y después analizar dicha documentación entregada a los auditores; la auditoría interna del SGSI consta de dos partes:

- ✓ **Sistema de Gestión.**

  Consta de la revisión de la documentación dentro del marco del sistema de gestión de seguridad de la información SGSI, se analiza el contexto del sistema, el alcance que tiene el SGSI, el análisis de la gestión de riesgo, la declaración de aplicabilidad (SOA), la política de seguridad, los roles de seguridad de la información y los controles de

seguridad entre otros factores y elementos o recursos que posea la empresa que es auditada en forma de gestión administrativa y operatividad de los procesos que realice la empresa Invimedic.

- ✓ **Pruebas de cumplimiento.**

  Esta fase de la auditoria y supervisión se valida la comprobación del alto grado de eficacia en la implementación de los controles de seguridad y definir los adecuados protocolos de seguridad para las intrusiones que genere el flujo de los activos de la empresa; entrevistas con la alta gerencia de la empresa, los usuarios que asisten a la empresa que se relacionen con el sistema de gestión de seguridad de la información, se analiza las áreas de riesgo y se verifica los objetivos con sus metas establecidas por la empresa Invimedic.

Después de la auditoría se generan las evidencias necesarias para verificar y validar el cumplimiento de los distintos apartados y los controles de las normas ISO27001, la implementación del sistema de gestión de seguridad de la información SGSI; el auditor elabora para presentar los debidos informes acorde a los resultados obtenidos para dar el conocimiento a la alta gerencia administrativa de la empresa, a las áreas auditadas, el comité de seguridad acorde a los procesos y al tratamiento del sistema SGSI a nivel empresarial en la empresa Invimedic.

El comité de seguridad del SGSI son los encargados de informar los resultados obtenidos y entregar al personal de mantenimiento del sistema que derivan a la realización de las auditorías internas dentro de la empresa Invimedic. Este informe del auditor debe de considerar lo siguiente:

1) Áreas y alcance auditado con la fecha de la auditoría.
2) Observaciones encontradas, acordadas con los auditados.

3) Valorar los puntos fuertes y áreas frágil y susceptible a la mejora del SGSI.
4) Acciones correctivas propuestas por el auditor.
5) Proponer las salvaguardas en los riesgos identificados.
6) Garantizar el cumplimiento de las normas ISO 27001 para la implementación del SGSI.
7) Recomendar las acciones correctivas de una salvaguarda.
8) Mejorar las acciones que pueden suponer evolución o madurez del SGSI auditado.
9) Documentar lo auditado.
10) Firma del auditor / auditores.

También cabe mencionar que la figura 13 hace referencia a siete fases que están clasificadas por cada requerimiento con su importancia a aplicar acorde a los elementos o factores ya estudiados en la sección 4.1 situación inicial de este documento; se puede mencionar que en cada fase tiene su propio indicador de requisitos que se describe de esta manera:

- ✓ La fase uno deriva del factor político y sus resoluciones a favor de la empresa Invimedic; en otras palabras, que:

    1) Los proveedores deben estar calificados y contar con las certificaciones correspondientes otorgadas por el ministerio de salud.
    2) También deben de tener convenios internacionales.
    3) Así mismo con la cartera de las empresas que proveen los insumos en el marco internacional acorde a las normativas internacionales.

Cabe mencionar que las fases o elementos para implementar el sistema de gestión de seguridad de la información SGSI en base de las normas ISO 27001 para la empresa Invimedic; son los lineamientos o requisitos para poder implementar un sistema del SGSI que le permita a la empresa conocer que recursos puede tener en consideración para el uso de este sistema en la gestión de seguridad de sus activos

y todos sus proceso en el tratamiento de la información de la empresa; que debe de ofrecer seguridad, confianza a los clientes, administración y proveedores.

La empresa Invimedic debe estar en constante mejora continua en verificar todo el debido desarrollo y la gestión de los controles de seguridad de los activos o información implementados basado en las normas ISO 27001; La empresa diseña un mapa de una de las fases de implementación para la empresa Invimedic que se visualiza los elementos o factores relevantes en ese factor; que les representan un valor considerable para el posicionamiento en un país que debe de regirse con las normas o leyes que imponga el estado o país a nivel empresarial, ver la descripción de la definición de la política en beneficio para la empresa Invimedic. Véase en la siguiente figura 14.

