DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN AL PROCESO DE TIC EN LA ORGANIZACIÓN ORTOPÉDICA ALCA PLUS S.A.S.

FABIO OMAR RUIZ RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
2024

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN AL PROCESO DE TIC EN LA ORGANIZACIÓN ORTOPÉDICA ALCA PLUS S.A.S.

FABIO OMAR RUIZ RIVERA

Proyecto de grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

CHRISTIAN REYNALDO ANGULO RIVERA
Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
2024

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Cúcuta, 01 de noviembre de 2023

DEDICATORIA

A Dios que me bendijo con el don de la constancia y la perseverancia, además por poner en mi camino primero la ingeniería de sistemas y ahora la oportunidad de esta especialización, porque a través de ella puedo explotar las habilidades y destrezas que él me brindo.

A mi madre, por haber sido mi apoyo incondicional en mi carrera; a mi esposa, por su paciencia, dedicación y motivación para culminar este proyecto, enseñándome que, aunque la vida es dura, hay que afrontarla con madurez y que, para lograr nuestras metas, debemos esforzarnos y dedicar tiempo; y por último a mi hijo, quien es mi motor, que me impulsa todos los días a ser mejor persona cada día.

AGRADECIMIENTOS

Primeramente, agradezco a mi esposa el apoyo emocional que me ha aportado, para motivarme todos los días a que debo hacer el esfuerzo de tiempo y dinero para crecer profesionalmente, quien en muchas ocasiones me vio desanimado y me impulsó a lograr este objetivo. También agradezco al personal de la organización Ortopédica Alca Plus S.A.S, por abrirme sus puertas y permitir llevar a cabo este proyecto, contribuyendo de forma positiva en la mejora del sistema de información de la organización; y al cuerpo de docentes de la universidad, por compartir sus conocimientos y brindarnos una educación de alta calidad.

CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pag.

GLOSARIO

El glosario en los estudios de proyecto de grado, trabajo de grado, tesis doctoral, entre otros, requieren de un apartado metodológico por medio del cual el investigador explane la significancia de un determinado término desarrollado dentro del contexto literario, cuya finalidad es servir como orientador al lector en la comprensión asertiva del contenido. Razón está por medio del cual se expresan los términos siguientes:

Activos: Hace referencia a los de bienes y servicios que posee la empresa, relacionado a las capacidades operativas y funcionales que conforma la actividad y varían de acuerdo a su naturaleza y origen.

Administrador: persona cuya función es gestionar los recursos asignados para una determinada organización.

Aseguramiento: proceso que conlleva al resguardo mediante mecanismos un recurso o cosa.

Amenaza: es la eventualidad de sensación de peligro, pues contra ella está la seguridad, llegando a comprometer el sistema informático. Esta amenaza puede ocasionar que se presente datos perdidos, robados o editados; generando un efecto negativo o daño al activo.

Brecha: evento que produce una rotura o separación entre dos o más actores, producido por diferencias de caracteres o cualidades.

Calidad: efecto positivo de una cosa o recurso, o institución o función, lo que da lugar a la excelencia.

Confidencialidad: Se refiere al esfuerzo que realiza la organización para mantener los datos en secreto o en privado, donde se da acceso dependiendo del tipo de activo y el rol que ejerce en la empresa.

Control: Son contramedidas o salvaguardias para prevenir, descubrir, afrontar o disminuir los riesgos de seguridad presentes en la infraestructura, los sistemas informáticos, la información y demás activos.

Criminal: persona cuyos actos son antisociales, es decir, sus actos son infundados en la inobservancia de la ley, pudiendo enmarcarse en el derecho penal como delincuente al cometer delitos.

Disponibilidad: El activo está disponible para los usuarios de acuerdo al rol que ejerce dentro de la empresa, es importante que la información sea coherente y accesible a las partes autorizadas.

Falencia: efecto de un acto que es débil de una organización, por la falta o ausencia de probidad, gestión, o administración en una organización.

Gestión: resultado de un proceso de dirección de una gerencia organizacional.

Herramienta: un proceso que permite diligenciar una gestión organizacional conlleva a las estrategias aplicadas en la gerencia.

Información: es un contenido de acceso a datos que incumben a un proceso organizacional.

Informática: es un procesamiento de datos que se generan a partir de una base organizacional gerencial.

Infraestructura: es una cuestión de base física, que conlleva a conformar un inmueble.

Inseguridad: contrario a seguridad, es un estado de vulnerabilidad para una organización desde lo material como lo inmaterial.

Integridad: los activos se diseñan o transforman dependiendo del rol que ejercen; e implica mantener la precisión, consistencia, y fiabilidad de los datos en el transcurso de su ciclo de vida.

Optimización: proceso que permite hacer uso del mínimo esfuerzo con el mayor y mejor resultado.

Organización: es una estructura gerencial que permite conjugar elementos y recursos bajo las cualidades de planificación, dirección y administración de recursos humanos y materiales.

Plan: un proceso metódico de una organización que conlleva asumir elementos a términos de corto, mediano y largo plazo, con temporalidad futura de un activo.

Política: es el acto de llevar a cabo una estrategia a términos de una organización, bajo parámetros de procedimientos ejecutivos de un activo.

Proceso: acto de gestión que conjuga una sistematiza metódica de un transcurrir de tiempo, la cual de ejecuta en un inicio y un término con resultados para un activo.

Recurso: es un medio que permite complementar un proceso organizacional de un activo.

Resguardo: es un proceso de acción de protección y seguridad de un activo o recurso.

Riesgo: es la probabilidad de que ocurra un incidente de seguridad.

Seguridad: mecanismo que se emplea para dar sensación de tranquilidad en una organización, bien en su personal o bien para asuntos de activos.

Sistema: es una estructura de procesos que se conjugan para un fin mismo, son plasmados desde lo informático inmaterial, como orgánico en lo natural.

Tecnología: es parte de la ciencia aplicada que transforma la materia en usos variables, es transformada constantemente.

Telecomunicaciones: conjunto de procesos comunicacionales tamizados de tecnología, de corto, mediano y largo alcance.

Transmisión: proceso comunicacional de trasladar de un sitio a otro, los datos e informaciones mediante varios mecanismos o medios, dados desde la informática como otras ciencias.

Vulnerabilidad: es una situación de riesgo o latente a provocar un daño.

RESUMEN

El presente trabajo tiene como propósito el estudio de las políticas de seguridad en la organización Ortopédica Alca Plus S.A.S, la cual se proyecta en un sistema de gestión de seguridad basada en la Norma ISO 27001:2022, sobre los denominados activos desde las Tecnologías de Información y Comunicación (TIC) y en función de las buenas prácticas.

Además se busca mitigar cualquier eventualidad presente en el manejo de la información, identificar y proponer controles bajo el uso de las políticas de seguridad que pueden garantizar los pilares de los activos de la información, lo cual se despliega en el objetivo general siendo Diseñar un sistema de gestión de seguridad de la información al proceso de TIC en la organización Ortopédica Alca Plus S.A.S, mediante la aplicación de la norma ISO 27001:2022 para el mejoramiento de la confidencialidad, integridad y disponibilidad de los activos.

La investigación se concibe en el marco de un estudio de tipo descriptivo, realizada en términos de un análisis y evaluación de las condiciones de aseguramiento de la calidad de la información, para identificar las políticas de la seguridad; la cual es parte de un diagnóstico previo. Asimismo, se tomó como herramienta de recolección de información dos cuestionarios, iniciada con una prueba piloto, bajo la experiencia y observación del autor, con apoyo de un GAP análisis tipificado dentro de la Normativa ISO 27001:2022. Este evento permitió comparar el desempeño real de la organización, a fin de identificar los activos de información que posee, y se continua con el diseño de sistema de gestión de la información, a partir de la adopción de estándares y buenas prácticas, sumadas las políticas que permiten el mejoramiento de los niveles de seguridad de los activos de información en la organización, complementado con el plan de buenas prácticas a partir de la norma ISO/IEC 27002:2022. Se finaliza con las conclusiones y recomendaciones.

Palabras claves: SGSI, Norma ISO 27001:2022, Proceso TIC, Activos de información, plan de Buenas prácticas; Políticas de seguridad.

ABSTRACT

The purpose of this work is to study the security policies in the organization Orthopedic Alca plus S.A.S., which is projected in a security management system based on the ISO 27001:2022 Standard, on the so-called assets, from the Information and Communication Technologies (ICT) and based on good practices.

In addition, it seeks to mitigate any eventuality present in the handling of information, identify and propose controls under the use of security policies that can ensure the pillars of the information assets, which is deployed in the general objective being: Design an information security management system to the ICT process in the organization Orthopedic Alca Plus S.A.S, through the application of ISO 27001:2022, for the improvement of confidentiality, integrity and availability of assets.

The research is conceived in the framework of a descriptive study, carried out in terms of an analysis and evaluation of the conditions of information quality assurance, to identify the security policies; which is part of a previous diagnosis. Likewise, two questionnaires were used as a tool to collect information, starting with a pilot test, under the author's experience and observation, with the support of a GAP analysis typified within the ISO 27001:2022 Standard. This event allowed to compare the actual performance of the organization, in order to identify the information assets it has, and continues with the design of information management system, from the adoption of standards and best practices, added the policies that allow the improvement of security levels of information assets in the organization, complemented with the plan of best practices from the ISO/IEC 27002:2022 standard. It ends with conclusions and recommendations.

Key words: ISMS, ISO 27001:2022 standard, ICT process, information assets, best practices plan; security policies.

INTRODUCCIÓN

En la actualidad las organizaciones ingresan al desafío de las tecnologías informáticas, iniciando con nuevos proyectos frente a la mejora de sus procesos, orientados a la protección de la información, pues se ve como es vulnerable a ataques informáticos tanto internos como externos. Por ello, se observa como los sistemas informáticos, los sistemas operativos, la red de datos y el uso no adecuado de estos por parte de los cibernautas, dan lugar a quedar expuestos a los delincuentes en la red. Estas falencias descritas dan cabida esencial al aseguramiento en profundidad de los sistemas operativos, con ello se evita las inseguridades, los daños a la información mediante mecanismos adecuados.,

La organización Ortopédica Alca Plus S.A.S, pertenece al sector salud, presta sus servicios de atención a pacientes en rehabilitación física y venta de aparatos ortopédicos, la cual carece de certificación en sistemas de gestión, teniendo falencias en el proceso de sistemas en seguridad de la información.

Se puede ver en el desarrollo de este documento, que para garantizar el sistema se necesita en muchas ocasiones restringir las propiedades del software, desactivar servicios, y robustecer otros aspectos que pueden ser fácilmente la puerta de entrada al sistema, de esta manera se reduce el riesgo a un gran número de vulnerabilidades. Cada organización posee sus propias necesidades, en la elaboración de este proyecto se busca diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2022, que garantice los pilares de la información y la mejora continua en la organización, en especial el resguardo de los activos de información.

En tal sentido, se requiere para el resguardo de activos fundamentarse en la norma 27001:2022, la cual contempla controles, objetivos y dominios, pero se pueden lograr a través de políticas asertivas para la organización. Por ello, el estudio se desarrollará para el mejoramiento de la confidencialidad, integridad y disponibilidad de los activos, cuyo objetivo general es Diseñar un sistema de gestión de seguridad de la información al

proceso de TIC en la organización, bajo elementos como las condiciones de aseguramiento, políticas de la seguridad de la información; activos de información, plan de buenas prácticas, cuyo estándares y niveles de seguridad de los activos permitirán el diseño.

Finalmente el estudio se iniciará con un glosario, introducción, un primer capítulo donde se desarrolla la definición del problema, un capítulo 2, la cual indica la justificación, un capítulo 3 que señala los objetivos, un capítulo 4 enmarcado en lo referencial (marco teórico, conceptual y legal), un capítulo 5 que indica el diseño metodológico, un capítulo 6 la cual se desarrollan los objetivos (condiciones de seguridad, activos de información políticas de seguridad de información que permitan diseñar un SGSI basados en la ISO 27001:2022),contemplados en un plan de buenas prácticas a partir de la norma ISO/IEC 27002:2022, finalizando con las conclusiones y las recomendaciones.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Los antecedentes surgen dentro de una investigación a razón de dar cuenta previa a los acontecimientos de hechos derivados del objeto de estudio, cuando el autor decide incluirlos dentro de un proyecto de grado; a los fines de aclarar y orientar al lector y en sí mismos, sobre el propósito del contexto investigativo metodológico.

Asumiendo el párrafo anterior, para un administrador de red o una persona encargada de administrar los recursos técnicos de una organización, es muy importante conocer su estado y controlarlo, obteniendo así una administración satisfactoria y fallas o errores menores de seguridad informática, incluidos los delitos. Se puede hacer proporcionando una política de seguridad bien implementada e incluida en las herramientas de gestión que definen la configuración de seguridad de la organización. A través de estos métodos, es posible conocer el nivel de los recursos técnicos proporcionados, como servidores, enrutadores, conmutadores, firewalls y cualquier activo técnico que haya sido detectado y analizado.

Al respecto, Ortiz señala que “la definición de las políticas de seguridad de la información le permitirá a la compañía generar una campaña de concientización de las políticas para que sean incorporadas por todos los colaboradores y terceros en sus actividades diarias con el propósito de ayudar a proteger la información de los clientes y de la compañía, disminuyendo así la materialización de incidentes de seguridad”[1]. Significa esa afirmación, que entre los riesgos más significativos están: el robo de información sensible y manipulación de activos, tanto de la entidad, como de sus clientes.

[1] ORTIZ BUITRON, Vanessa Catherine. Diseño de las políticas de seguridad de la información en la compañía de seguros S.A**.** [en línea], Trabajo de grado para optar al título especialista en seguridad informática. Bogotá. D.C, Colombia: Institución. Universidad Católica de Colombia. Facultad de Ingeniería (2021). (p.33). [Consultado: 17 abril 2024]. Disponible en: https://repository.ucatolica.edu.co/server/api/core/bitstreams/671c379e-57cf-4b0b-93d1-eccb021944e5/content

Del mismo modo, Ruiz señala como se generan los “daños y repercusiones relacionados con la confidencialidad, integridad y disponibilidad”[2]. Pues provocan las penalizaciones por incumplimiento a los acuerdos con el cliente, incluso hasta el cierre del negocio por las autoridades supervisoras.

Asimismo, el proceso en el contexto de la tecnología de la información y la comunicación (TIC), son en la actualidad una interacción entre los ordenadores y las telecomunicaciones de una organización, donde su procesamiento, almacenamiento y la misma transmisión de la información son tamizadas para mejorar la calidad de la comunicación, cuya tendencia es crear aquellos nuevos y rápidos medios de comunicación y mejores en cuanto a seguridad se refiere.

Finalmente, teniendo en cuenta las dimensiones de una mayor comodidad, calidad de vida, la contribución a la protección del medio ambiente, los costos empresariales y las medidas valiosas para organizar y asegurar la calidad y la seguridad de las actividades empresariales, se puede apreciar como en las labores que se realizan a diario, se lograrían optimizar el tiempo aplicable en el proceso y el aseguramiento de estas en la gestión de riesgos en especial en el sistema de gestión de seguridad de la información al proceso de TIC en la organización Ortopédica Alca Plus S.A.S.

1.2. DESCRIPCIÓN DEL PROBLEMA

La descripción del problema, como su propio nombre lo indica, es aquel recorrido que hace el autor-investigador sobre los síntomas, causas, pronóstico y control del pronóstico, la cual derivan de lo general a lo particular o viceversa, a los fines que dar

[2] RUÍZ TAPIA, Juan Alberto; ESTRADA GUTIÉRREZ, César Enrique y SÁNCHEZ PAZ, Ma. de la Luz. Propuesta de un Modelo de un Sistema de Gestión de Calidad en Seguridad de la Información basado en la norma ISO 27001 para Instituciones Educativas. En: Revista de Investigación Latinoamericana en Competitividad Organizacional [en línea]. Editorial RILCO. (febrero 2020). Volumen Nro. 5. [Consultado: 15 de agosto de 2022]. Disponible en https://www.eumed.net/rev/rilco/05/gestion-instituciones.pdf.

una perspectiva global de las falencias existentes, a que tenga lugar una problemática y le permita al lector una mirada asertiva.

En ese sentido, las instituciones de Salud hoy en día se ayudan con el proceso de Gestión de Información y Comunicación para realizar sus actividades diarias en la organización, por eso a medida que las organizaciones van creciendo se complica el control de la información. Se hace ineludible la implementación de un sistema de gestión de seguridad de la información, que conlleve a evitar los procesos innecesarios, ineficientes y que perjudiquen, de alguna manera, la calidad del servicio, y como consecuencia daños irreparables con alto costo empresarial para el mismo capital humano encargado que podría conllevar a sanciones y despidos, baja motivación y convicción laboral.

En relación con esto, el activo más importante que tienen las instituciones es la información y datos exclusivos de interés procedimental-organizacional. Por eso, toda empresa para asegurar la información y datos deberá implementar controles de seguridad internos y externos, pues les permitirán proteger las actividades, las cuales se desarrollan y condesciendan al logro de forma adecuada y positiva en la prestación del servicio, dado que haya un estado deseado en cuanto a estructural y además sea eficiente.

De este modo, se encuentra la organización Ortopédica Alca Plus S.A.S., que actualmente se observa en función a las labores que el autor realiza dentro de ella que presenta fallas por dentro y fuera de la empresa en cuanto a la protección de la información, pues al no tener controles y medidas documentados para el manejo de la información, se hace vulnerable al presentar pérdidas de datos, afectando considerablemente los aspectos de: a) la integridad, b) la confidencialidad de la información; c) datos almacenados en los equipos tecnológicos. Pero conociendo que son exclusivos, pertinentes y únicos en los actos administrativos procedimentales que se realizan cada día en la organización.

Todo ello indica de alguna manera que, a nivel tecnológico, vale decir desde el contexto de un software, la organización Ortopédica Alca Plus S.A.S., no cuenta en la actualidad con una administración, ni con un área o persona encargada que garantice el soporte y la optimización de los equipos, donde exista el compromiso de la seguridad de los ordenadores y telecomunicaciones, para el procesamiento, almacenamiento y la misma transmisión de la información, que permita mejorar la calidad de la comunicación y su seguridad; con el fin de dar cumplimiento a la vida útil de estos, la cual una vez en uso, son susceptibles de falencias tales como:

a) el ingreso a los equipos canalizados por medio de contraseñas, la cual presentan el mismo nombre y usuario del equipo, altamente vulnerables;

b) el ingreso desde la postura del literal a, provoca que la información sea vulnerable a robo de la información, siendo susceptible a la evasión de datos o perdidas incluso de estos, perjudicando la calidad de trabajo organizacional, y

c) daños al sistema de gestión desde la seguridad de la información al proceso de tic en la organización Ortopédica Alca Plus S.A.S.

Finalmente, las implicaciones acarreadas por las falencias son por no tener una seguridad oportuna mediante la aplicación de la norma ISO 27001:2022 y en función a la protección de la información basada en el proceso de las TIC, en los actos que resguardan los datos estrictamente esenciales para una empresa, dado que se hace pertinente el diseñar un sistema de gestión de seguridad de la información al proceso de TIC en la organización Ortopédica Alca Plus S.A.S que le permita el mejoramiento de: a) la confidencialidad; b) la integridad; y c) la disponibilidad de los activos.

1.3. FORMULACIÓN DEL PROBLEMA

La formulación de un problema concibe en una hipótesis que se genera por ser de mayor incidencia dentro del contexto situacional, pues se configura en una interrogante macro,

dando lugar a su desarrollo investigativo; a los fines de resolver y dar una solución o alternativa en propuesta de diseño, modelo, constructo, proyecto factible, entre otros.

En virtud de lo comentado, se tamiza la interrogante macro siguiente:
¿Cómo se puede garantizar la seguridad del sistema de gestión de la información al proceso de TIC en la organización Ortopédica Alca Plus S.A.S., mediante la aplicación de la norma ISO 27001:2022, para el mejoramiento de la disponibilidad de los activos, la integridad y la confidencialidad?

2. JUSTIFICACIÓN

La justificación de una investigación es aquel apartado que contiene la resolución al porqué se realiza o construye un estudio, pues de ello depende la visión e interés social y académico de la propuesta investigativa. En este particular, el presente documento pretende mejorar el proceso de seguridad informática en la organización Ortopédica Alca Plus S.A.S., a la intencionalidad de presentar una propuesta de controles y políticas que permitan garantizar los pilares de la seguridad de la información organizacional.

De la misma manera, y debido a la calidad de la información que operan las organizaciones de la salud, se hace fundamental tener un plan de seguridad que se relacione con la protección integral, disponibilidad y confidencialidad. Los sistemas y procesos que controlan la información se evidencian que estos se han vuelto imprescindibles para todas las organizaciones, pues, conforman una parte crucial de las infraestructuras como un factor crítico para lograr su misión.