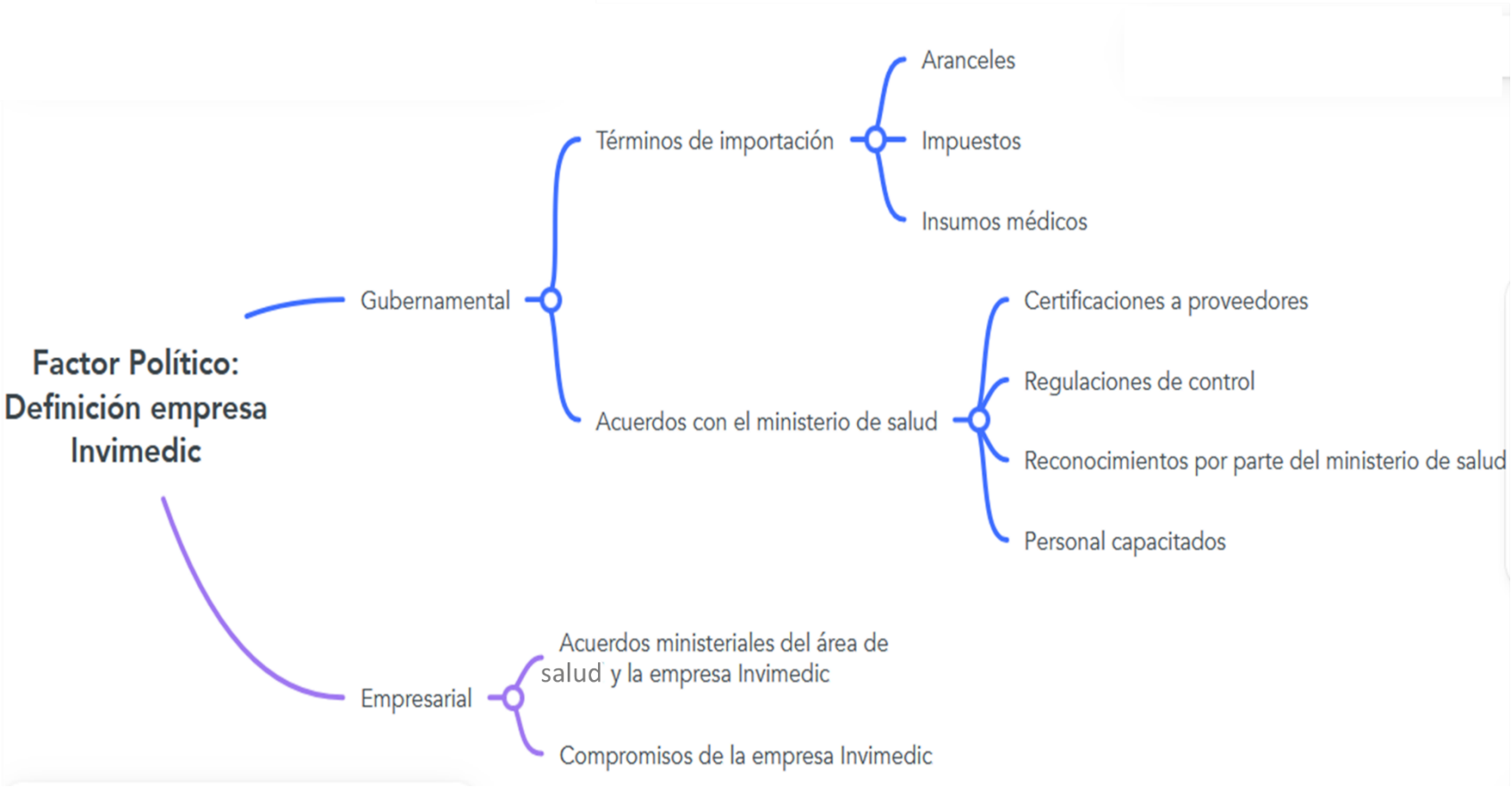

Figura 14. Descripción de la definición de la política

✓ La fase dos se deriva del alcance del SGSI puede describir la viabilidad en aplicar, se puntualiza:

1) Los límites para la protección de la información y otros activos.
2) Es importante la implementación en las medidas de seguridad que posea la empresa Invimedic.
3) Permitir definir el control de los flujos de los activos entre las áreas asignadas en la gestión de seguridad de la empresa Invimedic.

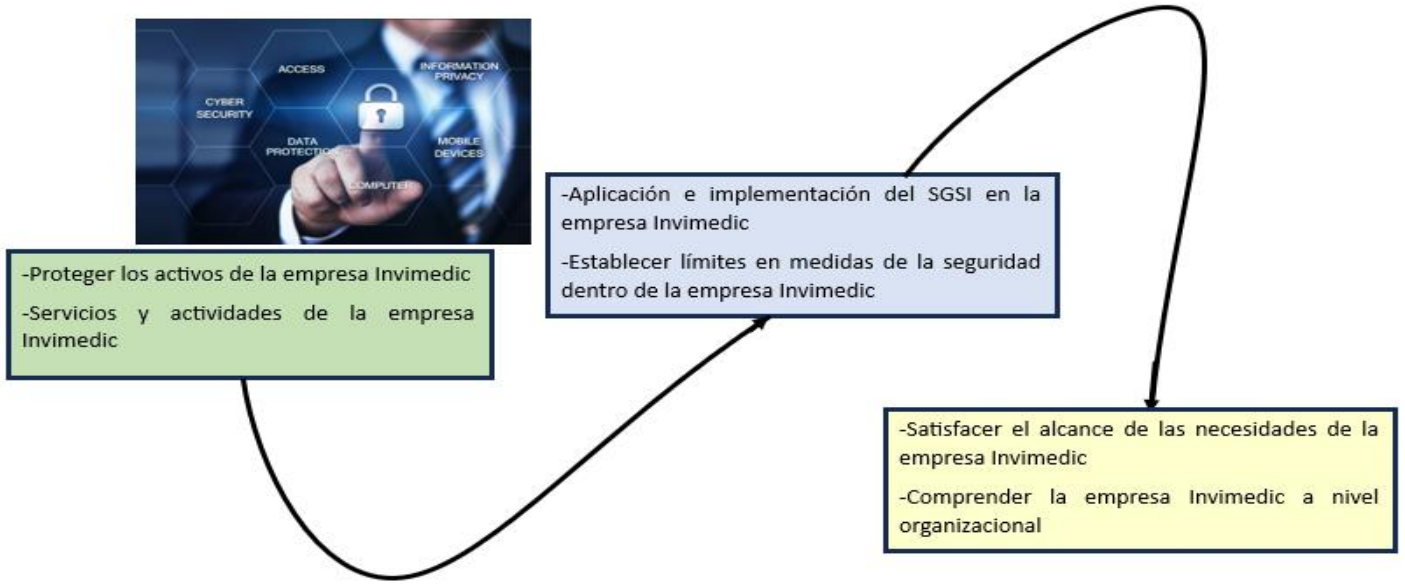

Figura 15. Alcance de un SGSI - empresa Invimedic

- ✓ La fase tres se enfoca en los análisis de riesgo que consiste en la práctica de identificar, seleccionar y analizar las amenazas que establece el uso de las salvaguardas para evitar cualquier tipo de riesgo en el marco empresarial que puedan afectar a la empresa Invimedic.

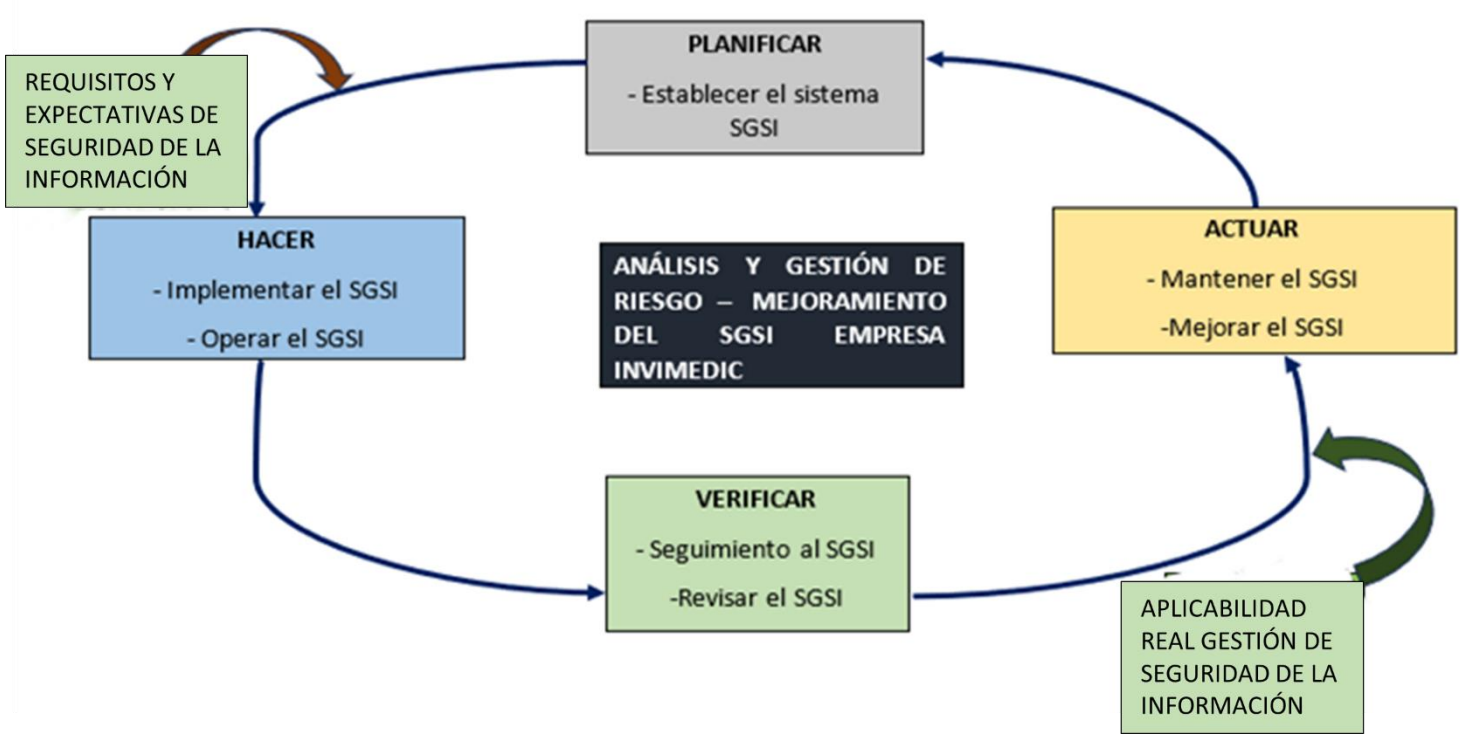

Figura 16. Análisis de riesgo - empresa Invimedic

La implementación de un SGSI para los sistemas en gestión de control y seguridad es la decisión de la alta gerencia de la empresa Invimedic para cumplir el objetivo de garantizar los tres pilares fundamentales en seguridad que son la confidencialidad, integridad, disponibilidad; estos sistemas son apoyados en un constante proceso en gestión de seguridad y salvaguardar la información con el resto de los procesos que generen en el tratamiento de los activos de la empresa Invimedic.