Lo comentado anteriormente significa que, ayuda a comprender los diversos ataques existentes y el cómo mitigar el riesgo a ser atacados tecnológicamente, así como pensar en la búsqueda de los cibercriminales. Además, se concibe cuál es el objetivo asertivo que los delincuentes tecnológicos pudiesen implementar para realizar los ataques a los recursos informáticos.

En ese sentido, se deben de asumir competencias para el uso adecuado del internet teniendo en cuenta las amenazas y riesgos que ella se encuentra, cuidar la información personal y organizacional del cómo pueden los criminales llegar a utilizarla. Por ende, es de gran importancia al conocer que se transforma en una necesidad, la cual busca averiguar y poner en conocimiento a los empleados y usuarios las diferentes herramientas que están disponibles en beneficio de elevar en la organización los niveles de seguridad informática. Igual manera, se debe tener en cuenta, como acción previa, el diseño de un plan de tecnologías de la información que se enmarque dentro de un sistema de información para Ortopédica Alca Plus S.A.S, como Organización, y así se

permita facilitar una protección completa al sistema y una mejora a las políticas, personas, procesos y gestión del riesgo que se realizan durante todo el año lectivo.

Finalmente, se quiere con la propuesta, desarrollar el presente documento, la cual busca un diseño acorde con el sistema de gestión orientado hacia la seguridad de la información y al proceso de TIC en la organización Ortopédica Alca Plus S.A.S., mediante la aplicación de la norma ISO 27001:2022, para la disponibilidad de los activos, el mejoramiento de dos dimensiones: a) la confidencialidad; y b) la integridad; a los fines de generar toda la protección del sistema de información misional, por lo que se genera la interrogante ¿cómo se hará? Pues, bien, se hará mediante el uso de las metodologías adecuadas, las cuales permitan al investigador el poder evaluar la seguridad en cuanto a los activos de información, que son parte de la organización empresarial.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar un SGSI al proceso de TIC, mediante la aplicación de la norma ISO 27001:2022, para el mejoramiento de la confidencialidad, integridad y disponibilidad de los activos en la organización Ortopédica Alca Plus S.A.S.

3.2. OBJETIVOS ESPECÍFICOS

- Evaluar las condiciones del SGSI al proceso TIC, mediante el uso de la norma ISO 27001:2022, en la organización Ortopédica Alca Plus SAS.

- Categorizar los activos de información del proceso de TIC, a partir de una metodología de gestión de riesgo que permita una valoración de los controles de confidencialidad, integridad y seguridad.

- Proponer un diseño de SGSI adaptado a ISO 27001:2022, complementado en estándares al proceso TIC, y buenas prácticas de un plan imbricado a ISO/IEC 27002:2022, que permitan el mejoramiento de los niveles de seguridad de los activos de información en la organización Ortopédica Alca Plus S.A.S.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

El marco teórico inmerso en lo referencial es un apartado estructural de una investigación lo cual, mediante una metodología, desarrolla todas las teorías pertinentes del estudio. En este sentido, Mingueza señala con respecto al marco teórico que: “son una herramienta valiosa para los investigadores, ya que proporcionan un contexto y una base para entender los resultados de la investigación y cómo se relacionan con el campo de estudio”[3].

Es por ello, que el marco teórico constituye un aspecto de extrema relevancia para la investigación pues se refiere a las teorías que fundamentan la investigación en relación con el estudio que se proyecta diseñar. Así pues, Ocampo expresa que “la teoría desempeña un papel fundamental en la investigación científica, ya que a través del marco teórico se proporcionan los principios y los supuestos que ayudan a explicar y predecir los fenómenos observados” [4].

En este orden de ideas, se puede afirmar que, el marco teórico se diseña partiendo de un cuerpo teórico amplio, o directamente a partir de la consideración de una teoría. Para proceder a esta elaboración, se debe haber realizado una revisión de diversa literatura existente sobre el tema objeto de estudio. Cabe resaltar que, este es el resultado de una mezcla ecléctica de diferentes perspectivas y de puntos de vistas teóricos e incluso posturas contrapuestas.

---

[3] MINGUEZA, Sergio. Marco teórico: definición, estructura y ejemplos. [en línea]. (31 de enero de 2023). [Consultado: 17 de abril de 2024]. Disponible en: https://expertouniversitario.es/blog/marco-teorico/#toc_Que_es_un_marco_teorico.

[4] OCAMPO WILCHES, Ana Cristina. Papel de la teoría en la investigación. [en línea]. (septiembre de 2023). [Consultado: 17 de abril de 2024]. Disponible en: https://www.researchgate.net/publication/374248226_Papel_de_la_teoria_en_la_investigacion.

Finalmente, para dar contexto al objetivo nro. 1, se sistematiza un Sistema de Seguridad de la Información (SGSI), proceso y normas, importancia tecnológica empresarial, vulnerabilidades del proceso TIC y las perspectivas y aplicabilidad de la Norma ISO 27001:2022.

4.1.1. Sistema de Seguridad de la Información (SGSI), proceso y normas.

Los Sistemas de Seguridad de la Información, conceptualizados por Da Silva representan: "medidas y acciones que tienen como objetivo proteger todos los datos de una empresa que han sido generados, recibidos, analizados, procesados y/o almacenados. El propósito de la seguridad de la información es blindar a la organización de ataques digitales de ciberdelincuentes así como protegerla de fugas de datos y accidentes tecnológicos"[5].

Asimismo, el SGSI es definido según ISO 27001:2022 como: "Un sistema de gestión para la Seguridad de la información se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan a la seguridad de la información en una empresa u organización"[6].

Se infiere que de allí parte la conceptualización basada en el estudio que se pretende diseñar respecto a un SGSI que resguarde los activos para la organización Ortopédica Alca Plus. S.A.S.

4.1.1.1. Importancia Tecnológica Empresarial

Se hace oportuno mencionar, la importancia que asoma toda empresa respecto a sus activos de información, pues se debe destacar las falencias en la documentación, el

[5] DA SILVA, Douglas. ¿Qué es la seguridad de la información?. [en línea]. (18 de septiembre de 2023). [Consultado: 17 de abril de 2024]. Disponible en: https://www.zendesk.com.mx/blog/que-es-seguridad-de-informacion/.
[6] ISO 27001:2022. Norma ISO 27001:2022 [sitio web]. Madrid España. [Consultado: 30 de agosto de 2022]. Disponible en: https://normaiso27001:2022.es/.

control, la falta de organización y la ausencia de funciones y responsabilidades, la cual ponen en riesgo la integridad y la vulnerabilidad del sistema tecnológico por la amenaza de pérdidas significativas, dado que la información es un activo de la organización. Para contrarrestar estos efectos, Martelo, Madera y Betin[7], señalan, la importancia está en qué la información, cómo un activo, requiere de normas, políticas y protección de datos basadas en la teoría organizativa. Por ejemplo, en la interrelación entre personas y recursos materiales, la seguridad de la información es especial, igual el control de acceso de los usuarios, otro sería la seguridad de la red en materia de tecnología. Todo ello como tejido requerido para una verdadera toma de decisiones que garantice el renglón del proceso de las TIC.

Finalmente, este apartado concibe que una situación como la antes planteada no puede desconocer el avance tecnológico que se viene presentando en este Siglo XXI, pues trae sus propios desafíos, preocupaciones a los altos directivos organizacionales. Gómez[8], indica que se hace necesario incrementar los niveles de disponibilidad, integridad y confidencialidad, ambos en lo que respecta a la información que se maneje en las organizaciones, la cual puedan garantizar la protección de los activos de información en el mundo empresarial.

4.1.1.2. Vulnerabilidades del Proceso de TIC

Se permite, sobre la base de las vulnerabilidades, indicar la postura de Martelo, Madera y Betin[9], quienes exponen qué cómo el mundo de las redes se exterioriza a diferentes amenazas con los ataques de los ciberdelincuentes, estos únicamente buscan es sabotear la confidencialidad de la información para modificarla y así obtener un beneficio, ya sea económico, comercial, competitivo o simplemente inquiriendo que el agresor

[7] MARTELO; MADERA y BETIN. Op.cit, p.130.
[8] GÓMEZ, F. (2020). La Importancia de implementar un SGSI en nuestra organización. [blog]. Safe Society. Disponible en https://www.safesociety.co/blogitem/4/la-importancia-de-implementar-un-sgsi-en-nuestra-organizacion.
[9] MARTELO; MADERA y BETIN. Op. cit., p. 133.

alcance renombre. En este proceso tecnológico se evidencia que existe y existirán vulnerabilidades, por las cuales toda empresa debe trabajar para el resguardo de activos. Sin embargo, el tener un buen SGSI mejora esta problemática no solo en lo que afecta a las grandes empresas u organizaciones dotadas de infraestructura para su funcionamiento, hoy en día, hasta las pequeñas empresas, los gobiernos o personas del común no se escapan de estos ataques informáticos, la experiencia y la información que, a diario, en labores del manejo de los activos de información se conocen y basan sus riesgos en el proceso de las TIC.

Se observa en la actualidad como, los desafíos a que se ven enfrentados las grandes, medianas y pequeñas empresas son preocupantes, puesto que el impacto a los daños informáticos ha generado pérdidas de millones de dólares. Asimismo, los procesos con las TIC, y los grandes avances tecnológicos, han conmovido el mundo empresarial, puesto que los SGSI son prioridad para el control y supervisión, además la cualidad de garantizar los activos de información.

Por ante lo expuesto, se puede traer a colación a los autores Martelo, Madera y Betin[10], quienes dicen que conoce en el mundo empresarial estudios recientes donde informan que en los últimos años se han presentado más de ciento noventa y ocho (198) millones de ciberataques, los cuales ponen en riesgo las variables siguientes: a) la disponibilidad de la información; b) la credibilidad, c) la confidencialidad; y d) la integridad. Significa que los SGSI., son relevantes para una empresa, en especial cuando se trata de los avances del desarrollo tecnológico, la cual cada vez es mejor, debiéndose invertir en el campo de la seguridad informática como una necesidad y prioridad.

4.1.1.3. Perspectivas y aplicabilidad de la Norma ISO 27001:2022.

Sobre este particular, se trata de un sistema que proporciona seguridad, evalúa de forma continua y adecuada los riesgos que golpean a diario en el entorno empresarial, y

[10] MARTELO; MADERA y BETIN. Ibíd., p. 134.

proporciona las mejores prácticas y procedimientos para establecer controles que protejan y aseguren el elemento más valioso del negocio: la información.
Se hace evidente y fundamental que cada organización o empresa radique e implante su SGSI basado en la norma ISO 27001:2022, la cual proporcione un proceso sistemático para proteger la información frente a los ciberataques, cuyo propósito es comprometer las variables siguientes: a) la disponibilidad de la información; b) la credibilidad, c) la confidencialidad; y d) la integridad. Siendo así, las perspectivas comerciales, legales, contractuales y reglamentarias, evidencian la necesidad de la aplicabilidad de la ISO 27001:2022, la cual entra a conformar parte de un lineamiento rector, porque es trazada para garantizar la selección de las medidas de seguridad adecuadas y proporcionadas, así como el proteger la información de acuerdo con requisitos reglamentarios.

Por ante lo expuesto, un diseño sobre SGSI, hace que las empresas más jóvenes sean más productivas y entiendan la responsabilidad que adquieren cuando tratan con información de sus clientes. Asimismo, proporciona un aval para los activos de información y la seguridad de estos, puesto que es aceptado a nivel mundial que el tema del SGSI es la base sobre la cual riela la efectividad de la seguridad de la información dentro de una organización.

Finalmente, todos estos aspectos mencionados, hacen que un sistema de gestión de seguridad de la información, requiera a todo efecto la garantía de seguridad del activo de información, para que permita analizar y gestionar los riesgos a los que está expuesta la empresa, fundamentados en los procesos misionales y activos de información mismos, con los que se cuenta, y así llegar a lograr la garantía con un mayor control en relación con las amenazas, sin perjuicios directos o indirectos del funcionamiento de una organización.

4.1.2. El SGSI y activos de información del Proceso de TIC, riesgos y control

El conocer qué beneficios trae a las organizaciones sobre la implantación de un SGSI, evidentemente data su importancia, entendiendo que las ventajas que aportan son beneficiosas y de forma positiva en las operaciones empresariales, tanto financieras, como de talento humano, en este caso particular dan lugar a mejores procesos tecnológicos y a sus activos de información. Se puede observar que la implantación de un SGSI, trae una serie de ventajas, entre ellas las que a continuación se mencionan: a) El proceso empresarial, costos y recursos aplicables; b) La gestión de riesgos vs competitividad: una prioridad empresarial; c) Los controles de confidencialidad, integridad y seguridad.

4.1.2.1. Proceso empresarial, Costos y recursos aplicables.

El proceso empresarial, costos y recursos aplicables en una organización, permiten una continuidad del negocio, pues bajo una viabilidad de una empresa, esta puede verse comprometida con la filtración de datos. Concatel[11], en su contexto, señala que se debe implementar un SGSI, la cual contribuya en responder acertadamente ante cualquier eventualidad o amenaza. La implementación de un sistema puede contribuir significativamente a la optimización de recursos y costes en una organización, permitiendo lograr identificar y mitigar los riesgos de seguridad de la información, reduciendo con esto las posibilidades de incidentes costosos, como brechas de seguridad, pérdida de datos o interrupciones en el negocio.

Sin embargo, una incorrecta aplicabilidad del funcionamiento del SGSI podría ocasionar pérdidas económicas asociadas tanto a ataques cibernéticos y filtraciones de datos, como a interrupciones del servicio y fallas del sistema.

[11] CONCATEL. Ventajas de la implantación de un SGSI. [blog]. Barcelona, España. 2022. [Consultado: 31 de agosto de 2022]. Disponible en: https://acortar.link/eGEjsN.

4.1.2.2. La Gestión de riesgos Vs Competitividad: Una prioridad empresarial.

La competitividad, como dimensión, se permite a medida que transcurre el tiempo, sea observada en cuanto a los mercados y sus valoraciones, desde la óptica positiva en cuanto a las políticas de control de la seguridad de la información. Concatel[12] indica que, la credibilidad de las organizaciones sobre los SGSI, va en aumento, puesto que su implantación supone una garantía de calidad que demuestra el compromiso de la empresa con la protección de la información que se almacena y/o transmite. Todo lo expuesto permite disponer de la certificación ISO/IEC 27001:2022, aquella cuya esencia da lugar a convertirse en un elemento que diferencia una empresa de sus competidores.

De esa manera, la confianza en la organización se fortalece, en función a las prioridades de los SGSI, la cual puede ser el mantener la privacidad y la integridad en mayoría de las organizaciones y, especialmente, de aquellas que manejan información personal y sensible de sus clientes, usuarios y proveedores.

Es evidente, que tener en las organizaciones un SGSI, aumenta la confianza en la organización, la cual es una garantía de su compromiso con la confidencialidad y protección de sus datos.

4.1.2.3. Controles de confidencialidad, integridad y seguridad

El cumplimiento de la ley y demás normativas, permiten se adecuen las políticas de seguridad a los requisitos exigidos, tanto nacionales, como internacionales, pero asumiendo que su no cumplimiento da lugar a las sanciones relacionadas cuando no se resguardan los datos almacenados, la privacidad y la protección de las organizaciones, las cuales deben de evitarse. El fiel cumplimiento a las normativas debe estar ajustado a lo ordenado por los entes u órganos ejecutivos del Estado. En otras palabras, es ganar-ganar, es un atrevimiento decir que, la garantía de los activos de información de una

[12] CONCATEL, Op. cit., p.01.

empresa u organización, dependen de la confidencialidad, integridad y aseguramiento de sus datos. Con ello se evidencia la garantía de una buena captación de clientes y negocios, asumiendo el control de las vulnerabilidades de los datos y seguridad, además de la imagen empresarial frente al uso un SGSI.

Cuando se asume el reto de conquistar clientes, siempre se observará que tan confiable e integral, es una organización. De allí que, se evidencia la necesidad de obtener nuevos negocios y fidelizar clientes, esto radica en función al proceso de las TIC y su conjugación a obtener nuevos clientes. Es decir, que al implementar un ISO 27001:2022, trae como beneficio es que esta certificación no solo contribuye a las nuevas organizaciones a demostrar que emplean las mejores prácticas sobre la seguridad de la información, sino que mejora las relaciones comerciales, manteniendo clientes existentes y ofreciendo ventajas de marketing sobre sus competidores, porque hay compensación ante las vulnerabilidades de datos y seguridad.

Se hace oportuno evitar las pérdidas financieras y las sanciones asociadas con las vulneraciones de datos y seguridad, sea un asunto que dentro del proceso financiero las faltas en cuestiones de seguridad de datos pueden incurrir en sanciones y multas bastante elevadas, teniendo en cuenta que, a mayor dimensión y complejidad de una organización, más posibilidades existen de una multa de mayores dimensiones.

En efecto, para las organizaciones jóvenes, una sanción por temas asociados con la vulneración de datos puede representar su extinción o su desaparición, puesto que una recuperación, después de una desbastadora multa, se hace cuesta arriba, y alta complejidad respecto a la motivación y otros elementos intrínsecos por parte del capital humano desde la dirección hacia abajo, hablando de niveles jerárquicos.

Por tal razón, se hace productivo contar con ISO 27001:2022, el estándar global aceptado para la gestión eficaz de los activos de información, pues se pueden evitar este tipo de penalizaciones altamente costosas por incumplir con los requisitos de protección

de información y por las pérdidas financieras ocasionadas por la vulneración de la seguridad de la información. Todo ello permite multiplicar la imagen empresarial.

La protección y mejoramiento de la reputación de una organización, asume diferentes fases, siendo primero a lo que afectan los ataques cibernéticos, pues es a la reputación y a las finanzas de la organización involucradas, donde se supone que su política no es eficaz.

Cabe resaltar que los ataques cibernéticos y tecnológicos, aumentan diariamente en el proceso financiero y operativo, tanto en volumen como en impacto. Implementar un sistema de gestión desde la seguridad de la información, la cual favorece y otorga protección a la organización ante esta falta de confianza, puesto que con este se demuestra que por necesidad se han tomado las medidas para proteger la organización.

4.1.3. El plan de buenas prácticas, Normativa de Seguridad de la Información.

La seguridad de la información puede ser un resultado positivo desde la mirada financiera; minimizando ocurrencias en los procesos, que garanticen protección y reflejen una estadística bajo cero amenazas tecnológicas, entre otras. A razón de este escenario, se estandariza y surge una norma internacional ISO 27002, planteada en Ostec. Iso 27002[13], en ella se alinean las buenas prácticas hacia una gestión de la seguridad de la información. Obviamente, una organización basada y protegida bajo la esencia de un SGSI, esta garantiza una continuidad en sus procesos de seguridad, alineados a los objetivos estratégicos que posea la empresa.

Se evidencia que, las buenas prácticas provienen de ISO/IEC 27002, en ella se establecen los códigos sobre las mejores prácticas para apoyar la implantación del SGSI organizacional en cuanto a controles se refiere. Además, hay una simbiosis entre

[13] OSTEC. ISO 27002: Buenas prácticas para gestión de la seguridad de la información. [sitio web]. Ubarão, Brasil. Business Security; [Consultado: 22 de agosto de 2022]. Disponible en: https://acortar.link/Szl5C0.

riesgos-activos; porque dada las circunstancias de una empresa, estas deberían velar por la tecnología, en especial el proceso TIC. Con ello, una gestión de la seguridad de la información, puede dar ventajas, como certificación, ante variables como concienciación, control de activos y riesgos de estos, políticas de control, generar competitividad, optimización de costos ajustados a las leyes, entre otras normativas vigentes.

Por lo tanto, la norma ISO/IEC 27002, referenciada en Ostec Iso 27002[14], contiene elementos direccionados hacia los controles de seguridad de la información, se evidencia aspectos que en ella trata como: a) Adquisición, desarrollo y mantenimiento de sistemas; b) Conformidad y control de acceso; c) Gestión de activos, continuidad e incidencias; d) Organización de la Seguridad de la Información; e) Política de Seguridad de la Información; y f) Seguridad comunicacional, recursos humanos, física y medio ambiente. Todo ello garantiza la seguridad de la información empresarial, y gestiona camino a la certificación de seguridad ante el proceso de implantación de las buenas prácticas.

Lo antes contemplado, permite que una organización gestione adecuadamente y con parámetros estandarizados un plan de buenas prácticas, la cual conlleva asegurar y contrarrestar las amenazas y las variantes de ataques a las que se ven expuestas la información de la organización, estas son cada vez más, así como a los sistemas empleados para su tratamiento.