La planificación y creación de una política en la empresa Invimedic se apoya en el sistema SGSI su implementación es supervisar, revisar, mantener y mejorar la protección de los activos de la información que gestiona la empresa Invimedic; los requisitos en base de la política de seguridad de la información de la empresa representa los lineamientos, las estrategias en los logros de los objetivos que permita la evaluación ininterrumpido en los factores de riesgo; es tener una gestión eficaz de los mismos que incluye el liderazgo, estructura empresarial, las políticas, la planificación, responsabilidades y procedimientos para una aplicación exitosa del sistema SGSI para la empresa Invimedic.

En el marco de la implementación del SGSI que tiene la empresa Invimedic en su contexto legal, político, geográfico y los requisitos de la seguridad en el contexto del cumplimiento legislativo y normativo en base a las necesidades de la empresa y las partes interesadas que son los empleados, clientes, proveedores, inversionistas; así mismo, es fundamental el liderazgo, supervisión y el soporte de la dirección de sistema y telecomunicación que garantice el buen funcionamiento del sistema y detecta las oportunidades para la mejora del sistema del SGSI en beneficio de la empresa Invimedic.

La empresa Invimedic para prestar sus servicios a la salud debe de tener la respectiva documentación que cumpla con los requisitos y regulaciones reguladas en relación de la gestión de la información del personal de la salud y también de sus clientes; también con su respectiva privacidad de sus datos a nivel competitivo empresarial. Es importante el compromiso de la gerencia empresa Invimedic que tiene un rol fundamental, garantizar la implementación de un SGSI; las actividades en la gestión de los resultados obtenidos son adecuados para estar disponibles trabajar, capacitar

a todo el personal relacionados para la estructuración del SGSI, que organiza programas de monitoreo y los controles de seguridad para el sistema de gestión de seguridad de la información SGSI implementada en la empresa Invimedic.

- ✓ La fase cuatro tiene el enfoque de la gestión de riesgo en el contexto organizacional y el grado de aseguramiento requerido gestionar un sistema SGSI; permite evaluar los riesgos y definir las aplicaciones de control de seguridad, las medidas necesarias con el uso de las salvaguardas para eliminar o minimizar para evitar posibles consecuencias que pueda afectar a la empresa Invimedic.

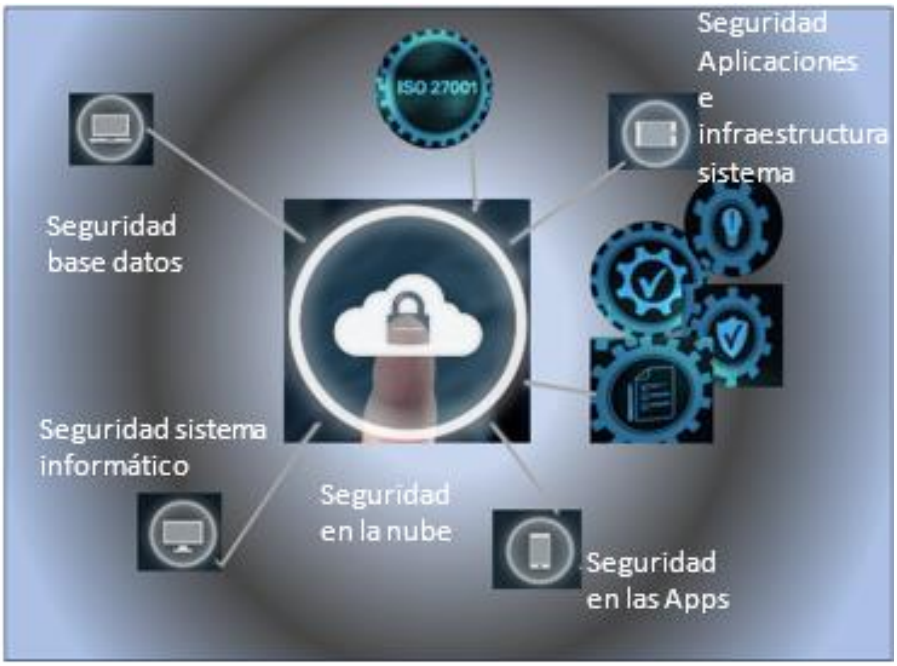

Figura 17. Gestión del riesgo - esquema de seguridad

- ✓ La fase cinco en los lineamientos del marco SGSI es la selección de controles a implementar con un alto grado aseguramiento requerido, los controles adicionales en establecer las políticas de seguridad referente a los activos de la empresa Invimedic; talento humano; actualizar los recursos y las herramientas electrónicas de seguridad.

- ✓ La fase seis es el enfoque de los controles adicionales y la declaración aplicabilidad de la implementación del SGSI, permite identificar los controles de la empresa Invimedic para afrontar los riesgos que son identificados; confidencialidad, integridad de la información para la operatividad de la empresa Invimedic.
- ✓ La Fase siete son las medidas preventivas correctivas y mejoras para la revisión del sistema se rigen a comprobar la aprobación de los requisitos del SGSI y con el cumplimiento de la empresa Invimedic; implementar las normas de forma correcta y eficaz; la alta dirección de la empresa Invimedic debe de revisar y garantizar la seguridad de los activos de la empresa en base de los lineamientos de las ISO 27001 por un determinado tiempo dos veces al año; un SGSI debe de cumplir los ajustes, la eficacia, la revisión constante e incluir un test de oportunidades de las necesidades para las mejoras del SGSI a cumplir con los objetivos del sistema de gestión de seguridad de la información.

4.3 Evaluación de efectividad

Es importante establecer que información se requiere evaluar para cuantificar el rendimiento del sistema de gestión de seguridad de la información SGSI; determina que debemos medir y controlar en la gestión de los controles de seguridad que la empresa tiene la capacidad, supervisar con los requisitos al valorar en beneficio de la seguridad de la información y la eficaz de un sistema de gestión de seguridad de la información SGSI al tener una evaluación de efectividad para la empresa Invimedic.

La evaluación efectiva del sistema de gestión de seguridad de la información SGSI implementada en la empresa Invimedic tienen las distintas necesidades de evaluar los activos; es importante controlar la participación de los eventos de sensibilizar con respecto a la seguridad de la información, la empresa observa la calidad del evento, es por los objetivos específicos establecidos basado en la norma ISO 27001; permite gestionar los activos de la información con los lineamientos requeridos por los estándares internacionales.

En el desarrollo de este proyecto investigativo dentro del marco de los objetivos específicos se propuso una evaluación del sistema de gestión de seguridad de la información SGSI basados en las normas ISO 27001: 2013 implementada en la empresa Invimedic; considerar de manera estricta el cumplimiento del factor ético por los autores de dicho documento que permita asegurar el origen de la investigación; respetar los derechos de propiedad de los artículos, libros de texto y de las fuentes electrónicas consultadas que son necesarias para estructurar la debida documentación.

Para el desarrollo de este proyecto de implementación de las normas ISO 27001 basados en el sistema de gestión de seguridad de la información SGSI, se determina la encuesta a 50 personas del personal encargado de las áreas de seguridad y de soporte de sistemas de la empresa Invimedic se empleó las siguientes preguntas:

DIMENSIÓN 01: EVALUACIÓN DE EFECTIVIDAD DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA INVIMEDIC.			
NRO.	**PREGUNTA**	**SI**	**NO**
1	**¿**Considera usted que las políticas de la seguridad de la información están documentadas y respaldadas**?**	**52%**	**48%**
2	**¿**Existen lineamientos establecidos por el control de seguridad para los activos de la empresa Invimedic**?**	**64%**	**36%**
3	**¿**Existen procesos documentados, que respaldan a las salvaguardas en los equipos de TI, ante problemas medioambientales**?**	**54%**	**46%**
4	**¿**Existen procesos documentados que cumplan los lineamientos de los responsables de los equipos de TI**?**	**52%**	**48%**
5	**¿**Existen procesos documentados para evaluar la gestión y operaciones en las comunicaciones de la empresa Invimedic**?**	**54%**	**46%**
6	**¿**Existen procesos de seguridad física y ambiental para salvaguardar la información**?**	**64%**	**36%**
7	**¿**Existen procesos con las debidas medidas de seguridad para los equipos y del Software**?**	**54%**	**46%**
8	**¿**Los procesos operativos de los sistemas de la información están seguros por las medidas de seguridad implementada en la empresa Invimedic**?**	**64%**	**36%**
9	**¿**Existen protocolos para el mantenimiento de los sistemas de comunicación**?**	**58%**	**42%**
10	**¿**Existen lineamientos que permitan evaluar a las políticas de seguridad de la información**?**	**50%**	**50%**
11	**¿**Existen lineamientos para evaluar los roles y las funciones del personal del SGSI**?**	**60%**	**40%**
12	**¿**Existen procesos de evaluación para la gestión de los controles de accesos que se gestionan dentro de la empresa**?**	**48%**	**52%**

¿Considera usted que las políticas de la seguridad de la información están documentadas y respaldadas?

Figura 18. Políticas de la seguridad de la información

De la pregunta 1 propuesta en la encuesta el 52 % representa el si la información de los documentos y son respaldadas por el SGSI basadas en las normas ISO/IEC 27001 de la empresa Invimedic; y el 48 % representa el no que consideran que las políticas de la seguridad de la información no se encuentran documentados ni están respaldadas por la empresa Invimedic.

¿Existen lineamientos establecidos por el control de seguridad para los activos de la empresa Invimedic?