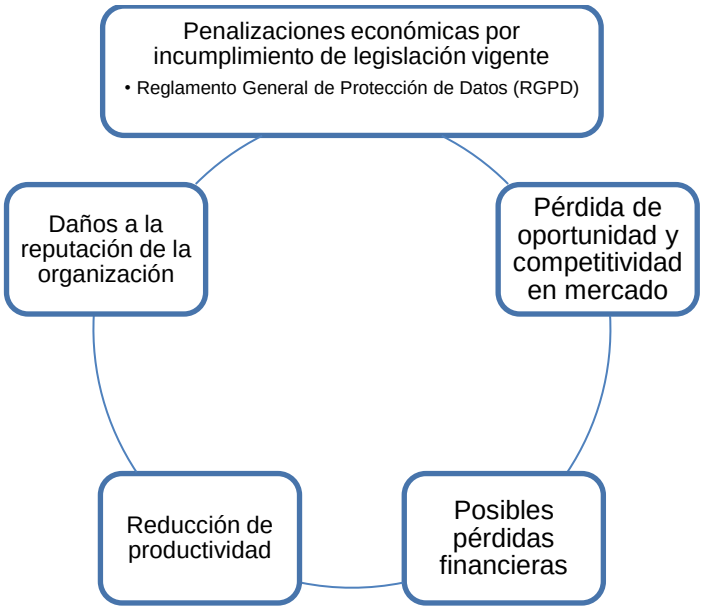
Por lo tanto, se hace necesario contar con un SGSI, con ello un plan de buenas prácticas que permita resolver de forma controlada estos riesgos y garanticen la protección correcta de los activos de una organización, así como, se puedan detectar los ataques que se generen contra la organización, para ello se deberá contar con un plan, la cual dé respuesta rápida y eficaz ante incidentes de problemas de seguridad. Ante la resolución de un plan de buenas prácticas se debe asumir este dentro del SGSI, pues debería conformar todos los aspectos de riesgos.

[14] Ibíd., p.01.

4.1.3.1. Seguridad de la Información basada en riesgos para un plan de buenas prácticas ante un SGSI.

No contar con un SGSI, como lo indica *Semic Effective It Solutions* [15], aumenta el riesgo de incidentes de seguridad. Es por ello que, construir un plan de buenas prácticas, pueden evitar las consecuencias, como se exponen en la figura 1.

Figura 1. Consecuencias ante la ausencia de un SGSI de una organización.



Fuente: SEMIC EFFECTIVE IT SOLUTIONS. ¿Por qué necesitamos un SGSI?. Publicado el 22 de octubre de 2018. Disponible en: https://www.semic.es/es/content/por-que-necesitamos-un-sgsi

Como es de observarse en la Figura 1, las consecuencias de una organización, cuando no cuenta con un verdadero SGSI, la hace acreedor de una vulnerabilidad, cuyos riesgos son de alto costo[16]. Un plan de buenas prácticas, ayuda al mejoramiento, y evita o reduce

[15] SEMIC EFFECTIVE IT SOLUTIONS. ¿Por qué necesitamos un SGSI? [blog]. Madrid, España. 22 de octubre del 2018. [Consultado: 01 de septiembre de 2022]. Disponible en https://www.semic.es/es/content/por-que-necesitamos-un-sgsi.

[16] ISOTools Excellence. ¿Cuáles son los motivos por los que implementar un Sistema de Gestión de Seguridad de la Información? [blog]. Blogs Seguridad de la Información. Blog especializado en Seguridad de la Información y Ciberseguridad. 22 de Octubre de 2020. [Consultado: 10 de noviembre de 2022].

en algunos costos materiales y capital humano; tanto así que, entre las cinco consecuencias nombradas, la de mayor incidencia son las penalizaciones económicas por incumplimiento de legislación vigente, prevista en el Reglamento General de Protección de Datos (RGPD), aunque con menos incidencia están las pérdidas de oportunidad y competitividad en mercado, las posibles pérdidas financieras, la reducción de productividad y por si fuera poco, están los daños a la reputación de la organización.

En atención a lo comentado, es clave la implantación de un plan de buenas prácticas enmarcado en el SGSI, al igual que ocurre con otros sistemas de gestión, permeados de la calidad, es una decisión estratégica, pues daría cabida en la organización, la cual persigue el objetivo principal al garantizar las tres variables de seguridad, entre ellas: a) la disponibilidad de la información; b) la confidencialidad; y c) la integridad. Este sistema siempre estará apoyado por un proceso continuo de Gestión de Riesgos para asegurar el tratamiento adecuado de los riesgos identificados y estará integrado con los demás procesos que conforman la organización para contribuir al logro de los objetivos.

De esa manera, se observa, como un SGSI se podría tomar como referencia para diseñar, poner en práctica, supervisar, verificar, conservar y hacer mejoras para proteger los activos de información de la organización. Entendiendo que la base o referencia de un sistema siempre será la Política de Seguridad de la Información, donde la empresa plasmará su contexto, los requerimientos de seguridad y la estrategia para la consecución de los objetivos.

Evidentemente, *Semic Effective It Solutions*[17], expresa que un sistema estará basado en una evaluación continua de los riesgos que permita una gestión eficaz y eficiente de los mismos, e incluye el liderazgo, planificación, responsabilidades, estructura organizativa, políticas, roles, procedimientos, procesos y recursos para una exitosa implementación del sistema. Se comparte esta posición, pues el éxito de esa implementación de un SGSI,

---

Disponible en: https://www.pmg-ssi.com/2020/10/cuales-son-los-motivos-por-los-que-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion/

[17] *Semic Effective It Solutions*. Op. cit., p. 01.

dependerá del grado del entendimiento que se tiene de la Organización en su contexto, bien en lo legal y normativo, o político, o bien en lo geográfico, entre otros, y de los requisitos de seguridad, tanto por cumplimiento legislativo o normativo, como las propias necesidades de las partes interesadas como pueden ser los empleados, clientes, proveedores o inversores.

Asimismo, *Semic Effective It Solutions*[18], indica lo fundamental que es contar en todo momento con tres elementos esenciales para la implementación de un plan de buenas prácticas donde su eje prioritario sea el SGSI, la cual son plasmados por PDCA, *(Plan-Do-Check-Act);* cuya finalidad es la garantía del buen funcionamiento sobre cualquier sistema de activo de información, además la de detectar oportunidades de mejora, con la aplicación del Ciclo de Deming.

Figura 2. Elementos esenciales de un SGSI, dentro del Ciclo de Deming.

Fuente: ISO TOOLS EXCELLENCE. Descubre qué es un SGSI y cuáles son sus elementos esenciales. [Consultado el 10 de julio de 2022]. Disponible en: https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cuales-sonsus-elementos-esenciales/

[18] Ibíd., p.01.

La figura 2, permite ilustrar los tres elementos básicos que deben constituirse al implantar en una empresa un SGSI.[19], entre ellos se cuentan con el liderazgo, la supervisión y el soporte de la Dirección[20].

La situación antes planteada, hace que un plan de buenas prácticas, mediante un sistema garantice que la seguridad se incorpora como un elemento esencial de las redes y sistemas de información intentando implantar en la Organización la cultura de *Security By Design* (seguridad por diseño), sin olvidarnos del desarrollo seguro del software, que encajaría perfectamente en esta cultura preventiva.

De manera pues, a pesar de las medidas de seguridad implantadas, es muy probable que la organización sufra algún incidente de seguridad, por ello el sistema tendrá que incluir un plan de respuesta ante incidentes, las cuales permitan un tratamiento eficaz y eficiente de los mismos.

Por último, pero no menos importante, es la formación y la concienciación en materia de seguridad de la información por parte de los directivos empresariales. Hay que formar a las partes interesadas lo interesante de identificar y detectar posibles amenazas para prevenir su materialización, esto verdaderamente ponen en riesgo la seguridad de la información o de los recursos de tratamiento de ésta, en opinión de la experiencia del autor en la organización Ortopédica Alca Plus, S.A.S; entre otros elementos, estos son algunos de los motivos del porqué de la implementación de un Sistema de Gestión enmarcado en la Seguridad de la Información en la organización. Todo hace necesario el que se debe de alguna manera conocer el contenido de la Norma ISO/IEC 27001:2022, la cual especifica los requisitos de un SGSI, que conlleve las variables siguientes: a) mejorarlo de manera continua y permanente, b) establecer las líneas de acción, c) implementar medidas de seguridad, y d) mantener la seguridad permanente del Sistema.

---

[19] BETANCOURT, Diego. Ciclo de Deming (PDCA): Qué es y cómo logra la mejora continua. [En línea]. 02 de agosto de 2018. [Citado 1 de diciembre de 2022]. Disponible en: (www.ingenioempresa.com/ciclo-pdca).
[20] ISOTools Excellence. Op.cit. 01.

4.1.3.2. Normativa ISO/IEC 27002:2013 ante la Seguridad de la Información

La seguridad de la información desde la óptica de la estandarización, *Universitat Oberta de Catalunya*[21]*, establece* que esta se encuentra en la normativa ISO/IEC 27002:2022, y por lo tanto se gestiona como un estándar internacional, la cual se implanta en los controles de un Sistema de Gestión que contemple la Seguridad de la Información, en su estructura concentra varios controles entre ellos: acceso a datos y claves en lo administrativo, criptográficos y por si fuera poco los confidenciales o secretos.

Igualmente, *Universitat Oberta de Catalunya*[22], indica que la ISO/IEC 27002:2022 contiene en su estructura controles que atiende a los datos siguientes: 14 dominios; 35 objetivos de control; y 114 controles. Además, se forja la Seguridad de la información, la denominada Ciberseguridad, incluida la protección sobre la privacidad, aquellos controles que proporcionan los elementos del conjunto de referencia de la seguridad de la información desde la óptica de los controles, objetivos y dominios.

Igualmente, ISO 27001:2022, hace referencia a ISO 27002. Esta norma es un catálogo de buenas prácticas para la seguridad de la información, basado en la experiencia de la implementación de controles aceptados por empresas y organizaciones globales. Igual sirve como una guía para implementar las medidas y controles de seguridad. Esta guía se debe usar como una lista de verificación para seleccionar los controles adecuados a partir de un análisis de riesgos. Esto determinará los recursos necesarios y los ciento catorce controles, las cuales se agrupan en catorce capítulos, y estos subdivididos en áreas de seguridad.[23]

---

[21] UNIVERSITAT OBERTA DE CATALUNYA. Principales novedades de la norma ISO /IEC 27002:2013. [Blog]. 4 de julio 2021. España. [Consultado: 22 de agosto de 2022]. Disponible en https://blogs.x.uoc.edu/calidad-iso/principales-novedades-de-la-norma-iso-iec-270022013/.

[22] Ibíd, p.01.

[23] ISO 27001:2022. Norma ISO 27001:2022. [sitio web]. Madrid. España; [Consultado: 22 de agosto de 2022]. Disponible en: https://normaiso27001:2022.es/.

Como es de observarse, la norma 27002, su propia estructura cuenta con catorce capítulos, se ubican además treinta y cinco categorías (objetivos de control) y los ciento catorce controles, que lógicamente se asocian a los objetivos. Se debe destacar que la normativa in comento se presenta como referente innovador de controles seleccionados y certificable de ISO/IEC 27001:2022, las cuales dieron un giro cambiante a partir del 16-02-2022, al ser publicada por ISO (*International Organization for Standardization*) la actualización de ISO 27002.

En ese sentido, el Estándar tiene una nueva estructura, comenzando con una introducción (que contextualiza el valor de la información específica de ISO/IEC 27000; Alcance (indica control de proceso); sin indicaciones reglamentarias (sin términos, definiciones y abreviaturas en el contexto reglamentario); estructura del documento (cláusula, tema y atributos y diseño de cada estructura de control incluida en la norma, incluidos los controles de seguridad organizacional, personal, física, tecnológica). También se aplica dos anexos, uno sobre las características de los controles y otro sobre vínculos entre ISO/IEC 27002 (2022-2013); concluye con una bibliografía (documentos citados en la norma).[24]

Es por ello que, la novedad adquirida de la ISO 27001:2022, está referida al nombre actual asumiendo varios constructos: a) Seguridad de la información; b) Ciberseguridad; c) Protección de la privacidad; pero enmarcada en los Controles de seguridad para la información. Se infiere que la norma abre un abanico de dimensiones que deben considerarse como la prevención, detección y respuesta a ciberataques y protección de los datos; otras dimensiones son los cambios en controles de seguridad y nueva estructura de atributos de controles. Respecto a esta última, considera el tipo de control, las propiedades de seguridad de la información, conceptos de ciberseguridad, las capacidades operativas y por último pero no menos importante los dominios de

[24] GLOBAL SUITE SOLUTIONS: Los principales cambios de la actualización de la norma ISO 27002:2022. (28 de 02 de 2022). [sitio web]. [Consultado: 7 de noviembre de 2022]. Disponible en: https://www.globalsuitesolutions.com/es/cambios-norma-iso-27002-2022/.

seguridad, la cual aborda los controles desde los dominios de seguridad de la información denominados Gobernanza-ecosistema, Protección, Defensa, Resiliencia.[25]

4.1.4. Los Estándares, Políticas y objetivos de seguridad de la información.

El principal objetivo del SGSI se encuentra referido a los estándares y a las políticas de seguridad informática. Dichas variables conforman el documento breve de alto nivel, lo cual requiere ser detallada en las organizaciones públicas y privadas, donde de alguna manera deben ser conocidas como elemento sine qua non en aportar la seguridad de la información, especialmente hacia los activos de información para el control y seguimiento de procesos de las TIC.

A ese efecto, Alvarado[26] señala que, el SGSI tiene sus propias políticas estratégicas, las cuales explanan sus objetivos en función al rendimiento y control de seguridad. Además, se establece sobre la conceptualización de los activos, la función a la seguridad de la información, y menciona que un Activo de información en el marco del estándar ISO/IEC 27001:2022, representa para una organización, una prioridad en tres dimensiones de propiedad: a) la confidencialidad; b) la integridad; y c) la disponibilidad. Todos merecen control, completitud, y acceso al uso de los sistemas informáticos; no obstante, trabajar las herramientas con datos informáticos.

Al respecto, ISO en su página oficial, explana políticas estratégicas y objetivos que conllevan respecto a la norma ISO/IEC 27001:2022, en ella especifica los requisitos las cuales son de carácter general y están destinados a aplicarse a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Este respaldo permite la implementación de medidas tales como el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la

[25] GLOBAL SUITE SOLUTIONS. Op.cit., 01.
[26] ALVARADO, Claudia. Sistema de gestión de seguridad de la información: qué es y sus etapas. [Blog]. Bogotá. 2022. [Consultado: 28 de agosto de 2022]. Disponible en https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas.

información en el contexto de la organización. Al evaluar los riesgos de seguridad de la información, se adaptan a las necesidades de la organización.[27]

Se observa como la norma ISO presenta sus propios estándares a nivel mundial, siempre relacionados con los SGSI, en función a ser un activo de información empresarial, dado en control de riesgos, orientados a la seguridad informática.

Seguidamente, en el portal de Sisteseg.com, se hace referencia a las políticas y estándares de Seguridad de la Información que se indican en las normas 27001:2022, donde se pueden apreciar los siguientes aspectos: las estrategias para aplicar controles en la interacción entre usuarios y activos informáticos. Promueve la independencia de los ambientes de la entidad y sirve como base para un modelo de seguridad. Describe la dependencia cultural de la organización, el análisis de riesgo, la clasificación de la información, la seguridad del recurso humano, la seguridad física y la administración de operaciones de cómputo y comunicaciones. Además, incluye la audiencia, introducción, definiciones, objetivo, enunciado de la política, políticas y procedimientos relacionados, roles y responsabilidades, así como la forma de abordar las violaciones a la política. Dicha norma alude a los estándares de seguridad, los cuales pueden ser cuantitativos o cualitativos, dependiendo del valor o parámetro establecido en los procedimientos. Esto se aplica a las contraseñas en términos de longitud e historial, los Sistemas Operativos, los eventos registrados en logs, y los estándares de seguridad para Switches, Routers y VPN.[28]

---

[27] ISO. ISO/CEI 27001:2022:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. [sitio web]. Octubre del 2013. Chile. [Consultado: 20 de agosto de 2022]. Disponible en https://www.iso.org/standard/54534.html.

[28] Sisteseg.com. Seguridad de la información ISO 27001:2022. [sitio web]; [Consultado: 28 de agosto de 2022]. Disponible en: https://www.sisteseg.com/informatica.html.

4.1.5. El SGSI y el proceso de las TIC, niveles de seguridad de los activos de información.

La seguridad de la información requiere su propio tratamiento, y para ello, se evidencia que los procesos donde amerita un SGSI, deben contar con la protección debida. No obstante, en el portal de CEUPE[29], indica que la protección garantista de una organización tiene su base en la fiabilidad, eficiencia en seguridad de la información, dando cabida a indicadores como: un rendimiento positivo, la confianza a clientes, captación de inversores, una continuidad organizacional, mínimo riesgo de daño e impacto potencial en las actividades y procesos eficaces en coste/beneficio de gestión, y en especial el proceso TIC.

De acuerdo a esta conceptualización, CEUPE, trabaja sobre políticas de seguridad de gestión de riesgos e información de seguridad, su misión es garantista en cuanto al proceso TIC, que abarca: a) la confidencialidad; b) la integridad; y c) la disponibilidad de la información. Es evidente que toda organización aplique políticas y directivas de seguridad eficaz y eficiente para la seguridad de los activos de información.

Finalmente, las políticas de seguridad tamizan todos los niveles incluidas las tecnologías, el capital humano, los principios, el mismo proceso organizacional, y los controles sobre las actividades de conectividad, redes, y en especial el resguardo de los activos de información de la organización, bajo la expectativa de las amenazas y vulnerabilidades.

4.2. MARCO CONCEPTUAL

El marco conceptual desde la mirada metodológica contempla los elementos mediante el cual el autor de un trabajo o estudio de investigación, quiere dejar claro cuál es la percepción asertiva de una palabra, dando lugar a sus presupuestos, ya definidos con anterioridad.

[29] CEUPE. Política de seguridad de la información y SGSI. [sitio web]. [Consultado: 21 de agosto de 2022]. Disponible en https://acortar.link/lLXUoH.

4.2.1. Norma ISO 27000

Es una norma internacional relacionada con la implementación de la ISO-27001:2022, que garantiza la seguridad, privacidad y protección de la información, datos y sistemas que la utilizan. Constituye una ventaja que mejora la competitividad y la reputación de la organización. Esto se obtiene explorando cuales son los principales problemas que afectan la información y luego proteger lo que es necesario para impedir que existan problemas.

4.2.2. Norma ISO 27001:2022

Este es un estándar internacional que le permite garantizar la confidencialidad e integridad de los datos e información y los sistemas que los procesan. En función a ser la norma, el portal Sisteseg.com, indica el cómo se regirá la propuesta, la cual se tomará en cuenta lo indicado en la normativa desde sus conceptualizaciones concebida por Organización Internacional de Normalización; con el fin de asistir en la administración de la protección de datos en una organización. La versión actual de la Norma se conoce como ISO/IEC 27001:2022 y se trata de una actualización de la primera versión publicada en 2005. Esta norma fue desarrollada a partir de la adaptación de la norma británica BS 7799-2 por parte de la ISO. El certificado de ISO 27001:2022 resulta atractivo para cualquier compañía, independientemente de su tamaño y sector de trabajo. La determinación sobre si implementar o no un sistema de gestión de la seguridad de la información depende de lo crucial que sean los activos de información en una organización, ya que son elementos indispensables para alcanzar sus metas.[30]

Como puede verse, la norma 27001:2022 es una de las principales para proteger los activos de seguridad de la información de una organización. A nivel mundial y regional, la norma ISO 27001:2022 puede considerarse como el punto de referencia para la certificación de la seguridad de la información en las organizaciones.

---

[30] Sisteseg.com. Seguridad de la información ISO 27001:2022. [sitio web]; [Consultado: 28 de agosto de 2022]. Disponible en: https://www.sisteseg.com/informatica.html.

4.2.3. Norma ISO 27002

Es un estándar que contiene lineamientos para la seguridad de la información de la organización, además de imbrica en las prácticas de gestión de la seguridad de la información.

4.2.4. Activos de información

Son aquellos recursos de una organización, las cuales son parte de un Sistema de Gestión de Seguridad de la Información para el mejor funcionamiento y propósitos. Los activos son imbricados por la norma ISO 27001:2022, en ella se plasma los inventarios de activos de información. En cuanto al costo, un activo es de valor esencial para una organización, la cual representa según su naturaleza una destacada importancia.

Obedece su conceptualización a que la norma ISO 27001:2022, tiene como objetivo la protección de los activos de la información de cualquier organización, por lo que, ésta debe ser protegida ante cualquier eventualidad y riesgo o amenaza. La información fundamental empresarial es lo que se denomina activo de información. Su tendencia en la actualidad y clasificación obedece a estándares por su naturaleza, entre ellos están: Digitales (Personal-Financiero-legal, y otros); Activos tangibles (Investigación, Estratégicos y comerciales, y otros); Activos intangibles (Conocimiento, Imagen corporativa, Ventaja competitiva, y otros); Software de aplicación (Propietario, Cliente, Gestión de la información, entre otros); Sistemas operativos (Servidores, Ordenadores Dispositivos de red, y otros); Activos físicos (Infraestructura, Controles de entorno, Hardware, Activos de servicios de TI); y los Activos humanos (Empleados, Externos, entre otros).

4.2.5. Ciberseguridad

En la actualidad, se evidencia que los ataques cibernéticos ocasionan daños en los teléfonos móviles, ordenadores y redes informáticas inalámbricas. Para los hackers no existe restricción alguna que permita ingresar en el ciberespacio. Los ciberdelincuentes

conocen las debilidades que existen en la protección de la información para copiar, borrar o pasar a reescribir la información y atacar las redes sociales, gracias a las vulnerabilidades existentes en las estructuras cibernéticas.

4.2.6. Magerit

Esta metodología desarrollada por el Consejo Superior de Administración Electrónica tiene como objetivo examinar, controlar y reducir los riesgos asociados con el uso o implementación de las tecnologías de la información en el ámbito de las instituciones gubernamentales. La importancia de la metodología Magerit radica en su capacidad para identificar y evaluar los riesgos potenciales que podrían afectar la seguridad de la información y la operatividad de los sistemas; facilita el análisis del impacto que los riesgos pueden tener en la organización, sus activos y sus procesos; ayuda a priorizar las acciones necesarias para mitigar o gestionar los riesgos identificados, optimizando así los recursos disponibles y contribuye al cumplimiento de regulaciones y estándares relacionados con la seguridad de la información, lo que es crucial en entornos regulados.

4.2.7. Seguridad de la información

El Consejo Superior de Administración Electrónica ha creado una metodología conocida como Seguridad de la información para analizar y manejar los riesgos que surgen debido a la creciente dependencia de la Administración y de la sociedad en general de las tecnologías de la información para cumplir con las tareas asignadas. También se conoce como un conjunto de prácticas destinadas a mantener los datos seguros del acceso no autorizado o las alteraciones. Aquí hay un amplio vistazo a las políticas, principios y personas utilizadas para proteger los datos.

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

Las iniciales SGSI son un sistema de gestión de seguridad de la información, cuyo origen se encuentra en el idioma inglés. La norma ISO/IEC 27001:2022 define un conjunto de

políticas de gestión de información. En el seno de una empresa donde se lleva a cabo el diseño, ejecución y seguimiento de un conjunto de protocolos con el fin de administrar de manera eficiente el acceso a la información, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

El método usado en SGSI, reduce al mínimo los peligros relacionados con la seguridad de la información en un sistema de administración. La intención es identificar a todas las personas involucradas en el sistema de información empresarial mediante el procedimiento implementado por la organización. El método comentado define las condiciones necesarias para mantener la disponibilidad de la información, garantizar la confidencialidad e integridad.

4.2.9. Proceso en TIC

Es desde la mirada de la SGSI aquel mecanismo transformable de las Tecnologías de la Información y las Comunicaciones (TIC), susceptibles de métodos en conjunto, procesos de producción e instrumentos de relevancia tecnológica, por medio del cual se manejan sobre equipos con programas informáticos, permitiendo integralidad, confiabilidad y fiabilidad procesal. Además, se conjuguen en su contexto, el resguardo y almacenaje de información valiosa para una organización, pero, que a la vez no le sean vulnerados sus códigos.

4.3. MARCO LEGAL

El Marco legal, es aquel apartado metodológico de una investigación, cuya razón es dar a conocer al lector las normas y leyes que son vinculantes con el estudio, y que de alguna manera genera una orientación debida y actualizada de su contenido legal.

4.3.1. Ley 1273 de Delitos informáticos de 2009

En Colombia los diferentes delitos informáticos se sancionan mediante la Ley 1273 de Enero 5 de 2009, sancionada por el Congreso de la República[31]; la cual modifica el Código Penal, crea un nuevo bien jurídico tutelado denominado "protección de la información y datos", preservan integralmente los sistemas que utilicen las TIC, entre otras disposiciones.

En ese sentido, dentro de la Ley 1273, se estipulan 10 delitos informáticos agrupados en dos capítulos que los sancionan reflejados en la tabla 1.

Tabla 1. Delitos informáticos derivados de la Ley 1273.

Capítulo I	**De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.**	
	Artículo 269A:	Acceso abusivo a un sistema informático
	Artículo 269B:	Obstaculización ilegítima de sistema informático o red de telecomunicación.
	Artículo 269C:	Interceptación de datos informáticos.
	Artículo 269D:	Daño Informático.
	Artículo 269E:	Uso de software malicioso.
	Artículo 269F:	Violación de datos personales.

Tabla 2. (continuación)

Capítulo II	Artículo 269G:	Suplantación de sitios web para capturar datos personales.
	Artículo 269H:	Circunstancias de agravación punitiva
	De los atentados informáticos y otras infracciones	
	Artículo 269I:	Hurto por medios informáticos y semejantes

[31] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 2009. nro. 47223. p. 1-4. [Consultado: agosto 22 de 2022]. Disponible en: https://acortar.link/4j40E3.

	Artículo 269J:	Transferencia no consentida de activos.

Fuente: COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 2009. nro. 47223. p. 1-4. [Consultado: febrero 8 de 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Como es de observarse los delitos informáticos explanados en la Ley 1273, son en sí direccionados a tres aspectos básicos, la confidencialidad, la integridad y la disponibilidad, porque los tres convergen en los sistemas informáticos, bien en lo físico, en lo informático o desde la misma web, donde de alguna manera hay una sustracción, daño, modificación, u obstáculo de la información en contra del medio o estructura que la resguarda.

4.3.2. Ley Estatutaria 1581 de 2012.

Esta norma establece las pautas generales para salvaguardar la privacidad de la información personal. El propósito de este derecho es promover el desarrollo del derecho constitucional que permite a todas las personas tener acceso, actualizar y corregir la información que se ha recopilado sobre ellas en bases de datos o archivos. También se protegen otros derechos, libertades y garantías constitucionales mencionadas en el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de dicha Constitución.

Asimismo, Colombia a través del Congreso de la República,[32] sanciona la Ley 1581, según lo expuesto en esta legislación, los principios y regulaciones que se encuentran

[32] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (23, diciembre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales [en línea]. Santa Fe de Bogotá, D.C.: Diario

en esta ley se aplicarán a los datos personales almacenados en cualquier base de datos que puedan ser procesados por entidades tanto públicas como privadas.

4.3.3. Decreto 1377 de 2013

Esta norma Colombiana, fue sancionada por el Congreso de la República, mediante Decreto 1377,[33] la cual genera el reglamento parcial de la Ley 1581 de 2012. Tiene como finalidad regular de manera parcial la Ley 1581 de 2012, la cual establece normas generales para salvaguardar la información personal.

Oficial. Nro. 48587 de octubre 18 de 2012. [Consultado: agosto 16 de 2022]. Disponible en: https://acortar.link/szeUrq.

[33] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1377. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Derogado Parcialmente por el Decreto 1081 de 2015. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. Nro. 48834 del 27 de junio de 2013. [Consultado: agosto 22 de 2022]. Disponible en https://acortar.link/7rg6J9.

5. DISEÑO METODOLÓGICO

El diseño metodológico establece la forma en que se debe recopilar, analizar y presentar la información necesaria para responder a las preguntas de investigación o resolver el problema planteado.

Para el desarrollo del presente documento, se realiza una investigación a profundidad dentro de un marco de referencia como lo es la normatividad ISO 27001:2022; es decir que se conoce la situación actual de la organización la cual se quiere hacer la propuesta, y al mismo tiempo, se aplicará un modelo de investigación de tipo descriptiva. Esta última permite describir los procesos, actividades, recolección de datos y personal de la organización de la unidad de análisis Ortopédica Alca Plus S.A.S.

El proceso metodológico se llevará a efecto mediante el inicio de un análisis y evaluación de las condiciones de aseguramiento de la calidad en cuanto a información manejada en la organización, para así poder diseñar las políticas de la seguridad de la información, esto daría respuesta al primer objetivo específico que es “Evaluar las condiciones del sistema de gestión de seguridad de la información al proceso TIC en la organización Ortopédica Alca Plus SAS, mediante el uso de la norma ISO 27001:2022”. Dicha evaluación se desarrollará para conocer la situación actual de la organización mediante la aplicación de una prueba piloto, que consistirá en un cuestionario dicotómico a las personas encargadas del área de Sistemas y a otros procesos, con el fin de conocer el punto de vista de estas personas frente a la seguridad de la información. Posteriormente para reforzar esta información se aplicará un GAP análisis explanado en la normativa 27001:2022, aplicable a la unidad de análisis Ortopédica Alca Plus, mediante un proceso que permitirá comparar el desempeño real de la organización.

Posteriormente para dar continuidad al proceso metodológico se aplicará en la propuesta la identificarán los activos de información que posee en la actualidad (año 2022) la organización Ortopédica Alca Plus S.A.S. Este apartado dará respuesta al objetivo específico segundo que consiste en: “Categorizar los activos de información del proceso de TIC, a partir de una metodología de gestión de riesgo que permita una valoración de los controles de confidencialidad, integridad y seguridad”.

Luego, y siguiendo los pasos de contracción de la propuesta se daría contextualidad y estructura del diseño de sistema de gestión de la información, según ISO 27001:2022, a partir de la adopción de estándares y un plan de buenas prácticas que permitan el mejoramiento de los niveles de seguridad de los activos de información. El plan de buenas prácticas se generará a partir de la norma ISO/IEC 27002:2022; con el fin de determinar cuáles riesgos se minimizarían respecto a pérdida, robo, daño o modificación de la información existente en la organización Ortopédica Alca Plus S.A.S.

Finalmente, se deberá tener en cuenta que la organización no cuenta con ninguna práctica o modelo de seguridad, el resultado que arrojará el levantamiento de información indicará que se deben elaborar y estructurar todas las políticas correspondientes a cada área. Que luego conjugarían en establecer los requisitos para la elaboración del diseño, la cual se construiría a partir de las políticas adecuadas que garanticen la seguridad de los activos de la información de la organización Ortopédica Alca Plus. S.A.S.

6. DESARROLLO DE LOS OBJETIVOS

El desarrollo de los objetivos es un apartado en la cual describe de qué manera se desarrollan según la metodología planteada y para ello, se expresan los cuatro objetivos específicos, dejando claro que el último es la integralidad de los tres primeros, para orientar la propuesta a dar respuesta al principal u objetivo general. Para el desarrollo de los apartados se darán en el siguiente orden:

a) Condiciones del sistema de gestión de seguridad de la información al proceso TIC en la organización Ortopédica Alca Plus SAS, mediante el uso de la norma ISO 27001:2022(6.1).
b) Activos de información del proceso de TIC, a partir de una metodología de gestión de riesgo que permita una valoración de los controles de confidencialidad, integridad y seguridad (6.2)
c) Diseño de sistema de gestión de la información, según ISO 27001:2022, a partir de la adopción de estándares y buenas prácticas que permitan el mejoramiento de los niveles de seguridad de los activos de información en la organización Ortopédica Alca Plus S.A.S (6.3).

6.1. Condiciones de Seguridad en Ortopédica Alca Plus

Las condiciones de seguridad de la unidad de análisis, se describe a los efectos de dar respuesta a este apartado mediante la aplicación de dos cuestionarios dicotómicos (anexo 1 y 2), como prueba piloto, pero además y para reforzar este contenido se empleará un GAP análisis 27001:2022. Evidentemente con ello se obtiene la información necesaria arrojada por los participantes respecto a evaluar las condiciones de seguridad que presenta la Ortopédica Alca Plus, S.A.S.

En el mismo sentido y para dar claridad y contexto a lo que es un GAP análisis 27001:2022, aplicable a la unidad de análisis Ortopédica Alca Plus, según Laoyan, expresa: “Un análisis de brechas (también conocido como análisis GAP o análisis de

necesidades) es un proceso que se usa para comparar el desempeño real de la empresa con el desempeño deseado. La “brecha” se entiende como el espacio en donde se encuentra tu negocio actualmente y donde te gustaría que esté”.[34] Significa que esta estrategia de recolección de información una vez aplicada como se indica, se hace a través de una lluvia de ideas, arrojando las posibles estrategias, esto de alguna manera permitirá obtener las acciones flameadas en presupuestos al logro de objetivos, mediante la identificación de puntos débiles o vulnerables, para hacer la medición de recursos que posee actualmente, entre otros.

En este entendido la organización Ortopédica Alca Plus S.A.S se dedica a prestar servicios de venta de aparatos ortopédicos, posee diferentes procesos, donde cada empleado tiene un rol definido, de acuerdo a sus habilidades, experiencia y conocimientos, teniendo claridad de las actividades que desempeñan. Ante lo expuesto, y debido a la actividad comercial de la Organización, concede a los empleados el acceso a información confidencial, ocasionando un mayor nivel de riesgo, permitiendo que se genere una mala reputación, mayores pérdidas y un cierre total.

Se observa que otra de las falencias encontradas es la falta de medidas para asegurar los activos, pues no se lleva un control al momento de retirarlos, la facilidad de conexión a los dispositivos informáticos de la entidad, poca seguridad al momento de navegar y descargar diferentes programas, dado que no se cuenta ningún tipo de protección que realice un control en el momento de ingresar a la web.

De igual manera, como resultado observable en el personal de la Organización, se aprecia un alto porcentaje de exposición de la información ante ataques informáticos debido a la falta de conocimiento en temas de seguridad por parte de todos los empleados, falta participación activa del personal en el control de la información, no se cuenta con política de seguridad y gestión de riesgos de seguridad; ello indica la

[34] LAOYAN, Sarah. Cómo implementar el análisis de brechas para alcanzar los objetivos de negocios. [en línea]. Asana en Español. (17 de mayo de 2022). [Consultado: 28 de agosto de 2022]. Disponible en: https://asana.com/es/resources/gap-analysis.

necesidad de poder implementar la metodología Magerit, la cual permite tener diferentes medidas y controles de seguridad, ayudando al cierre de falencias y logrando implementar un modelo de seguridad de la información.

Se deduce que existen vulnerabilidades de los sistemas de seguridad de activos de información, pero que con el fin de conocer éstas, las amenazas y lo riesgos informáticos presentes en la Organización Ortopédica Alca Plus S.A.S, se hace necesario una atención especial al personal que pertenece al proceso de los sistemas y demás áreas como por ejemplo la Gerencia, Contabilidad, Talento Humano y Comercial, entre otras, las cuales conllevan a ser resguardadas y protegidas.

En lo que respecta, al personal que labora en la Organización Ortopédica Alca Plus S.A.S, a continuación, se describen los cargos existentes en el cuadro 1.

Cuadro 1. Personal de Proceso Sistemas

Cargo	Cantidad
Coordinador de Sistemas	1
Ingeniero de Sistemas	1
Técnico de Sistemas	2

Fuente: Elaborado por el autor.

Cuadro 2. Personal de otros Procesos

Cargo	Cantidad
Gerente	1
Contador	1
Jefe de Talento Humano	1
Jefe de Ventas	1

Fuente: Elaborado por el autor.

De acuerdo con las respuestas adquiridas de la prueba piloto, según anexos 3 y 4; así como las visitas e inspecciones a las áreas, se logró conocer la situación de la

Organización frente a la seguridad de la información, teniendo como referencia los controles de la norma ISO/IEC 27001:2022.

- La organización debe diseñar un manual de políticas de seguridad de la información que le permita definir controles de seguridad, limitando el acceso a la información.

- El área de sistemas es el responsable de los protocolos que se deben realizar para tomar todas las medidas necesarias para proteger la información manejada por todas las áreas de la organización.

- La Organización cuenta solamente con una protección básica de antivirus ESET, con una licencia que debe actualizarse anualmente; así mismo se logra identificar que la organización no cuenta con un cronograma que permita conocer el estado del antivirus en los equipos.

- Se evidencia procedimientos documentados, los cuales no han implementado para la realización de los mantenimientos preventivos e instructivos del buen uso de los equipos.

- El personal desconoce la periodicidad con la que se debe actualizar los procedimientos debido a que esa actividad es realizada por el ingeniero encargado del área de sistemas y no es socializada a todo el personal.

- El Gerente se encuentra comprometido como la máxima autoridad con temas relacionados a la tecnología e implementación de controles de seguridad; pero desconoce la importancia de contar con un sistema de gestión de seguridad de la información.

- No se realizan capacitaciones al personal que los oriente en la importancia que tiene la seguridad de la información.

- Se tienen definidos usuarios y roles para el personal dependiendo del área al que pertenezcan; pero se encuentra la falencia de que todos los roles cuentan con los mismos permisos.

- La información se encuentra clasificada en cuatro categorías: confidencial, restringido, uso interno y público; pero evidencia la falta de capacitación al personal para poder clasificarla de manera correcta.

- Se cuenta con un mecanismo de seguridad basado en un usuario y contraseña; pero se observa que las contraseñas no cuentan con los mínimos requisitos de seguridad establecidos.

- El usuario tiene autorización para gestionar la contraseña de ingreso al sistema; lo que genera que la información se encuentre expuesta ataques de cibercriminales.

- La infraestructura de la Organización se encuentra conformada por un servidor que se encarga de administrar la información y protocolos de seguridad, con 10 equipos distribuidos en las diferentes áreas de la organización que se encuentra conectados a través de una red LAN.

- Se realizan mantenimientos correctivos en los equipos dependiendo de la necesidad que se genera en el momento, mas no se cuenta con un mantenimiento preventivo para evitar daños en los equipos.

- La Organización posee un inventario de algunos activos registrado en la contabilidad, pero no tiene un control total de todos ellos.

- Los respaldos son realizados mensualmente, pero solo en los equipos de los jefes de área, lo que conlleva a no tener en su totalidad el respaldo de la información además que el ciclo de respaldo es muy extenso al recomendado.

- Aunque se han detectado varias falencias con respecto a la seguridad de la información la Organización ha contado con la suerte de no presentar ningún tipo incidente de seguridad.

- Dentro de las medidas que implementa la Organización se cuenta con un antivirus, un control de ingreso al servidor y unas copias periódicas a la información.

Según lo evidenciado en las respuestas de los cuestionarios aplicados al personal de Ortopédica Alca Plus S.A.S, la Organización tiene que realizar inversiones en protección de la información, porque los trabajadores carecen de concientización en un tema tan importante como es la seguridad en los datos y los riesgos que conllevan el no tener implementados métodos y procedimientos adecuados para la protección de la información.

Los antes expuesto significa que la Organización en estudio no cuenta con la implementación de políticas de seguridad y asignación de roles y responsabilidades, ello no le permite garantizar la confidencialidad, integridad y disponibilidad de la información, ni minimizar los riesgos que le afecten en su estructura organizacional. Esto da cabida a entender lo importante de aplicar ISO 27001:2022, que en la actualidad presenta 114 controles, a estos efectos se puede indicar los propósitos que derivan de las14 secciones del Anexo A, allí se trabaja lo expuesto en la tabla 2.

Tabla 3. Propósitos de ISO 27001:2022.

Propósito	**Descripción**
Políticas de seguridad Informativa	revisión de políticas
Organización seguridad informativa	responsabilidad, móviles y teletrabajo
Seguridad Recursos Humanos	empleo general
Gestión de recursos	inventario, clasificación y gestión
Control de Acceso	usuario y gestión
Criptografía	gestión de claves
Seguridad física y ambiental	áreas seguras
Seguridad Operacional	gestión de tecnologías

Tabla 4. (continuación)

Seguridad Comunicacional	**seguridad, redes y mensajería**
Adquisición, desarrollo y mantenimiento de Sistemas	seguridad de procesos
Relaciones proveedores	Seguimiento
Gestión Incidencias Seguridad Informativa	eventos y evidencia
Aspectos Seguridad Informativa, gestión negocial	planear, procesar, verificar
Cumplimiento	protección intelectual, datos personales, y revisorías

Fuente: Elaborado por el autor.

Seguidamente se hace un barrido del contenido existente de la Declaración de aplicabilidad de la ISO 27001:2022 para la Organización objeto de estudio, la cual se expresa en los términos de descripción numerales sobre dominio y control, sí aplica o no, como se justifica y la responsabilidad dada, todo de la manera más sintetizada.

Tabla 5. Dominios y controles de la Declaración de la Aplicabilidad.