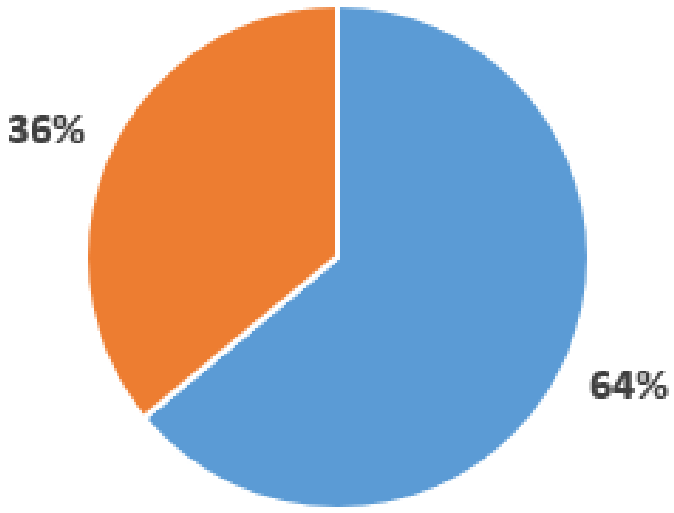

Figura 19. Lineamientos establecidos por el control de seguridad

De la pregunta 2 propuesta en la encuesta el 64 % representa si la empresa cuenta con los lineamientos establecidos en el control de seguridad de los activos de las normas ISO 27001 aplicados por la empresa Invimedic; y el 36 % representa no tienen establecidos los lineamientos establecidos dentro de las normas ISO 27001 por la empresa Invimedic.

¿Existen procesos documentados, que respaldan a las salvaguardas en los equipos de TI, ante problemas medioambientales?

Figura 20. Procesos documentados que respaldan las salvaguardas

De la pregunta 3 propuesta en la encuesta el 54 % representa si la empresa cuenta con las debidas medidas de seguridad que respaldan a todos los procesos de los equipos TI y de los activos de las normas ISO 27001 aplicados por la empresa Invimedic; y el 46 % representa no cuenta con las debidas medidas establecidas que puedan respaldar en los procesos de los equipos TI en las normas ISO 27001 por la empresa Invimedic.

¿Existen procesos documentados que cumplan los lineamientos de los responsables de los equipos de TI?

Figura 21. Procesos documentados del personal responsable de los equipos TI

De la pregunta 4 propuesta en la encuesta el 52 % representa si la empresa cuenta con las debidas medidas de seguridad que respaldan al personal y todos los procesos de los equipos TI y de los activos de las normas ISO 27001 aplicados por la empresa Invimedic; y el 48 % representa no cuenta con el personal con la debida capacitación que puedan respaldar los equipos TI en las normas ISO 27001 de la empresa Invimedic.

¿Existen procesos documentados para evaluar la gestión y operaciones en las comunicaciones de la empresa Invimedic?

Figura 22. Procesos documentados para evaluar la gestión y las operaciones

De la pregunta 5 propuesta en la encuesta el 54 % representa si existen procesos con la respectiva evaluación de la gestión y operaciones en las comunicaciones que existen en los equipos de TI de las normas ISO 27001 aplicados por la empresa Invimedic; y el 46 % representa no cuenta con la debida evaluación de la gestión y las operaciones que puedan respaldar los equipos TI en las normas ISO 27001 de la empresa Invimedic.

¿Existen procesos de seguridad física y ambiental para salvaguardar la información?

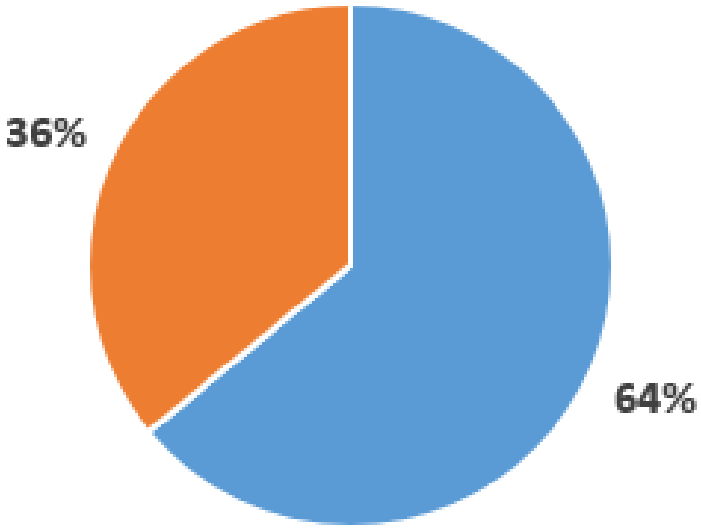

Figura 23. Procesos de seguridad física y ambiental de la información

De la pregunta 6 propuesta en la encuesta el 64 % representa si existen procesos con la respectiva seguridad física y ambiental para respaldar la debida información que gestione la empresa Invimedic en base a las normas ISO 27001; y el 36 % representa no cuenta con la debida respectiva seguridad física y ambiental que puedan respaldar la información gestionadas en las normas ISO 27001 de la empresa Invimedic.

¿Existen procesos con las debidas medidas de seguridad para los equipos y del Software?

Figura 24. Procesos con las debidas medidas de seguridad para los equipos y los sistemas

De la pregunta 7 propuesta en la encuesta el 54 % representa si existen procesos con la respectiva medida de seguridad para los equipos y los sistemas que existen en los equipos de TI de las normas ISO 27001 aplicados por la empresa Invimedic; y el 46 % representa no existen la debida medida de seguridad para los equipos y los sistemas de información en los equipos TI en las normas ISO 27001 de la empresa Invimedic.

¿Los procesos operativos de los sistemas de la información están seguros por las medidas de seguridad implementada en la empresa Invimedic?

Figura 25. Procesos de los sistemas de la información están seguras en la empresa Invimedic

De la pregunta 8 propuesta en la encuesta el 64 % representa si existen los procesos en los sistemas de la información en los equipos de TI se encuentran seguros ISO 27001 aplicados por la empresa Invimedic; y el 36 % representa no existen la debida seguridad en los procesos de sistemas de la información en los equipos TI en las normas ISO 27001 de la empresa Invimedic.

¿Existen protocolos para el mantenimiento de los sistemas de comunicación?

Figura 26. Los protocolos para el mantenimiento de sistemas de comunicación

De la pregunta 9 propuesta en la encuesta el 58 % representa si existen los protocolos pares el debido mantenimiento en los sistemas de la información en los equipos de TI se encuentran seguros ISO 27001 aplicados por la empresa Invimedic; y el 42 % representa no existen los debidos protocolos de seguridad en los procesos de sistemas de la información en los equipos TI en las normas ISO 27001 de la empresa Invimedic.

¿Existen lineamientos que permitan evaluar a las políticas de seguridad de la información?

Figura 27. Lineamientos para evaluar las políticas de seguridad de la información

De la pregunta 10 propuesta en la encuesta el 50 % representa si existen los debidos lineamientos que evalúen las políticas de seguridad de la información en los equipos de TI se encuentran seguros ISO 27001 aplicados por la empresa Invimedic; y el 50 % representa no existen los debidos lineamientos de seguridad en la política de seguridad de la información en los equipos TI en las normas ISO 27001 de la empresa Invimedic.

¿Existen lineamientos para evaluar los roles y las funciones del personal del SGSI?

Figura 28. Lineamientos para evaluar los roles y funciones del personal

De la pregunta 11 propuesta en la encuesta el 60 % representa si existen los lineamientos evaluativos a los roles y funciones del personal encargado del SGSI en los controles de seguridad ISO 27001 aplicados por la empresa Invimedic; y el 40 % representa no existen los debidos lineamientos evaluativos al personal de los roles y funciones del personal encargado del SGSI e ISO 27001 de la empresa Invimedic.

¿Existen procesos de evaluación para la gestión de los controles de accesos que se gestionan dentro de la empresa?

Figura 29. Procesos de evaluación para la gestión de controles de accesos

De la pregunta 12 propuesta en la encuesta el 48 % representa si existen los respectivos procesos evaluativos para la gestión de los controles de accesos en el SGSI en los controles de seguridad ISO 27001 aplicados por la empresa Invimedic; y el 52 % representa no existen los debidos procesos evaluativos para la gestión del SGSI e ISO 27001 de la empresa Invimedic.

Discusión

Al llevar a cabo el desarrollo de esta investigación, es proponer la implementación de un SGSI e ISO 27001:2013 y diseñar la aplicación para su utilización para cumplir los requerimientos de las normas ISO 27001; que son la clave para obtener excelentes resultados, dentro del marco de desarrollo para crear un sistema de seguridad para el resguardo de la información de la empresa Invimedic; estos resultados beneficia a la empresa por su transparencia en la gestión de la información y administrar los controles de seguridad de los sistemas informáticos y de los activos.

La tecnología de la información en la actualidad, la confidencialidad, integridad y disponibilidad son factores importantes y es prioritario en el punto de vista de la seguridad; las tecnologías de la seguridad de la información son usadas en la arquitectura tienen buenas características contra los ciberataques que amenazan a las infraestructuras de la empresa Invimedic; esto incluye a la exposición de los datos de los pacientes, personal médico y administrativo, en el momento de la entrega de los mismos que amenazan los bienes o los activos de la empresa Invimedic.

Los requisitos esenciales para la aplicación de la implementación de un sistema de gestión de seguridad de la información e ISO 27001 permiten a la administración de todos los procesos que gestione la empresa, las técnicas, la metodología en el uso de las ISO 27001 para el acceso íntegro del manejo de la información en base de las fases del sistema de gestión de seguridad de la información que determinan todos los lineamientos y requerimientos que deban de cumplir el diseño de un sistema de gestión de la seguridad de la información SGSI bajo los requisitos de las normas ISO/IEC 27001:2013, y por cada fase los SGSI cumplen una determinada función que ejerza la empresa Invimedic por la gestión de la información y todos los procesos con los datos que emplea en el centro médico de especialidades.

El objetivo de esta propuesta es demostrar que las normas ISO 27001 implementada para la seguridad de la información y presentar un diseño que puede ser mejorado por otros investigadores.