N°	**Dominio/control**	**Descripción del control**	**Aplica (Si/No)**	**Justificación**	**Responsabilidad**
1	Política para la seguridad de la información	Diseñar manual de políticas seguridad	No	Definir controles de seguridad	Organizar información
2	Seguridad de los recursos humanos	Capacitar personal	No	Importancia de la seguridad	Talento Humano
3	Gestión de activos	Inventariar activos	Si	Contabilidad, control general	Control activos
4	Control de acceso	Actualizar licencia, control de ingreso al servidor	Si	Estado del antivirus en los equipos.	Gestión riesgos
5	Criptografía	Protección básica de antivirus ESET	Si	Proteger la información y ciclo de respaldo	Sistemas control

Tabla 6. (continuación)

6	Seguridad física y del entorno	Roles del personal	Si	Definición usuarios	Seguridad general
7	Seguridad de las operaciones	Mecanismo de seguridad	Si	Usuario y contraseña	Operaciones
8	Seguridad de las comunicaciones	Infraestructura servidor, interconexión red LAN.	No	Información y protocolos de seguridad	Mantener comunicaciones
9	Adquisición desarrollo y manteniendo de sistemas	Instructivos del buen uso de los equipos	Si	Mantenimientos preventivos	Gestionar Administración
10	Relaciones con los proveedores	Periodicidad de procedimientos	Si	Socializada al personal.	Gestionar Administración
11	Gestión de incidentes de seguridad de la información.	Usuario gestiona contraseña	No	Riesgo ataques cibercriminales.	Gestión de riesgo
12	Aspectos de seguridad de la información de la gestión de continuidad de negocio.	Gerente comprometido	No	Sistema de SGSI	Gestión de riesgo
13	Cumplimiento	Mantenimiento correctivos	Si	Mantenimiento preventivo, evita incidente seguridad	Gerencia operaciones

Fuente: Elaborado por el autor.

En vista de lo antes planteado, se procesa tal información mediante el mecanismo gráfico[35], para describir los porcentajes de cumplimiento.

[35] DEJAN, Kosutic. La importancia de la Declaración de aplicabilidad para la norma ISO 27001:2022. [en línea]. Base de conocimientos de ISO 27001:2022 e ISO 22301. (s/f). [Consultado: 10 de diciembre de

Figura 3. Cumplimiento sí o no de las declaratoria de aplicabilidad

Cumplimiento Control	**SI**	**NO**
Diseño de un manual	60	40
Capacitación	60	40
Inventarios activos	80	20
Actualización de licencia	50	50
Protección antivirus	60	40
Roles personal	70	30
Mecanismo seguridad	55	45
Infraestructura servidor	70	30
Instructivos uso	60	40
Periodicidad procedimental	60	40
Gestión de contraseñas	60	40
Gerente está comprometido	60	40
Mantenimiento correctivos	80	20

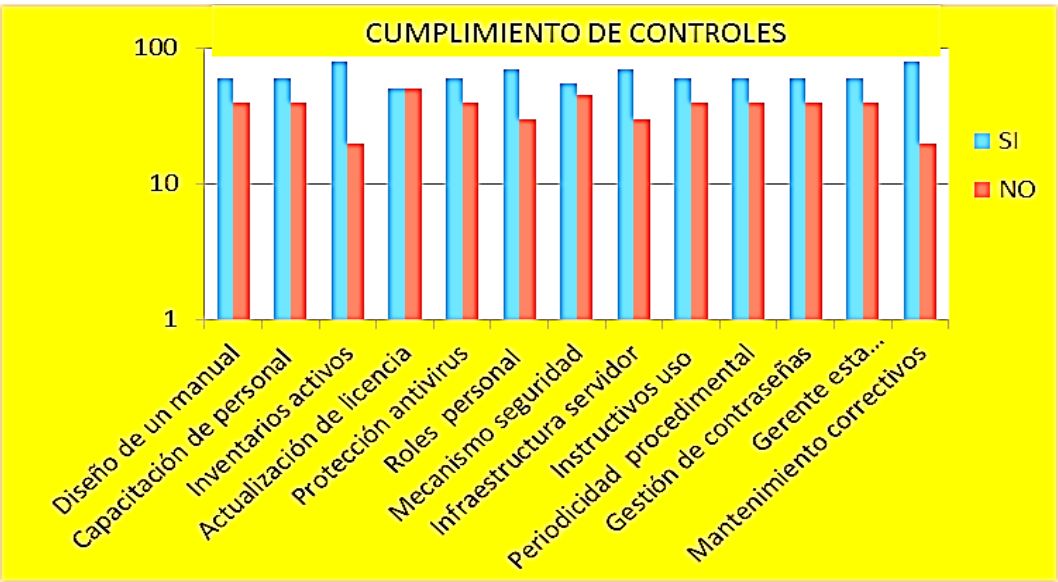
Fuente: Elaborado por el autor.

Como puede observarse, los controles expresados en el gráfico 3 y 4; ambos se agregaron como una imagen, ellos indican, qué tanto porcentaje se da cumplimiento a la aplicabilidad de los controles según ISO 27001:2022, es decir, el renglón “SI” o “NO”, ambos sumados en cada fila dan un porcentaje del 100 por ciento, según se expresan los datos que fueron tomados del análisis y apreciados de los resultados obtenidos y en función a los instrumentos. Entendiendo que la Declaración de aplicabilidad de la ISO 27001:2022 para la Organización objeto de estudio, desarrolla numerales sobre dominio y control, que al sumar la columna del “SI” y divididos por la cantidad de controles, arroja un resultado de cumplimiento en porcentaje del 63,46%, mientras que su complemento en la columna del “NO”, refleja un 36,54%, resultado del sumar verticalmente y dividir entre los controles, para un total del 100%. Indicando desde el análisis cuantitativo que, existe un positivo cumplimiento del SI, pues se podría decir, existe un nivel de bueno,

2022]. Disponible en: https://advisera.com/27001:2022academy/es/knowledgebase/resumen-del-anexo-a-de-la-norma-iso-27001:20222013/.

pero con falencias del 36,54%; la cual debe mejorarse en función a los planes que se innoven para tal fin.

Figura 4. Cumplimiento de los controles y porcentaje del “SÍ” o “NO”.



Fuente: Elaborado por el autor.

Como puede observarse, en las figuras 3 y 4, el cumplimiento del SÍ o NO de los controles según la norma ISO 27001:2022, la Organización Ortopédica Alca Plus S.A.S, se encuentra en la actualidad en un cumplimiento positivo que arroja un resultado del 63, 46%, mientras que lo negativo arroja un resultado del 36,54%. Indica que se debe preparar mecanismo, programas o planes que permitan mejorar tal situación. ¿Por qué aplica un 63,46% positivo?, pues está evidente que la gerencia y la gestión de riesgo se encuentran trabajando en función de mejorar continuamente, pero las falencias existen, y existen por falta de un diseño del sistema de gestión de seguridad de la información que se adapte al proceso de las TIC en la Organización, este instrumento servirá de gran apoyo y baluarte en los términos de la seguridad informática, dando lugar al barrido de las falencias y evidenciar la importancia de que tanto anhela toda estructura gerencial.

6.2. Activos de Información de la Organización Ortopédica Alca Plus S.A.S

Los activos de información de una organización tienen su propia clasificación, que más adelante se realiza a través de un cuadro. Es importante identificar los activos de información más representativos en la organización de acuerdo con la actividad que desempeñan. A continuación, se utilizará la metodología de Magerit, con el fin de conocer los activos de información más relevantes que posee Organización Ortopédica Alca Plus S.A.S.

6.2.1. Identificación de activos críticos de la organización

Como primer paso se debe identificar los activos de información más importantes en la Organización Ortopédica Alca Plus S.A.S:

Tabla 1. Activos de Información de la Organización Ortopédica Alca Plus S.A.S

TIPO	CÓDIGO	NOMBRE DEL ACTIVO	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO
Comunicaciones[C]	[AL001]	Switch	Coordinador de Sistemas	Ingeniero de Sistemas
Datos[D]	[AL002]	Datos de configuración Router NET GEAR	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL003]	Informes de Mantenimiento de equipos	Coordinador de Sistemas	Técnico de Sistemas
	[AL004]	Información personal del Talento Humano de la Organización	Jefe de Talento Humano	Ingeniero de Sistemas
	[AL005]	Repositorio con las Hoja de Vida Proveedores	Contador	Jefe de Ventas
	[AL006]	FTP con Información privilegiada y confidencial de proveedores	Jefe de Ventas	Coordinador de Sistemas

Tabla 1. (continuación)

Hardware[Hw]	[AL007]	Equipo de cómputo Facturación	Jefe de Ventas	Coordinador de Sistemas
	[AL008]	Informática personal pc	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL009]	Canales dedicados de comunicación	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL010]	Firewall	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL011]	Servidor Bases de Datos	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL012]	Teléfonos Oficina	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL013]	Servidor Web	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL014]	Access Point Outdoor (Ubiquiti AP-AC Pro)	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL015]	Periféricos y pendrives	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL016]	Sistema de alimentación Ininterrumpida - UPS	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL017]	Equipos portátiles	Coordinador de Sistemas	Ingeniero de Sistemas
Servicios[S]	[AL018]	Intranet	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL019]	Gestión de identidades	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL020]	Conexión de telefonía	Coordinador de Sistemas	Ingeniero de Sistemas
Software[Sw]	[AL021]	Licencias Antivirus ESET	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL022]	Licencias Windows Server 2016 Essencials	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL023]	Licencia LINUX	Coordinador de Sistemas	Ingeniero de Sistemas

Tabla 1. (continuación)

	[AL024]	Ofimática – office	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL025]	Navegador Web	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL026]	Servidor de Terminales	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL027]	Antivirus	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL028]	Cliente de correo electrónico	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL029]	Sistema operativo Win 10 professional	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL030]	Página Web	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL031]	Transferencia de Archivos	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL032]	Controlador de Dominio	Coordinador de Sistemas	Ingeniero de Sistemas
	[AL033]	Servidor operacional	Coordinador de Sistemas	Ingeniero de Sistemas
Soporte[Media]	[AL034]	Cintas magnéticas para almacenamiento de Backups	Coordinador de Sistemas	Ingeniero de Sistemas

Fuente: Datos suministrados por la administración de la organización Ortopédica Alca Plus S.A.S, 2022.

6.2.2. Dependencia de Activos de Información

En este segundo paso se documenta la dependencia entre los activos de información, determinando como un activo superior influye en otro inferior, generando una amenaza. Dentro de los activos inferiores se encuentran los de comunicaciones, los cuales tiene como fin apoyar los procesos de la organización, pero al fallar estos activos no ocasionan

el cese de las actividades, como a diferencia de los activos superiores que son indispensables para el funcionamiento de los procesos.

Por último, es importante resaltar que los activos de información se encuentran resguardados en las mismas instalaciones de la organización.

Cuadro 3. Dependencia de activos de la organización Ortopédica Alca Plus S.A.S

Tipo	Código	Nombre del activo	[AL001]	[AL002]	[AL003]	[AL004]	[AL005]	[AL006]	[AL007]	[AL008]	[AL009]	[AL010]	[AL011]	[AL012]	[AL013]	[AL014]	[AL015]	[AL016]	[AL017]	[AL018]	[AL019]	[AL020]	[AL021]	[AL022]	[AL023]	[AL024]	[AL025]	[AL026]	[AL027]	[AL028]	[AL029]	[AL030]	[AL031]	[AL032]	[AL033]	[AL034]
COMUNICACIONES[C]	[AL001]	Switch		x					x		x	x	x	x	x	x			x																x	
DATOS[D]	[AL002]	Datos de configuración Router NET GEAR			x														x																	
	[AL003]	Informes de Mantenimiento de equipos							x	x									x																	
	[AL004]	Información personal del Talento Humano de la Organización					x	x																												
	[AL005]	Repositorio con las Hoja de Vida Proveedores				x		x																												
	[AL006]	FTP con Información privilegiada y confidencial de proveedores				x	x																													
HARDWARE[HW]	[AL007]	Equipo de cómputo Facturación																																		
	[AL008]	Informática personal pc																																		
	[AL009]	Canales dedicados de comunicación							x	x			x			x			x			x													
	[AL010]	Firewall	x						x	x		x	x	x	x	x			x	x					x	x	x	x		x	x	x	x	x	x	x
	[AL011]	Servidor Bases de Datos							x	x									x																	
	[AL012]	Teléfonos Oficina																																		
	[AL013]	Servidor Web																		x	x						x			x		x				
	[AL014]	Access Point Outdoor (Ubiquiti AP-AC Pro)							x	x									x																	
	[AL015]	Periféricos y pendrives							x	x									x																	
	[AL016]	Sistema de alimentación Ininterrumpida - UPS							x	x									x																	
	[AL017]	Equipos portátiles																																		
SERVICIOS[S]	[AL018]	Intranet							x	x									x																	
	[AL019]	Gestión de identidades							x	x									x																	
	[AL020]	Conexión de telefonía												x																						
SOFTWARE[SW]	[AL021]	Licencias Antivirus ESET	x						x	x		x	x	x	x	x			x	x					x	x	x	x		x	x	x	x	x	x	x
	[AL022]	Licencias Windows Server 2016 Essencials										x	x										x				x									
	[AL023]	Licencia LINUX											x																							
	[AL024]	Ofimática – office							x	x									x																	
	[AL025]	Navegador Web							x	x									x	x																
	[AL026]	Servidor de Terminales							x	x									x	x																
	[AL027]	Antivirus	x						x	x		x	x	x	x	x			x	x					x	x	x	x		x	x	x	x	x	x	x
	[AL028]	Cliente de correo electrónico															x									x	x	x				x			x
	[AL029]	Sistema operativo Win 10 professional							x	x									x																	
	[AL030]	Página Web							x	x									x																	
	[AL031]	Transferencia de Archivos											x																						x	
	[AL032]	Controlador de Dominio							x	x					x				x								x									
	[AL033]	Servidor operacional	x						x	x	x	x	x		x	x			x	x	x	x							x							
SOPORTE[MEDIA]	[AL034]	Cintas magnéticas para almacenamiento de Backups							x	x									x																	

Fuente: Magerit-versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I-Método, [en línea]. 2016., p.5. [Consultado el 04/08/2016]. Disponible en Internet: https://www.ccn-cert.cni.es/publico/heramienta/pilar5/magerit.

6.2.3. Valoración de los activos

La valoración de riesgo para una determinada organización puede asumirse en estándares dados en Magerit-versión 3.0, el uso de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, en ella se plantea nomenclatura, categoría y la propia valoración.

El siguiente paso a realizar es determinar la valoración de los activos de información que posee la organización, basado en las dimensiones de Autenticidad, Trazabilidad, Confidencialidad, Integridad y Disponibilidad[36].

Cuadro 4. Valoración del Riesgo

VALORACIÓN DEL RIESGO	**NOMENCLATURA**	**CATEGORÍA**	**VALORACIÓN**
	MA	Crítico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Elaborado por el autor.

En el cuadro 4, se explana la nomenclatura, la categoría y la valoración cromática y numérica, de la manera siguiente: La nomenclatura MA, cuya situación categórica es crítica (21 al 25), significa un requerimiento de atención inmediata; la nomenclatura A, es una categoría importante (16 al 20), representa que es grave y con sentido de requerimiento de atención; la nomenclatura M, es una categoría apreciable (10 al 15), expresa que , la cual significa sea objeto de una atención de estudio para su tratamiento; la nomenclatura B, es una categoría Bajo (5 al 9), simboliza que es asumible, cuyo razón

[36] Magerit-versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I-Método, [en línea]. 2016., p.5. [Consultado el 04/08/2016]. Disponible en Internet: https://www.ccn-cert.cni.es/publico/heramienta/pilar5/magerit.

moldea aceptación; la nomenclatura MB, es una categoría despreciable (1 al 4), indica una aceptación del riesgo permanente cuya condición debe tomarse con prudencia y justificación en cuanto al impacto residual asumible.

En general, esto permite la consideración de efectos de daños absolutos potenciales e independientes; mientras que el riesgo supera la probabilidad de ocurrencia; Esto proporcionará información útil para tomar decisiones sobre la protección de activos valiosos contra amenazas y medidas de seguridad valiosas.

En el cuadro 5, se indican los activos de información de Ortopédica Alca Plus S.A.S, la cual se enmarca la valoración, con datos de nombre del activo, el riesgo y los valores cuantitativos de la autenticidad, trazabilidad, confidencialidad, integridad y la disponibilidad, terminando en la columna del valor.

Cuadro 5. Valoración de los activos de información de Ortopédica Alca Plus S.A.S

NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDA	INTEGRIDAD	DISPONIBILIDAD	VALOR
[MEDIA]Cintas magnéticas para almacenamiento de Backups	APRECIABLE	9	9	25	9	25	15
[SW]Licencias Antivirus AVG	IMPORTANTE	9	9	25	25	25	19
[D]Datos de configuración Router NET GEAR	IMPORTANTE	9	9	25	25	25	19
[D]Informes de Mantenimiento de equipos	APRECIABLE	9	25	9	25	9	15
[SW]Licencias Windows Server 2016 Essencials	IMPORTANTE	9	9	25	25	25	19
[SW]Licencia LINUX	IMPORTANTE	9	9	25	25	25	19
[D]Información personal del Talento Humano de la Organización	APRECIABLE	9	9	25	25	9	15
[HW]Equipo de cómputo Facturación	APRECIABLE	9	9	25	9	25	15
[S]Intranet	CRITICO	25	25	25	25	9	22
[SW]Ofimática – office	IMPORTANTE	9	9	25	25	25	19

Cuadro 6. (continuación)

[HW] Informática personal pc	IMPORTANTE	9	9	25	20	25	18
[SW] Navegador Web	IMPORTANTE	9	9	25	25	25	19
[SW] Servidor de Terminales	APRECIABLE	9	9	25	9	25	15
[SW] Antivirus	IMPORTANTE	9	9	25	25	25	19
[SW] Cliente de correo electrónico	IMPORTANTE	9	9	20	20	20	16
[SW] Sistema operativo Win 10 professional	APRECIABLE	9	9	25	9	25	15
[S]Gestión de identidades	IMPORTANTE	9	9	20	20	20	16
[S]Conexión de telefonía	BAJO	9	9	9	9	9	9
[HW] Canales dedicados de comunicación	CRITICO	25	25	25	25	25	25
[SW]Página Web	APRECIABLE	15	9	9	9	15	11
[HW] Firewall	CRITICO	25	25	25	25	25	25
[HW] Servidor Bases de Datos	CRITICO	25	25	25	25	25	25
[HW] Teléfonos Oficina	BAJO	9	9	9	9	9	9
[HW] Servidor Web	CRITICO	25	25	25	25	25	25
[HW] Access Point Outdoor (Ubiquiti AP-AC Pro)	IMPORTANTE	9	9	25	25	25	19
[D] Repositorio con las Hoja de Vida Proveedores	APRECIABLE	9	9	25	9	25	15
[D] FTP con Información privilegiada y confidencial de proveedores	APRECIABLE	9	9	25	25	9	15
[HW]Periféricos y pendrives	IMPORTANTE	9	9	20	20	20	16
[C]Switches	IMPORTANTE	9	9	20	20	20	16
[SW]Transferencia de Archivos	CRITICO	20	20	25	25	25	23
[SW]Controlador de Dominio	IMPORTANTE	9	9	20	20	20	16
[HW]Sistema de alimentación Ininterrumpida – UPS	APRECIABLE	9	9	15	9	15	11
[HW]Equipos portátiles	APRECIABLE	9	9	20	9	20	13
[SW]Servidor operacional	IMPORTANTE	9	9	25	25	25	19

Fuente: Elaborado por el autor.

Se observa que los activos de información de Ortopédica Alca Plus S.A.S, se enmarcan en una valoración, que va de un riesgo crítico (25), a un riesgo bajo (9) [37].

[37] Magerit-versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I-Método, [en línea]. 2016., p.5. [Consultado el 04/08/2016]. Disponible en Internet: https://www.ccn-cert.cni.es/publico/heramienta/pilar5/magerit.

Estos valores cuantitativos de autenticidad, trazabilidad, confidencialidad, integridad y la disponibilidad, terminando en la columna del valor, calculados mediante la sumatoria de los riesgos y divididos en la cantidad de cinco (5) que son los concurrentes.

6.2.4. Identificación de amenazas

En este punto se realiza la identificación y valoración de las amenazas, teniendo en cuenta el catálogo de amenazas que presenta Magerit versión 3.

Cuadro 7. Catálogo de amenazas

CATEGORÍA	DESCRIPCIÓN
[N]	Desastres Naturales
[I]	De origen Industrial
[E]	Errores y fallos no intencionados
[A]	Ataques Intencionados

Fuente: Elaborado por el autor.

A continuación, se identifican las amenazas más relevantes que pueden afectar los activos de información de Ortopédica Alca Plus:

Cuadro 8. Identificación de amenazas para cada activo

TIPO	NOMBRE DEL ACTIVO	AMENAZAS
COMUNICACIONES[C]	Switch	[I8] Fallo de servicios de comunicaciones
DATOS[D]	Datos de configuración Router NET GEAR	[E2] Errores del administrador [E4] Errores de configuración
	Informes de Mantenimiento de equipos	[A3] Manipulación de los registros de actividad (log) [A15] Modificación deliberada de la información
	Información personal del Talento Humano de la Organización	[E19] Fugas de información [A11] Acceso no autorizado

Cuadro 9. (continuación)

	Repositorio con las Hoja de Vida Proveedores	[E18] Destrucción de información [E19] Fugas de información
	FTP con Información privilegiada y confidencial de proveedores	[A11] Acceso no autorizado [A19] Divulgación de información
HARDWARE[HW]	Equipo de cómputo Facturación	[A25] Robo [N2] Daños por agua
	Informática personal pc	[A25] Robo [E23] Errores de mantenimiento / actualización de equipos (hardware)
	Canales dedicados de comunicación	[E20] Vulnerabilidades de los programas (software)
	Firewall	[E19] Fugas de información
	Servidor Bases de Datos	[E2] Errores del administrador
	Teléfonos Oficina	[I.9] Interrupción de otros servicios y suministros esenciales
	Servidor Web	[E2] Errores del administrador
	Access Point Outdoor (Ubiquiti AP-AC Pro)	[I5] Avería de origen físico o lógico [A11] Acceso no autorizado
	Periféricos y pendrives	[I5] Avería de origen físico o lógico
	Sistema de alimentación Ininterrumpida – UPS	[I6] Corte del suministro eléctrico
	Equipos portátiles	[A11] Acceso no autorizado
SERVICIOS[S]	Intranet	[A13] Repudio [A5] Suplantación de la identidad del usuario
	Gestión de identidades	[A5] Suplantación de la identidad del usuario [E2] Errores del administrador [A11] Acceso no autorizado
	Conexión de telefonía	[A7] Uso no previsto
SOFTWARE[SW]	Licencias Antivirus ESET	[E21] Errores de mantenimiento / actualización de programas (software) [A11] Acceso no autorizado

Cuadro 10. (continuación)

	Licencias Windows Server 2016 Essencials	[E20] Vulnerabilidades de los programas (software) [A7] Uso no previsto
	Licencia LINUX	[A11] Acceso no autorizado [A6] Abuso de privilegios de acceso
	Ofimática – office	[E8] Difusión de software dañino [E1] Errores de los usuarios
	Navegador Web	[A11] Acceso no autorizado [I.9] Interrupción de otros servicios y suministros esenciales [E.24] Caída del sistema por agotamiento de recursos
	Servidor de Terminales	[A11] Acceso no autorizado [E19] Fugas de información
	Antivirus	[A10] Alteración de secuencia [E2] Errores del administrador [A4] Manipulación de la configuración
	Cliente de correo electrónico	[E28] Indisponibilidad del personal [A30] Ingeniería social (picaresca) [A] Ataques intencionados
	Sistema operativo Win 10 professional	[A23] Manipulación de los equipos [E23] Errores de mantenimiento
	Transferencia de Archivos	[E15] Alteración accidental de la información
	Controlador de Dominio	[A8] Difusión de software dañino
	Servidor operacional	[A18] Destrucción de información
SOPORTE[MEDIA]	Cintas magnéticas para almacenamiento de Backups	[I7] Condiciones inadecuadas de temperatura o humedad [E25] Pérdida de equipos

Fuente: Elaborado por el autor.

6.2.5. Identificación de Vulnerabilidades

La vulnerabilidad es considerada como la debilidad que tiene un activo y que puede ser utilizada por la amenaza para causar daño o materializarse.

A continuación, se relaciona las vulnerabilidades por cada amenaza frente a cada activo de información de la organización:

Cuadro 11. Identificación de Vulnerabilidades para cada activo

Nombre del activo	**Amenazas**	**Vulnerabilidades**
Switch	[I8] Fallo de servicios de comunicaciones	No permite una comunicación estable entre los equipos
Datos de configuración Router NET GEAR	[E2] Errores del administrador	Acceso al equipo por falta de control con los accesos de preconfigurados de fabrica
	[E4] Errores de configuración	Contraseña administrador en poder de varios usuarios
Informes de Mantenimiento de equipos	[A3] Manipulación de los registros de actividad (log)	Falta de control de cambios en los registros de la ejecución de la actividad
	[A15] Modificación deliberada de la información	Registro con información falsa de la ejecución de la actividad
Información personal del Talento Humano de la Organización	[E19] Fugas de información	Falta de políticas de envío seguro de información
	[A11] Acceso no autorizado	Falta de aplicación de políticas de control de acceso
Repositorio con las Hoja de Vida Proveedores	[E18] Destrucción de información	Si los permisos no están bien definidos y no son granulares, se corre el riesgo que se altere o elimine la información accidentalmente
	[E19] Fugas de información	Si no se tiene políticas de prevención de fuga de información, ésta se puede filtrar y conllevaría a perdidas monetarias o de clientes a la empresa

Cuadro 12. (continuación)

FTP con Información privilegiada y confidencial de proveedores	[A11] Acceso no autorizado	No se evidencia Matriz de roles y permisos, se puede presentar accesos no autorizados a información sensible
	[A19] Divulgación de información	Si un atacante accede a esta información podría divulgarla, trayendo consigo no solo mala reputación a la organización, también problemas legales.
Equipo de cómputo Facturación	[A25] Robo	Falta de establecimiento de controles de acceso a zonas no autorizadas
	[N2] Daños por agua	Alimentación en puesto de trabajo que puede implicar derramamiento de líquidos sobre el equipo
Informática personal pc	[A25] Robo	Sustracción de equipos por falta de barreras perimetrales adecuadas entre la oficina y el exterior
	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento
Canales dedicados de comunicación	[E20] Vulnerabilidades de los programas (software)	Caída de internet
Firewall	[E19] Fugas de información	Fallo al filtrado de información.
Servidor Bases de Datos	[E2] Errores del administrador	Fallos al ingresar o tratar de acceder al servidor
Teléfonos Oficina	[I.9] Interrupción de otros servicios y suministros esenciales	Caída de internet o fallos eléctricos
Servidor Web	[E2] Errores del administrador	Fallos al ingresar o tratar de acceder al servidor
Access Point Outdoor (Ubiquiti AP-AC Pro)	[I5] Avería de origen físico o lógico	Sobretensión eléctrica por el no uso de protectores de picos de voltajes o productos deficientes.

Cuadro 13. (continuación)

	[A11] Acceso no autorizado	Posibilidad de ingreso no autorizado a la red si se utiliza claves de cifrado inferiores a WPA3 o sin la suficiente robustez
Periféricos y pendrives	[I5] Avería de origen físico o lógico	Fallas de energía en las instalaciones
Sistema de alimentación Ininterrumpida – UPS	[I6] Corte del suministro eléctrico	Fallas en el fluido eléctrico
Equipos portátiles	[A11] Acceso no autorizado	Acceso al equipo por falta de control con los accesos preconfigurados de fabrica
Intranet	[A13] Repudio	Falta de actualización de roles y privilegios por cambio de funciones
	[A5] Suplantación de la identidad del usuario	Falta de sistemas de doble autenticación
Gestión de identidades	[A5] Suplantación de la identidad del usuario	Abuso de privilegios de acceso
	[E2] Errores del administrador	Fallas de configuración que permite exposición de datos
	[A11] Acceso no autorizado	No se cuenta con control de acceso – Claves
Conexión de telefonía	[A7] Uso no previsto	Fallo por caída de internet o al tratar de ingresar a la conexión
Licencias Antivirus ESET	[E21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización
	[A11] Acceso no autorizado	Falta de control en la asignación de permisos a usuarios
Licencias Windows Server 2016 Essencials	[E20] Vulnerabilidades de los programas (software)	Falta de ejecución de actualizaciones
	[A7] Uso no previsto	Falta de controles en el acceso a funcionalidades del sistema
Licencia LINUX	[A11] Acceso no autorizado	Contraseña de usuario root débil

Cuadro 14. (continuación)

	[A6] Abuso de privilegios de acceso	Posibilidad de ejecutar comandos de borrado de información en directorios del sistema
Ofimática – office	[E8] Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
	[E1] Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc
Navegador Web	[A11] Acceso no autorizado	No se cuenta con control de acceso – Claves
	[I.9] Interrupción de otros servicios y suministros esenciales	Caída de Internet
	[E.24] Caída del sistema por agotamiento de recursos	Carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
Servidor de Terminales	[A11] Acceso no autorizado	No se cuenta con control de acceso o monitoreo para ingreso al dominio.
	[E19] Fugas de información	Manejo no adecuado de información por clasificación deficiente
Antivirus	[A10] Alteración de secuencia	No estar al día con las actualizaciones
	[E2] Errores del administrador	Antivirus sin seguimiento a las actualizaciones y estado
	[A4] Manipulación de la configuración	Desinstalación de programa e instalación de otro
Cliente de correo electrónico	[E28] Indisponibilidad del personal	Ausencia de personal que realiza el mantenimiento por enfermedad por enfermedad, vacaciones o actividades personales
	[A30] Ingeniería social (picaresca)	Manipulación de empleados por personas con intención de cometer fraude, extorsión o estafa
	[A] Ataques intencionados	Ataque destructivo - Ocupación enemiga

Cuadro 15. (continuación)

Sistema operativo Win 10 professional	[A23] Manipulación de los equipos	Bloqueo por parte de usuario final evitando la instalación de actualizaciones
	[E23] Errores de mantenimiento	Falta de mantenimiento de equipos servidores o mantenimiento realizado por personal sin la competencia adecuada
Transferencia de Archivos	[E15] Alteración accidental de la información	Alteración y eliminación de información por personal no autorizada
Controlador de Dominio	[A8] Difusión de software dañino	Se accede a información infectada o se puede compartir.
Servidor operacional	[A18] Destrucción de información	Se genera un daño global de información en el sistema.
Cintas magnéticas para almacenamiento de Backups	[I7] Condiciones inadecuadas de temperatura o humedad	Falta de sistema de control de temperatura y humedad en las instalaciones de almacenamiento
	[E25] Pérdida de equipos	Falta de registro de inventario de cintas

Fuente: Elaborado por el autor.

6.2.6. Controles y salvaguardas de los activos

Luego de conocer las amenazas y vulnerabilidades existentes en los activos de información de la organización Ortopédica Alca Plus S.A.S, se procede a verificar los controles o salvaguardas para proteger la información[38]:

[38] Magerit-versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I-Método, [en línea]. 2016., p.5. [Consultado el 04/08/2016]. Disponible en Internet: https://www.ccn-cert.cni.es/publico/heramienta/pilar5/magerit.

Cuadro 16. Controles identificados y el dominio pertinente con la ISO 27001:2022.

CONTROLES IDENTIFICADOS	**DOMINIOS ISO 27001:2022**
Deberían definirse claramente las responsabilidades. Incluye la asignación de responsables de los activos de información.	5. Política de seguridad.
Diseño e implementación de procedimientos relacionados al etiquetado de la información, teniendo en cuenta el esquema de clasificación de información adoptado por la organización.	5. Política de seguridad.
Identificar, documentar y revisar regularmente los requisitos para los acuerdos de privacidad o no socialización que muestren las necesidades de la organización para proteger la información.	5. Política de seguridad.
La gerencia debe apoyar activamente en la seguridad dentro de la entidad a través de direcciones claras demostrando compromiso, asignaciones explícitas y reconocimiento de las responsabilidades de la seguridad de la información.	5. Política de seguridad.
La información se debe organizar en función del valor, criticidad, susceptibilidad a ser divulgado o a modificación no autorizada y a los requisitos legales.	5. Política de seguridad.
Las herramientas de registro y los registros de información deben estar protegidos contra la manipulación y acceso no autorizado.	5. Política de seguridad.
Los procedimientos y las responsabilidades de la gerencia deben ser establecidos para lograr una efectiva, rápida y organizada respuesta a los percances que ocurran en la protección de la información.	5. Política de seguridad.
La asignación de contraseñas debe controlarse a través de un proceso de gestión formal. Las contraseñas temporales se deben entregar a los usuarios de forma segura. Se debe evitar el uso de mensajes electrónicos desprotegidos (texto sin cifrar). Las contraseñas nunca deben ser almacenadas en sistemas informáticos de forma desprotegida	6. Aspectos organizativos de la seguridad de la información
Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.	6. Aspectos organizativos de la seguridad de la información

Cuadro 9. (continuación)

Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	6. Aspectos organizativos de la seguridad de la información
La documentación de los sistemas debe estar protegido contra el acceso no autorizado.	7. Gestión de activos.
Los datos de prueba deben ser seleccionados cuidadosamente, así como protegidos y controlados.	7. Gestión de activos.
Todos los activos deben estar claramente identificados y clasificados en un inventario de acuerdo a su importancia. El inventario debe ser actualizado constantemente.	7. Gestión de activos.
Creación de Privilegios y perfiles de seguridad, que permitan identificar de manera exclusiva al personal teniendo en cuenta el cargo desempeñado	8. Seguridad ligada a los recursos humanos.
Todos los empleados de la entidad independiente de su contratación deben recibir capacitaciones en cuanto al trabajo que desempeñan, con el fin de apropiarse de conocimientos y actualizarse en políticas y procedimientos organizacionales.	8. Seguridad ligada a los recursos humanos.
Perímetros de seguridad (barreras como: paredes, entradas con uso de tarjetas) deben ser usadas para proteger áreas que contienen información y proteger instalaciones que procesan información.	9. Seguridad física y del entorno.
La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.	10. Gestión de comunicaciones y operaciones.
La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes de la entidad con roles relevantes y funciones de trabajo.	10. Gestión de comunicaciones y operaciones.
Las áreas seguras deben estar protegidas apropiadamente por controles que garanticen el acceso de personal autorizado	11. Control de acceso.
Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	11. Control de acceso.
Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.	12. Adquisición, desarrollo y mantenimiento de sistemas de Información.

Cuadro 9. (continuación)

Deberían existir procedimientos para controlar la instalación del software en sistemas operacionales.	13. Gestión de incidentes en la seguridad de la información.
Se deberían proteger los accesos a las herramientas de auditoría de sistemas con el fin de prever cualquier posible mal uso o daño.	13. Gestión de incidentes en la seguridad de la información.
Toda la información y los activos asociados con el proceso de información deben poseer un propietario en la entidad.	15. Cumplimiento.

Fuente: Elaborado por el autor.

Con base en lo anterior se puede validar que se hizo una identificación de los activos de información presentes en la organización Ortopédica Alca Plus S.A.S, donde se valoró los activos dependiendo del nivel de riesgo, se determinó las posibles amenazas y vulnerabilidades y se definió los controles para salvaguardas los activos que posee la empresa.

6.3. Políticas de Seguridad de Información que permitan Diseñar un SGSI basados en la ISO 27001:2022.

Antes de señalar la propuesta al diseño de SGSI adaptado a ISO 27001:2022, enmarcado en las políticas de seguridad como estándares a una necesidad de la implementación de SGSI, se plantea el ciclo PHVA. Este último es aquel cuyo propósito se enmarca en los SGSI, abordados por las directivas institucionales, quienes implementan la participación de todos los empleados, asegurando la implementación de las medidas de seguridad y salud laboral, la mejora del comportamiento, las condiciones y el medio ambiente, y el control efectivo sobre los riesgos en el lugar de trabajo y las vulnerabilidades, mediante el mecanismo de Planear, Hacer, Verificar y Accionar.

Por ello, un diseño de SGSI adaptado a ISO 27001:2022, enmarca el ciclo PHVA, donde Planear, es el principio básico que mejora la seguridad y la salud de los empleados, debe encontrar las cosas que han salido mal o que pueden corregirse y proponer ideas para resolver estos problemas, a través de cronogramas a corto, mediano o largo plazo; el

Hacer, plantea la acción planeada debe llevarse a cabo; la Verificación, deberá realizarse mediante una revisión de los procedimientos y acciones implantas para conseguir los resultados deseados; la Acción, conlleva a que se deben tomar las acciones correctivas para obtener el máximo beneficio en la seguridad y salud ocupacional de los empleados. En resumen, el ciclo del PHVA involucra las políticas de seguridad que se centran en la importancia de establecer los aspectos clave relacionados con el quién, qué, por qué, cuándo y cómo en la implementación del SGSI.

De esta manera, considerando la relevancia de que la organización identifique las demandas de sus diferentes grupos involucrados, y la evaluación de los mecanismos adecuados para preservar la seguridad de la data, es requerido establecer una política que tome en consideración los lineamientos generales de funcionamiento de la organización, sus objetivos institucionales, sus procesos esenciales, y que se adecue a las particularidades y condiciones individuales de cada una para que sea aprobada y supervisada por la dirección.

Así en un sistema de gestión de seguridad de la información, su diseño establece la importancia de una política clara y concisa desde la perspectiva de la dirección y la organización. Esta política debe ser de fácil lectura y comprensión, flexible y cumplible para todas las personas involucradas, sin ninguna excepción. Las políticas se establecen en función del tiempo, pudiendo ser de corta duración y basadas en los principios que dirigen las acciones dentro de la empresa para desarrollar un plan de prácticas adecuadas, las cuales se detallan en la siguiente sección.

6.3.1 El plan de buenas prácticas desde la perspectiva de la norma ISO/IEC 27002:2022.

El plan se basa en definir las actividades a ejecutar para mejorar la seguridad de la información en las empresas, generando procesos seguros en cuanto al resguardo de la información, mejorando el control de activos de información, orientado hacia la correcta

implementación de políticas de control y logrando con ello una mejor organización en los procesos.

6.3.1.1 Alcance

El plan de buenas prácticas definido para la Ortopedia Alca Plus. S.A.S, conlleva en la praxis, la tamización de cada uno de los elementos intrínsecos y extrínsecos orientados hacia la visión y misión, a los fines de lograr la eficiencia y eficacia de la gestión, mediante el contexto de cumplimiento de la Norma ISO/IEC 27002:2022. Este plan se fijará sobre las medidas de control de la información, la cual tendrá el resguardo en todos los elementos organizacionales en la complementariedad de las Políticas de Seguridad de Información que permitan el diseño del SGSI basados en la ISO 27001:2022.

6.3.1.2 Objetivos

a). Definir en las cláusulas de Control de accesos, Seguridad física y ambiental, Seguridad en la operativa y Seguridad en las telecomunicaciones, que permean los controles según la ISO 27002:2022.

b). Señalar las categorías de seguridad referidas a los controles según ISO 27002:2022 del área de sistemas para la eficiencia en la información.

c). Establecer las Políticas de Seguridad de Información que permitan el diseño del SGSI basados en la ISO 27001:2022.

6.3.1.3 Cronograma de actividades claramente definidas

- **Cronograma de actividades**

El presenta Cronograma describe las actividades a seguir en un tiempo determinado de forma trimestral y el funcionario o persona responsable de hacer cumplir tal actividad.

Actividades	Tiempo por trimestre año 2023				
	1er	2do	3ro	4to	Responsable
Creación de Políticas basadas en el análisis de los riesgos según los controles según la ISO 27002:2013					Coordinador de Sistemas
Sensibilización organizacional en actividades generadas para cada Departamento					Jefe de Talento Humano
Implementación de recursos tecnológicos desde el área de sistemas de los controles para la eficiencia en la información.					Ingeniero de Sistemas

Fuente: el autor

6.3.2. Desarrollo e los objetivos del plan de buenas prácticas

6.3.2.1. Definir en las Cláusulas de Control de accesos, Seguridad física y ambiental, Seguridad en la operativa y Seguridad en las telecomunicaciones, que permean los controles según la ISO 27002:2022.

Una vez realizado el análisis de las actividades basadas en los riesgos, se procede a revisar los controles según la ISO 27002:2022, los cuales servirá como base para definir un plan de buenas prácticas que debe implementar Ortopédica Alca Plus. S.A.S. Es importante considerar que, de acuerdo al organigrama de la organización, el área de sistemas es el encargado de implementar los controles para la eficiencia en la información. En el anexo 5 se muestra los controles a implementar de acuerdo al tipo de activo que posee la organización.

A continuación, se describen las clausulas sobre los controles de ISO 27002:2022.

a). Clausula Control de accesos: Las medidas de control de acceso están encaminadas a la seguridad de la información mediante políticas que la organización debe definir en la gestión de procesos según el acceso de los usuarios y los requisitos que sean necesarios, responsabilidad del usuario y los parámetros de protección y autenticación de la información en las aplicaciones del sistema. Los roles en un sistema de información

se agregan a los roles intermedios utilizando las dimensiones de liberación, cambio, revocación y determinación del usuario de acuerdo con los permisos asignados por el nivel de confianza relacionado con la seguridad de la información. La importancia es causada por los indicadores de identidad y aprobación de la red y el servicio.

b). Clausula Seguridad física y ambiental: Los estándares de seguridad física y ambiental definen reglas para evitar el acceso no autorizado, la destrucción y la intrusión en los sistemas de información de una organización. En otras palabras, los estándares deben permitir que solo el personal autorizado deba ingresar a las áreas de acceso restringido y crear las condiciones ambientales necesarias para que los componentes del sistema informático funcionen correctamente. En una organización como la Ortopédica Alca Plus. S.A.S., el objetivo principal de la seguridad física es proteger los sistemas informáticos, y los estándares creados para tal fin.

c). Clausula Seguridad en la operatividad: La seguridad operativa bajo la gestión organizacional es un procedimiento de gestión de cambios constantes que respaldan y protegen los registros y la información, en particular la información confidencial, que se gestiona para este propósito a través de un programa de monitoreo de la capacidad de los recursos. Una gestión de cambios para la Ortopédica Alca Plus. S.A.S, asegura la funcionalidad de los sistemas de información, mayor soporte organizacional por ser confidencial; para mantener las operaciones se debe identificar a los usuarios privilegiados y regular los altos riesgos en las operaciones del día a día a medida que introducen vulnerabilidades técnicas, por lo que esto se hace utilizando herramientas de prevención de pérdida de datos.

d). Clausula Seguridad en las telecomunicaciones: La seguridad de las telecomunicaciones se logra a través de procedimientos de control de los servicios de la red interna y mecanismos de seguridad asociados con las redes externas vulnerables. Para ello, se desarrollan requisitos técnicos basados en el nivel de servicio del personal de telecomunicaciones y de los proveedores de servicios. Asimismo, la Ortopédica Alca Plus. S.A.S, en su funcionabilidad deberá generar lineamientos de comunicación

relacionados con los servicios de llamadas como hosting, acceso a la red WAN, acceso a Internet y por supuesto definir protocolos de confidencialidad e intercambio de comunicaciones con terceros.