Esta investigación tiene por objetivo el tratamiento de la información digital y las salvaguardas para las mismas; en un futuro se tiene la intención de expandir y extender estas normas para incluir la seguridad de la información basadas en las normas ISO 27001 y el sistema de gestión de seguridad de la información SGSI, adicional es explorar las posibilidades de implementar el uso de la inteligencia artificial IA para los puntos de acceso o viabilidad a la información que se procese en la empresa Invimedic.

5 CONCLUSIONES

La presente documentación tuvo el objetivo general, implementar el sistema de gestión de seguridad de la información en la empresa Invimedic, por las normas internacionales estándar de seguridad de la información SGSI con las ISO 27001: 2013; realizar una evaluación general en la empresa Invimedic para que respalde los activos de la empresa.

Así mismo, se presentan las conclusiones obtenidas en base del desarrollo de la investigación, ver en las siguientes:

1. Se observa que lo descrito en la presente tesis permite realizar un estudio minucioso en relación con la situación inicial presento la empresa Invimedic; mejorar la gestión de los activos y minimizar las posibilidades de riesgo.
2. Al diseñar e implementar el sistema de gestión de seguridad de la información SGSI bajo los lineamientos de las ISO/IEC 27001:2013 para el respaldo de los activos de la empresa Invimedic.
3. Para realizar una evaluación efectiva del SGSI implementada en la empresa Invimedic se realizó un banco de preguntas de una encuesta que evidencia dicha evaluación aplicada al SGSI e ISO 27001:2013.

Referencias

ALDER, A., & WATKINS, S. G. (2019). THE ISO 27001 RISK ASSESSMENT. In *Information Security Risk Management for ISO 27001/ISO 27002, third edition* (pp. 87–93). IT Governance Publishing. https://doi.org/10.2307/j.ctvndv9kx.11

Chaiwut, N., & Rueangsirarak, W. (2022). An Online Gap Analysis on Cyber Security Principles for Thailand Organizations Based on ISO/IEC 27001:2013 Standard. *6th International Conference on Information Technology, InCIT 2022*, 479–484. https://doi.org/10.1109/InCIT56086.2022.10067572

Consultores McKinsey. (n.d.). *Esquema 7S (Siete eses)*.

Guo, H., Wei, M., Huang, P., & Chekole, E. G. (2021). Enhance Enterprise Security through Implementing ISO/IEC 27001 Standard. *2021 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2021*. https://doi.org/10.1109/SOLI54607.2021.9672401

Institute of Electrical and Electronics Engineers. (n.d.-a). *Proceeding of 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA): 4-5 November 2020, Bandung, Indonesia.*

Institute of Electrical and Electronics Engineers. (n.d.-b). *Proceeding of 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA): 4-5 November 2020, Bandung, Indonesia.*

Lopez-Leyva, J. A., Kanter-Ramirez, C. A., & Morales-Martinez, J. P. (2020a). Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001. *Proceedings - 2020 8th Edition of the International Conference in Software Engineering Research and Innovation, CONISOFT 2020*, 147–153. https://doi.org/10.1109/CONISOFT50191.2020.00030

Lopez-Leyva, J. A., Kanter-Ramirez, C. A., & Morales-Martinez, J. P. (2020b). Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001. *Proceedings - 2020 8th Edition of the International Conference in Software Engineering Research and Innovation, CONISOFT 2020*, 147–153. https://doi.org/10.1109/CONISOFT50191.2020.00030

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference on Cyber Management and Engineering, CyMaEn 2023*, 117–122. https://doi.org/10.1109/CyMaEn57228.2023.10051114

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management*, *68*(1), 87–100. https://doi.org/10.1109/TEM.2020.2977815

Monev, V. (2022). ISO 27001 Framework for Securing Election Infrastructure and Machine Voting. *2022 36th International Conference on Information Technologies, InfoTech 2022 - Proceedings*. https://doi.org/10.1109/InfoTech55606.2022.9897101

Consultores McKinsey, n.d

Putra, D. S. K., Tistiyani, S., & Sunaringtyas, S. U. (2021). The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries. *Proceeding - 2021 2nd*

International Conference on ICT for Rural Development, IC-ICTRuDev 2021. https://doi.org/10.1109/IC-ICTRuDev50538.2021.9656529

Tekhnicheski universitet--Sofiĭa,¯Institute of Electrical and Electronics Engineers. Bulgaria Section, & Institute of Electrical and Electronics Engineers. (n.d.). *2020 International Conference on Information Technologies (InfoTech-2020): proceedings of the 34th edition of the InfoTech Conference: 17th-18th September 2020, St. St. Constantine and Elena resort, Varna, Bulgaria*.

Tintin, R., & Hidalgo, M. (2023). Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data? *2023 9th International Conference on EDemocracy and EGovernment, ICEDEG 2023*. https://doi.org/10.1109/ICEDEG58167.2023.10122109

Wicaksono, A. C., Prabowo, S., & Oktaria, D. (2022). Risk and Security Measurement Based on ISO 27001 Using FMEA Methodology Case Study: National Government Agency. *2022 1st International Conference on Software Engineering and Information Technology, ICoSEIT 2022*, 6–11. https://doi.org/10.1109/ICoSEIT55604.2022.10029988