6.3.2.2. Señalar las categorías de seguridad referidas a los controles según ISO 27002:2013 del área de sistemas para la eficiencia en la información.

Las Categorías de Seguridad referidas a los controles según ISO 27002:2022 del área de sistemas para la eficiencia en la información, se plantean desde varios indicadores como los son:

a) Requisitos de negocio para el control de acceso.
b) Gestión de acceso de usuario.
c) Control de acceso a Sistemas y Aplicaciones.
d) Áreas seguras.
e) Seguridad de los equipos.
f) Copias de seguridad
g) Registro de actividad y supervisión
h) Consideraciones de las Auditorías de los Sistemas de Información.
i) Gestión en la seguridad de redes.
j) Intercambio de información con partes externas.

Como puede observarse, las categorías “indicador a hasta la d”, pertenecen a la Cláusula control de acceso; mientras que las categorías desde el “indicador e hasta la f”, pertenece a la Cláusula Seguridad física y ambiental. Luego, el “indicador g hasta el h”, pertenecen a la Cláusula Seguridad en la operatividad; finalmente las categorías desde el “indicador i hasta la j”, se expresan en la Cláusula de la Seguridad en las telecomunicaciones.

A continuación se presentan las categorías de seguridad referidos a la adecuada aplicación de los controles[39] dentro de un plan de buenas prácticas.

Cuadro 17. Aplicación de controles según ISO 27002:2022

Clausula	**Categoría de Seguridad**	**Nombre Control**	**Objetivos Aplicables A Ortopédica Alca Plus**	**Activo**
Control de accesos	Requisitos de negocio para el control de acceso	Control de acceso a las redes y servicios asociados	Establecer una política para el control en el acceso de la red a los usuarios de acuerdo a las funciones asignadas.	Intranet Conexión de telefonía Controlador de Dominio
	Gestión de acceso de usuario.	Gestión de altas/bajas en el registro de Usuarios	Aplicar los controles pertinentes para dar de alta y baja a los usuarios que tiene acceso a los tipos de información que maneja la organización	Access Point Outdoor Licencia LINUX Licencias Antivirus ESET Licencias Windows Server 2016 Essencials
		Retirada o adaptación de los derechos de acceso	Aplicar controles cuando los empleados terminen su contrato o servicio, para el retiro de los derechos en el acceso a los sistemas o instalaciones para el resguardo de la información.	Gestión de identidades Canales dedicados de comunicación
	Control de acceso a Sistemas y Aplicaciones	Restricción del acceso a la información	Establecer una política para restringir el acceso a los usuarios de acuerdo a la información que maneja y a las funciones que desempeña dentro de la organización.	Datos de configuración Equipos portátiles Firewall
		Gestión de contraseñas de usuario	Proporcionar a los empleados las contraseñas para acceder a Windows; posteriormente el empleado podrá cambiar la contraseña para su protección.	Informática personal pc (Ubiquiti AP-AC Pro) Router NET GEAR
Seguridad física y ambiental	Áreas seguras	Seguridad de oficinas y recursos	Diseñar y ejecutar un sistema de seguridad física a las instalaciones de la empresa.	Teléfonos Oficina Equipo de cómputo

[39] Controles ISO 27002-2013. Bogotá. Colombia; [Consultado: 2 de diciembre de 2022]. Disponible en: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf.

Cuadro 18. (continuación)

	Seguridad de los equipos	Instalaciones de suministro	Proteger los equipos de cortes de energía e interrupciones generadas por fallas en los suministros con la ayuda de un sistema de alimentación ininterrumpida, la cual permite mantener la continuidad de energía al equipo por un determinado tiempo para guardar y apagarlos de forma correcta.	Informes de Mantenimiento Navegador Web Ofimática – office Periféricos y pendrives Switch
		Seguridad en el cableado	Proteger contra interferencia o posibles daños los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información dentro de la organización.	Servidor operacional Repositorio con las Hoja de Vida Proveedores FTP con Información privilegiada y confidencial de proveedores de equipos
		Mantenimiento de los equipos	Realizar una vez al mes mantenimiento preventivo a los equipos, con el fin de garantizar su adecuado funcionamiento.	Informes de Mantenimiento Antivirus Facturación
		Control de salida de activos	Realizar el retiro o salida de los equipos con previa autorización de la Gerencia y el Coordinador de Sistemas.	Información personal del Talento Humano de la Organización
		Equipo informático de usuario desatendido	Velar por los equipos informáticos ante usuarios que no trabajan dentro de las instalaciones por parte del responsable del área de Sistemas, tener medios de almacenamiento cifrados, software para protección de la información, que eviten que la información se accedida por personas no autorizadas.	Cintas magnéticas para almacenamiento de Backups
		Política de puesto de Trabajo despejado y bloqueo de pantalla	Adoptar una política de puesto de Trabajo despejado para asegurarse que, en el momento de ausentarse de su área de trabajo, escritorios libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores. Documentación y medios de Almacenamiento extraíbles.	Información personal del Talento Humano de la Organización

Cuadro 19. (continuación)

Seguridad en la operativa	Copias de Seguridad	Copias de seguridad de la información	Proporcionar los mecanismos necesarios que garanticen la protección de la información ante algún desastre o falla de medios de almacenamiento.	Ininterrumpida – UPS
	Registro de actividad y supervisión	Registro y gestión de eventos de actividad	Realizar monitoreo permanente del uso de los recursos de la plataforma tecnológica y los sistemas de información por parte del empleo terceras partes permitidas de personal adscrito	Transferencia de Archivos
	Consideraciones de las Auditorias de los Sistemas De Información	Controles de auditoría de los sistemas de información.	Implementar las auditorias necesarias para verificar los sistemas operacionales; con la finalidad de no interrumpir los procesos de negocio.	Sistema de alimentación Sistema operativo Win 10 professional
Seguridad en las telecomunicaciones	Gestión en la seguridad de redes	Controles de red	Diseñar una política respecto al uso de redes, donde solo los empleados sean responsables del área puedan manejarlo.	Servidor Bases de Datos Servidor de Terminales Servidor Web
	Intercambio de información con partes externas.	Políticas y procedimientos de Intercambio de información	Dar seguridad y protección a la información cuando sea transferida o cambiada con otras organizaciones u otro destino externo y se debe establecer que los procedimientos y controles sean necesarios para el intercambio de información.	Transferencia de Archivos
		Mensajería electrónica	Establecer controles adecuados para impedir la pérdida de información archivada en los correos electrónicos.	Cliente de correo electrónico
		Acuerdos de confidencialidad y secreto	Fijar controles donde se mantenga el acceso de la información solo al personal autorizado según corresponda.	Gestión de identidades

Fuente: Elaborado por el autor.

6.3.2.3. Establecer las Políticas de Seguridad de Información que permitan el diseño del SGSI basados en la ISO 27001:2022.

A) Política General de Seguridad de la Información.

La organización Ortopédica Alca Plus S.A.S tiene el compromiso de proteger la información importante almacenada. Para lograrlo, se enfoca en mantener la confidencialidad, integridad y disponibilidad de los activos de información, así como en garantizar la continuidad de las operaciones. También se encarga de administrar y gestionar los riesgos, y de promover una cultura de seguridad entre los empleados, contratistas, proveedores y cualquier persona que utilice los activos de información la sociedad mercantil. Es importante recordar que todos los colaboradores y personas que interactúen con el Sistema de información son responsables de cumplir con esta política para que sea efectiva.

La información pertenece a la organización Ortopédica Alca Plus S.A.S, por lo cual las personas encargadas de manejar y cuidar la información generada por los procesos organizacionales tienen la responsabilidad de su tenencia y uso adecuado. Es importante que los empleados sean conscientes de los posibles peligros que podrían poner en riesgo la información que manejan. Se afirma que la política será evaluada cada año o en caso de detectarse cambios en la organización o situaciones que puedan afectarla, con el fin de garantizar su idoneidad y conformidad con los requisitos establecidos.

Objetivo.

Definir las medidas de seguridad y protección adecuada para la información generada por los diferentes procesos de la organización Ortopédica Alca Plus S.A.S, evitando la posibilidad de pérdida de información por diversas amenazas potenciales.

Alcance.

Estas políticas se aplican a cada uno de los procesos organizacionales y a todos los datos generados por los distintos activos de información de información de la organización Ortopédica Alca Plus S.A.S.

Criterios.

- Debe verificar que las políticas de seguridad de la información estén definidas, implementadas, revisadas y actualizadas.
- Reporte de eventos contra la infraestructura tecnológica y de seguridad de la información de la organización Ortopédica Alca Plus S.A.S.
- Todos los usuarios de los sistemas de información tienen la responsabilidad y la obligación de seguir las políticas, normas, procedimientos y mejores prácticas de seguridad de la información descritas en este manual.
- Permiso para realizar los controles de seguridad de la información correspondientes.
- Toda aplicación o software de cómputo debe ser adquirido o aprobado por la Administración de Sistemas de Información para verificar la funcionalidad, el cumplimiento de los requisitos legales, y los requisitos de infraestructura tecnológica admisibles, actualización y operación optimizada.
- La organización de Ortopédica Alca Plus S.A.S debe contar con un firewall que limite los ataques externos, permitiendo el ingreso únicamente a los usuarios autorizados.
- Se requiere una VPN (Red Privada Virtual) que permita el acceso externo seguro a las aplicaciones de los Sistemas de Información.
- Los gerentes, directores y coordinadores deben asegurarse de que todos los procesos de seguridad de la información se implementen y sigan correctamente.
- Las políticas de seguridad de la información serán revisadas una vez al año con el objetivo de mejorar continuamente la confidencialidad, confidencialidad, integridad y disponibilidad de los procesos de información.
- Solo se permite software autorizado comprado por una organización legítima o software libre.

- Todos los gerentes de la organización de Ortopedia Alca Plus S.A.S son responsables de reportar incidentes de seguridad, eventos sospechosos y uso indebido de los medios que identifiquen.
- La organización Ortopédica Alca Plus S.A.S contará con un plan de continuidad del negocio para asegurar la continuidad de las operaciones, en caso de imprevistos o desastres naturales.
- Cada empleado es responsable de mantener la confidencialidad, integridad y disponibilidad de los activos de información de acuerdo con esta política y las políticas y procedimientos de seguridad de la información inherentes

B) Política de Control de Acceso

Objetivo.

Proporcionar la seguridad razonable de los sistemas y recursos de información, a través de la gestión y el mantenimiento adecuados de las cuentas de usuario, y los derechos y privilegios relacionados, para acceder a servidores, aplicaciones, bases de datos, archivos organizacionales e instalaciones de procesamiento de datos.

Alcance.

Esta política aplica a todos los sistemas de información, bases de datos, equipos de informáticos, configuraciones y redes que la organización Ortopédica Alca Plus S.A.S tiene actualmente o tendrá en el futuro

Criterios.

- Tomar nota de la llegada y salida de los miembros del equipo en el departamento de procesamiento de datos.
- La Coordinación de Informática decide qué tareas se le asignarán a cada miembro del equipo según su posición, para tener un control sobre quién tiene acceso al sistema de información.
- Los operadores solo pueden adquirir datos a los que expresamente el propietario del activo les haya otorgado autorización.

- Cuando un empleado se retira de su cargo en la organización, se requiere que el jefe directo revise los archivos almacenados en las computadoras. Esta revisión se realiza para facilitar una reasignación formal y oportuna de las obligaciones y responsabilidades.
- Los empleados de la empresa Ortopédica Alca Plus S.A.S no pueden emplear herramientas para recabar datos de la red, tales como la identificación de puertos, servicios y archivos pertenecientes a la organización.
- Las claves no deben ser registradas o guardadas en áreas que puedan ser vistas fácilmente o en lugares cercanos a los sistemas de información que permiten su acceso.
- El empleado tiene la responsabilidad de utilizar correctamente las contraseñas asignadas para acceder a los sistemas de información; estas contraseñas y nombres de usuario son individuales y no pueden ser compartidos.
- La Coordinación de Informática será responsable de determinar la manera en que se registrarán, cancelarán y revisarán periódicamente los permisos de acceso a los sistemas de información asignados a los empleados. Estas acciones se llevarán a cabo en base a los cambios que puedan ocurrir en las áreas de trabajo, siempre y cuando se haya notificado previamente a la coordinación de Gestión Humana.
- Es necesario que los empleados de la organización firmen un acuerdo de confidencialidad que salvaguarde la información confidencial de la empresa antes de permitirles trabajar de forma remota.
- Es fundamental mantener un control riguroso sobre el acceso a los puertos de comunicaciones. Todos los Usuarios que necesiten establecer una conexión interna o externa deben obtener el consentimiento de la Dirección de sistema de información o la coordinación de informática.
- La Dirección de Sistemas de Información tiene la responsabilidad de mantener registros precisos y actualizados de todos los medios de comunicación utilizados para el intercambio de datos abiertos.
- Cualquier conexión en línea en la que el Usuario haya realizado tres intentos de identificación y contraseña incorrectos, debe ser desconectada de inmediato.

C) Política de Acceso a Redes y Servicios de Red

Objetivo.

Garantizar el acceso de forma segura y controlada a los servicios de red implementados en la organización Ortopédica Alca Plus.

Alcance.

Esta política aplica a la organización Ortopédica Alca Plus, en todos los servicios de red con los que cuenta.

Criterios.

- La implementación de herramientas por parte de la Coordinación de Informática buscará prevenir la descarga de software no autorizado y/o código malicioso en los dispositivos institucionales.
- A los empleados de la empresa Ortopédica Alca Plus S.A.S no se les permite utilizar redes sociales durante su horario de trabajo.
- Es importante que la descarga de archivos de Internet se realice con fines laborales y de manera sensata, para evitar perjudicar el servicio.
- Es necesario utilizar redes VPN seguras proporcionadas por la empresa Ortopédica Alca Plus S.A.S para acceder de forma remota a la red de la organización.
- Es necesario que la información guardada en las carpetas de los servidores de archivos sea de índole institucional.
- No está permitido guardar datos que no estén relacionados con las responsabilidades del usuario, información personal, canciones, vídeos, películas o cualquier archivo que pueda causar peligros informáticos, como programas o códigos dañinos.
- Queda terminantemente prohibido obtener, difundir o hacer pública información almacenada en los servidores de archivos o estaciones de trabajo, a menos que se cuente con la autorización explícita del propietario de dichos activos. • Para conectar los equipos de cómputo de la organización Ortopédica Alca Plus S.A.S., los usuarios deberán utilizar los puntos de red de datos.

- La Coordinación de Informática de la empresa Ortopédica Alca Plus S.A.S. es la encargada de llevar a cabo la gestión de los puntos de red de datos.
- Los impresos deben ser de índole institucional.
- Para imprimir, es necesario utilizar documentos de naturaleza institucional.
- Si algún problema surge con una impresora, no se debe permitir que los usuarios realicen tareas de reparación o mantenimiento. En lugar de eso, deben reportar cualquier falla a la Coordinación de Informática de Ortopédica Alca Plus S.A.S.
- Es responsabilidad de los usuarios del correo electrónico de la empresa evitar cualquier acción o conducta que represente una amenaza para la seguridad de la información.
- Se recomienda utilizar el correo electrónico exclusivamente para llevar a cabo las responsabilidades propias de la función y no para ningún otro propósito. El envío de correos con contenido que perjudique la integridad y reputación de las personas y la entidad no está permitido.
- La responsabilidad del contenido del mensaje y de cualquier información adjunta recae en cada usuario.
- Cada usuario tiene la responsabilidad de abrir y revisar los mensajes de origen desconocido, y se hace responsable de las consecuencias derivadas de la ejecución de cualquier archivo adjunto. En estas situaciones, es importante no responder a los mensajes, no abrir los archivos adjuntos y, en su lugar, se debe comunicar a la Coordinación de Informática de la empresa Ortopédica Alca Plus S.A.S.

D). Política de Escritorio y Pantalla Limpios

Objetivo.

Definir una política de responsabilidad compartida donde implique la implementación de prácticas adecuadas de organización y limpieza en el lugar de trabajo, junto con políticas de seguridad de la información que se enfoquen en un manejo eficiente y responsable de los activos de la organización hacia el logro de un ambiente seguro y propicio para la innovación y el progreso.

Alcance.

Esta Política, aplica a todos los colaboradores de la organización Ortopédica Alca Plus S.A.S, que cuenten con un espacio de trabajo asignado, un ordenador y se encarguen de manejar documentos físicos y/o digitales, donde se garantice la debida protección de la información y los sistemas, tanto interna como externamente.

Criterios.

- Los equipos que interactúen con personas ajenas a la organización deben ser colocados de forma que se evite la exposición de la pantalla.
- No se permite tener en el escritorio sustancias o líquidos que puedan causar daños a los equipos y documentos.
- Se tomarán fotografías al escritorio del funcionario que haya infringido las normas, en las cuales se observen cuadernos, documentos impresos, carpetas, monitores encendidos y cualquier otro objeto que vaya en contra de esta política. Estas imágenes servirán como respaldo para las acciones correctivas y/o administrativas que se determinen.
- La documentación y pruebas recopiladas sobre el incumplimiento de la política serán proporcionadas a la supervisión de control interno, quienes se encargarán de tomar las medidas correctivas necesarias.
- Se requiere que todos los dispositivos informáticos utilizados por el personal de la empresa Ortopédica Alca Plus S.A.S se ajusten de manera que su pantalla se bloquee automáticamente después de 20 minutos de inactividad.
- Es imprescindible que todos los equipos informáticos cuenten con un protector de pantalla, cuya configuración será determinada por la Dirección de Sistemas de Información.
- Es necesario que todos los equipos informáticos de la empresa Ortopédica Alca Plus S.A.S cuenten con un usuario y una contraseña para poder acceder al sistema operativo.
- Es importante evitar que cualquier persona pueda tener acceso a dispositivos de almacenamiento de información como USB, CD, DVD, Discos Duros Externos, entre otros.

- Es necesario que todos los empleados de la organización bloqueen sus equipos cuando no estén en sus puestos de trabajo. Esto se logra utilizando las opciones de cierre de sesión de Windows o los comandos de bloqueo como Control + Alt + Supr o la tecla de Windows + L.
- Se requiere que los empleados que utilicen los equipos de cómputo de la empresa Ortopédica Alca Plus S.A.S, los apaguen al finalizar su jornada laboral.
- A partir del momento en que se le proporciona y asigna un equipo de cómputo, el funcionario es plenamente responsable de su estado.
- No está permitido adherir calcomanías en las pantallas.
- El usuario debe asegurarse de mantener su equipo limpio por fuera.
- Asegurarse de que la puerta de la oficina esté cerrada con llave cuando no haya personal presente durante largos periodos de tiempo.
- Es obligatorio que todos los equipos de la empresa tengan como fondo la imagen de la organización Ortopédica Alca Plus S.A.S.
- Se permite que los equipos de informáticos y áreas de trabajo sean sometidos a revisiones y auditorías por parte de las áreas de control designadas por la entidad con el objetivo de verificar el cumplimiento de esta política.
- Cada funcionario tiene la responsabilidad de proteger los sistemas de información bajo su cuidado. Por lo tanto, es importante que aseguren su computadora portátil físicamente en todo momento utilizando cables de seguridad, con el fin de evitar posibles robos.

E). Política de Uso de los Activos

Objetivo.

Alcanzar y mantener la seguridad de los activos de información a través de la asignación de responsabilidades y tareas.

Alcance.

Esta política aplica a todos los procesos organizativos que puedan interactuar con el Sistema de información de la organización Ortopédica Alca Plus S.A.S.

Criterios.

- Los activos de información utilizada en la organización Ortopédica Alca Plus S.A.S es propiedad de esta y solo debe ser utilizada para fines laborales.
- Los empleados están obligados a usar exclusivamente los programas y equipos autorizados por la Gerencia y la Dirección de Sistemas de Información.
- La organización Ortopédica Alca Plus S.A.S será responsable de proporcionar a sus empleados los equipos informáticos y los programas instalados en ellos. Los datos e información creados, almacenados y recibidos en dichos equipos serán propiedad exclusiva de la organización Ortopédica Alca Plus S.A.S.
- Los empleados únicamente podrán realizar copias de seguridad de sus archivos personales o de información pública. Para copiar cualquier tipo de información clasificada o reservada, se requerirá el permiso del supervisor directo, según las normas establecidas para clasificar la información de acuerdo con los niveles de seguridad. El robo, la apropiación, el daño intencional o el uso indebido de la información para fines distintos a las actividades propios de la institución se considerarán infracciones sujetas a las sanciones establecidas por las leyes vigentes.
- De manera regular, la Coordinación de Informática llevará a cabo la evaluación del software empleados en cada área de la organización. Si descargas, instalas o utilizas aplicaciones o programas informáticos sin autorización, estarás incumpliendo las Políticas de Seguridad de la empresa.
- Es obligatorio que los Jefes, Directores y Coordinadores soliciten a la Dirección de Sistema de Información todos los requerimientos de aplicativos, sistemas y equipos informáticos.
- La Coordinación de Informática se encargará de mantener bajo su responsabilidad los medios magnéticos o electrónicos, como CDs u otros, que se entregan junto con el software, así como los manuales y las licencias de uso correspondientes. Además, se guardarán las claves necesarias para descargar el software desde los sitios web de los fabricantes, así como los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.
- No se debe permitir que los funcionarios cometan deliberadamente acciones que involucren la mala utilización de los recursos tecnológicos o que vayan en contra de

las políticas de seguridad de la información. Algunos ejemplos de esto podrían ser el envío o reenvío masivo de correos electrónicos o spam, jugar juegos en línea durante el horario laboral, utilizar constantemente las redes sociales personales, conectar periféricos o equipos que generen molestias a los colegas de trabajo, y similares.

- Los empleados no podrán llevar a cabo ninguno de las siguientes tareas sin contar con la autorización previa de la Dirección de Sistemas de Información.
- Puedes colocar programas en cualquier dispositivo
- Descargar programas o aplicaciones de Internet o de cualquier otro servicio en línea en cualquier dispositivo.
- Alterar, examinar, convertir o ajustar cualquier programa informático perteneciente a la organización.
- Queda prohibida la des compilación o realización de ingeniería inversa en cualquier software de propiedad de la organización.
- Hacer duplicados o difundir cualquier software que sea de propiedad de la institución.
- Modificar la configuración del hardware perteneciente a la entidad. n
- La persona encargada deberá asumir la responsabilidad por todas las transacciones o acciones realizadas utilizando su cuenta de usuario.
- Se prohíbe a cualquier empleado utilizar cuentas de usuario o contraseñas de otros trabajadores para acceder a la red o servicios TIC de la Organización Ortopédica Alca Plus S.A.S.
- Los empleados no tienen permiso para utilizar redes externas mediante sus dispositivos personales mientras se encuentren en las instalaciones de la organización Ortopédica Alca Plus S.A.S., como, por ejemplo, módems USB, Routers o wifi público. Esta situación pone en riesgo la seguridad de los recursos informáticos de la empresa.
- El área encargada de informática tiene la responsabilidad de garantizar el control de los accesos a internet, redes externas y redes internas de la entidad. Esto implica evitar que personas no autorizadas tengan acceso a los recursos informáticos y prevenir la entrada y expansión de virus.
- Es importante respaldar regularmente la información de la organización Ortopédica Alca Plus S.A.S y almacenarla de manera segura en lugares apropiados, para

asegurar su recuperación en caso de desastres o problemas con los equipos de procesamiento.

- En el proceso de separación laboral, los empleados deberán entregar todos los bienes físicos y/o electrónicos que les haya asignado la empresa Ortopédica Alca Plus S.A.S.

F). Política de Protección Contra Códigos Maliciosos

Objetivo.

Contar con una plataforma de hardware y software que garantice la seguridad y disponibilidad de la información y del software que la utiliza, bien en red interna de la organización Ortopédica Alca Plus S.A.S, para protegerse contra amenazas informáticas como malware, troyanos u otros virus que puedan comprometer la seguridad y disponibilidad de la información almacenada en los servidores, estaciones de trabajo y cualquier otro dispositivo de almacenamiento.

Alcance.

Aplica a todo tipo de proceso organizacional que produzca información de cualquier tipo.

Criterios.

- Medidas de seguridad contra software maligno.
- Es fundamental adoptar las medidas de seguridad correspondientes para resguardar la red interna de la empresa Ortopédica Alca Plus S.A.S, evitando, identificando y solucionando problemas ocasionados por software dañino como virus en las computadoras y servidores, troyanos, gusanos en la red y bombas lógicas.
- Es importante considerar la sensibilización de los usuarios respecto a las medidas de seguridad contra software malicioso que posee la empresa, así como garantizar los adecuados accesos a sistemas y el control de modificaciones.
- No se debe instalar software no autorizado.
- Es necesario contar con la autorización previa de la coordinación de informática antes de descargar cualquier software o aplicación de Internet.

- La organización Ortopédica Alca Plus S.A.S debe contar con una plataforma de antivirus, tanto en hardware como en software, en su red de servidores y computadoras para prevenir la difusión de virus mediante archivos externos adquiridos de otras redes.

La plataforma de Antivirus deberá cumplir con los siguientes requerimientos:

- Sistema de gestión centralizado.
- Mantener una constante y centralizada actualización de los DAT mediante un proceso automatizado.
- Implementación de la distribución automática de actualizaciones en las estaciones de trabajo.
- Monitoreo centralizado.
- Se ha comprobado un elevado nivel de detección.
- Mínimo efecto en la rapidez de respuesta de las estaciones.
- Salvaguardar la integridad de todos los equipos y servidores pertenecientes a la red de la empresa Ortopédica Alca Plus S.A.S.
- Posee la capacidad de ejecutarse en las diversas plataformas presentes en la organización, como Windows, Linux y otras opciones.
- Sistema de alerta integrado para detectar y controlar la propagación de virus.
- En caso de requerir consulta a terceros, se proporciona apoyo centralizado de la herramienta. Apoyo presencial y/o telefónico para asistencia técnica y contratos de apoyo.
- Se debe proporcionar información acerca de cada equipo que cuente con la herramienta instalada, como su dirección IP, procesador, sistema operativo, capacidad de almacenamiento, memoria RAM, entre otros datos relevantes.
- Para prevenir la propagación de virus, es necesario llevar a cabo una revisión regular de los equipos informáticos en busca de amenazas. Se recomienda hacerlo en silencio.
- Cada día se deberá llevar a cabo una evaluación del rendimiento del sistema antivirus. En caso de que surja un problema con virus en algún equipo informático

deberá seguirse un procedimiento de recuperación de ataques de virus y código malicioso.

- La coordinación de informática deberá estar suscrita a los boletines de alerta tanto del fabricante como del proveedor del antivirus, así como de los principales fabricantes de antivirus en el mercado, para determinar y seguir las recomendaciones de terceros en caso de ataques o vulnerabilidades, también para diferenciar y determinar los diversos riesgos o falsos virus.
- La herramienta de Antivirus que se implemente en la organización tendrá carácter de corporativo y por ende será obligatoria su instalación y uso en todo el equipamiento computacional sean estos servidores, estaciones de trabajo, notebook y otros dispositivos. Cualquier equipo que no cuente con esta protección de antivirus, no podrá ser conectado a la red de datos local de la institución.
- Se requiere que el antivirus se instale en un ordenador con requisitos mínimos para su funcionamiento, y es responsabilidad de la coordinación informática verificar que el equipo cumpla con estas condiciones. Si el dispositivo no es compatible, el equipo no podrá acceder a la red de datos.
- El ajuste de la configuración del antivirus variará según los servicios que brinde el equipo, siendo responsabilidad de la coordinación de informática determinar la opción más adecuada.
- Mientras el antivirus tiene la tarea de emitir alertas sobre posibles infecciones, si son los propios usuarios quienes notan estas alertas en sus dispositivos, deben comunicarlo de inmediato a la coordinación de informática a través de una llamada telefónica o por correo electrónico.

G). Política Para Ejecutar Copias de Seguridad

Objetivo.

Garantizar la información institucional de la entidad siempre disponible, protegida y confidencial a través de la adecuada administración de las copias de seguridad y su recuperación cuando sea necesario, como necesidad de periodicidad, confidencialidad, integridad y disponibilidad adecuada de los datos cuando sea necesaria.

Alcance.

Esta política se implementa en relación a todos los datos producidos dentro de la organización.

Criterios.

- Las áreas de supervisión, gestión y organización necesitan pedir a la unidad de tecnología de la información que les proporcione espacio en el servidor para guardar la información.
- Después de reservar el espacio en el servidor, es necesario establecer un nombre de usuario y una contraseña, así como determinar qué usuarios tendrán acceso y podrán editar la información.
- Las copias de respaldo se llevarán a cabo regularmente considerando la importancia de los datos. Estas copias se guardarán en el servidor de la empresa Ortopédica Alca Plus S.A.S.
- Asegurar que los medios sean resguardados y almacenados en una institución ajena a la empresa Ortopédica Alca Plus S.A.S., donde la información esté protegida y mantenga su integridad.
- Asegurar que los medios sean custodiados y guardados en una entidad externa a la organización Ortopédica Alca Plus S.A.S., donde se garantice la seguridad y la integridad de la información.
- Para requerir un duplicado de datos ya sea por cuestión de consulta o por extravío, el superior, líder o responsable solicitará al área de tecnología de la información mediante el documento determinado para este propósito.
- No está permitido guardar en los servidores de la Empresa datos personales o información no autorizada legalmente, siguiendo las leyes de derechos de autor aplicables.
- La sección de informática supervisa de manera periódica los registros de seguimiento y sucesos de las herramientas, junto con los procedimientos de las copias de seguridad llevadas a cabo. Si se detecta alguna alarma o se tiene alguna sospecha acerca de la calidad del respaldo, es necesario volver a realizarlo y dar seguimiento para corregir cualquier problema encontrado.}

- Para evitar complicaciones en la ejecución del procedimiento, es recomendable programar los respaldos durante la noche.
- A fin de evitar inconvenientes, es preferible programar los respaldos en horario nocturno.
- Es conveniente programar los backups durante la noche para evitar interrupciones en el proceso.
- Asegurar la ejecución exitosa de los respaldos implica programarlos en horario nocturno.
- Se recomienda planificar los backups durante la noche con el objetivo de evitar contratiempos en su realización.

H). Política Para la Transferencia de Información

Objetivo.

Proteger la información transferida al interior de la organización Ortopédica Alca Plus S.A.S.

Alcance.

Aplica para toda la información interna y externa

Criterios.

- El objetivo de la organización es compartir información con entidades gubernamentales y privadas, de acuerdo a las necesidades de la entidad, con el fin de automatizar servicios y mejorar la gestión de la empresa Ortopédica Alca Plus S.A.S.
- La entidad realizará convenios de transmisión de datos tras la petición a la dirección de tecnología de la información.
- La transmisión de datos debe ser establecida mediante un acuerdo interadministrativo o contractual, el proceso de transferencia debe llevarse a cabo según lo estipulado en el Manual de Contratación.

- La comunicación interna dentro de la organización se llevará a cabo utilizando los canales oficiales de transmisión de datos.
- Se utilizarán los medios de comunicación oficiales para transferir la información dentro de la organización.
- La transmisión de información dentro de la empresa se realizará a través de los medios de comunicación autorizados.
- Se utilizarán los canales de comunicación oficiales para transmitir información dentro de la organización.
- La transmisión de datos en un soporte físico se llevará a cabo siguiendo las directrices establecidas por la organización en el Programa de Administración de Documentos.
- El movimiento de datos digitales
- El traslado de información digital
- El intercambio de datos digitales
- La transmisión de datos digitales
- La comunicación de información digital
- El área de informática llevará a cabo la instalación de herramientas seguras para transferir información dentro de la entidad.
- La unidad de informática debe poner en marcha los recursos adecuados para garantizar que la información se trasmita de forma segura dentro y fuera de la organización Ortopédica Alca Plus S.A.S, evitando su interceptación, copia, alteración, enrute incorrecto y destrucción.
- La coordinación de informática tiene la responsabilidad de supervisar las operaciones para redirigir automáticamente el correo electrónico a direcciones externas de correo.
- El departamento de informática supervisará el uso de servicios de transferencia de archivos ajenos mediante la herramienta FTP.

l). Política de Seguridad Para Relación con Proveedores

Objetivo.

Garantizar la información que se produce entre la organización Ortopédica Alca Plus S.A.S y los proveedores.

Alcance.

Esta política aplica para la información que se genera entre la organización Ortopédica Alca Plus S.A.S Y los diferentes proveedores.

Criterios.

- No revelar los términos y condiciones de contratación a personas ajenas a la parte involucrada.
- Realizar las labores de negocio considerando las directrices de software definidas por la empresa Ortopédica Alca Plus S.A.S.
- Cualquier información generada entre la empresa Ortopédica Alca Plus S.A.S y sus distintos proveedores debe ser verídica.
- Proporcionar datos de la empresa Ortopédica Alca Plus S.A.S únicamente cuando sea necesario.

J). Política de Tratamiento de Datos Personales

Objetivo.

Garantizar que la empresa Ortopédica Alca Plus S.A.S se comporte como el encargado de proteger sus datos personales y los utilizará exclusivamente con los propósitos permitidos.

Alcance.

Esta política aplica para la información que maneja Ortopédica Alca Plus S.A.S respecto a sus miembros, empleados y proveedores.

Criterios.

Modo en que se utiliza la información.

Previa autorización del titular de los datos personales le permitirá a la organización Ortopédica Alca Plus S.A.S dar el siguiente tratamiento:

- Con el objetivo de los trámites administrativos internos de la entidad.
- Identificar y describir a los ciudadanos y grupos de interés, así como desarrollar estrategias para mejorar la forma en que se presta el servicio.

- Proporcionar atención y soluciones a las solicitudes, quejas, reclamaciones, denuncias y sugerencias presentadas a la empresa.
- Nutrir el Sistema de Información
- Obtener y revisar la información del sujeto del dato almacenada en archivos de entidades tanto públicas como privadas.
- Realizar sondeos anticipados de la satisfacción y la percepción de los grupos de valor
- Transmitiendo datos relevantes para el público en general.

Derechos de los titulares de los datos personales.

La organización Ortopédica Alca Plus S.A.S se compromete a asegurar que el titular de los datos personales pueda hacer uso completo de los derechos que se mencionan a continuación:

- Obtener, mantener al día y corregir su información personal. La posibilidad de ejercer este derecho también se aplica a los datos que sean parciales, inexactos, incompletos, divididos, engañosos o que estén siendo tratados sin la debida autorización o en contra de su prohibición expresa.
- Se requiere obtener evidencia de la autorización concedida a la compañía Ortopédica Alca Plus S.A.S para realizar el manejo de información personal.
- Obtener información sobre cómo se utilizan y tratan sus datos personales, al presentar una solicitud a través de los canales de atención al cliente.
- Realizar denuncias ante la Superintendencia de Industria y Comercio sobre violaciones a lo establecido en la legislación y otras regulaciones que la cambien, añadan o completen.
- Anular la autorización y/o pedir la eliminación de uno o más datos si el tratamiento no cumple con los principios, derechos y garantías constitucionales y legales. La revocación o eliminación se llevará a cabo en los casos en los que la Superintendencia de Industria y Comercio determine que se han cometido acciones que vulneran la ley y la Constitución en el manejo de los datos.
- Tener acceso gratuito a la información personal que haya sido procesada.

Se sugiere llevar a cabo la implementación de las políticas de seguridad de la información, las cuales deben contar con la aprobación de la alta dirección y el comité de seguridad. Esto permitirá vigilar su cumplimiento y determinar si es necesario revisarlas y actualizarlas.

6.3.3. Importancia del SGSI en la organización Ortopédica Alca Plus S.A.S

En este recorrido de las políticas de la entidad objeto de estudio, se puede llegar a determinar qué importancia del SGSI en la organización Ortopédica Alca Plus S.A.S, proviene de los *stakeholders* (grupos de trabajo), de la evaluación del marco de control requerido para la seguridad de la información.

La prueba final debe tener en cuenta la política, el marco general en el que opera la empresa, sus fines institucionales, su proceso y, sobre todo, la adecuación de las condiciones particulares y particulares de cada persona autorizada y dirigida por el directorio.

En relación a esto, hay una serie de directrices concretas que permiten poner en práctica y utilizar elementos en cualquier área de actividad. En lo que respecta a la seguridad de la información, estas políticas se manifiestan como estrategias que la organización implementará de manera correcta mediante los requisitos estipulados por las autoridades.

Finalmente, se establecen los lineamientos que resaltan la importancia de implementar un Sistema basado en la Seguridad de la Información, donde se incluyen: velar por las medidas de salvaguardas indispensables para custodiar y dar garantías de la seguridad de los datos del proceso; implementar la seguridad correspondiente en relación a los recursos de información y sistemas; asegurando el acceso controlado y seguro a los servicios definidos en la red; contemplando una política de responsabilidad compartida para fomentar condiciones laborales óptimas; lograr y mantener los activos de información seguros, asignando roles específicos; disponer de un sistema de software y

hardware que resguarde la disponibilidad e integridad de la información; logrando la seguridad y privacidad de la información institucional mediante los mecanismos apropiados; proteger la información transmitida dentro de la empresa; asegurar la información generada en colaboración con los proveedores; y finalmente, asegurar que los datos personales de los empleados evaluados sean debidamente registrados.

CONCLUSIONES

Para evaluar las condiciones de aseguramiento de la información en la organización Ortopédica Alca Plus SAS, se aplicó dos tipos de cuestionarios, uno dirigido específicamente al área de sistemas y otro a los demás procesos que conforma la organización, donde arrojó como resultados que la organización debe hacer una inversión en la protección de la información, pues no tiene implementado procedimiento, política y método que le permitan resguardar la información, quedando la información vulnerable a robos y pérdidas; así como la falta de conocimiento que tienen los empleados en cuanto a seguridad de la información, pues no tienen definidas sus roles y responsabilidades frente a este tema de suma importancia para la organización.

Para reconocer los activos de información que posee la organización Ortopédica Alca Plus SAS se utilizó la metodología Magerit, donde inicialmente se identificó treinta y cuatro (34) activos críticos que tiene la organización de acuerdo a su clasificación, luego se realizó la valoración de los activos basados en las dimensiones de autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad, permitiendo identificar las amenazas, vulnerabilidades y controles que se deben tener para la protección de la información.

Con el fin de controlar y salvaguardar los activos de la organización, se propone inicialmente controlar el acceso a la información, la cual debe estar resguardada por el área de Sistemas, donde se restrinja el uso a todo el personal y se habilite el acceso a los empleados dependiente de las funciones que desempeña en la organización; se debe asignar contraseña a los equipos; contar con un sistema de alimentación ininterrumpida (UPS) para proteger los equipos de cortes de luz y otras fallas que se generen; realizar mantenimientos preventivos a los equipos; copias de seguridad que garanticen la protección de la información y auditorías permanentes a los diferentes procesos que maneja a la organización, con el fin de verificar la implementación de las políticas y procedimientos relacionados con la seguridad de la información.

RECOMENDACIONES

Es necesario que la Gerencia asigne un presupuesto para la implementación de controles que permitan mejorar la seguridad de los procesos y sistemas.

Se propone a la organización realizar capacitaciones al personal enfocadas en los protocolos que se deben aplicar en la organización para mejorar la seguridad de la información.

Se debe invertir en herramientas de seguridad informáticas como antivirus y firewall actualizado, los cuales mejoran la protección de la organización de ataques externos.

Entre otras necesidades se plantea recomendar lo siguiente:

- Debe definirse roles y responsabilidades de los empleados
- Debe entrenarse al personal especializado en materia de controles de acceso a la información, con seguridad a la asignación de contraseña a los equipos
- Debe exponerse al personal la identificación de las amenazas, vulnerabilidades y controles para la protección de la información.
- Debe haber un sistema de alimentación ininterrumpida (UPS) para proteger los equipos de cortes de luz y otras fallas generadas
- Debe implementarse procedimientos, políticas y métodos para resguardar la información.
- Debe mantenerse siempre copias de seguridad para garantizar la protección de la información
- Debe planificarse auditorías permanentes a los diferentes procesos
- Debe plantearse una inversión en la protección de la información
- Debe realizarse un mantenimiento preventivo a los equipos

BIBLIOGRAFÍA

ALVARADO, Claudia. Sistema de gestión de seguridad de la información: qué es y sus etapas. [Blog]. Bogotá. 2022. [Consultado: 28 de agosto de 2022]. Disponible en https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas.

CEUPE. Política de seguridad de la información y SGSI. [Sitio web]. [Consultado: 21 de agosto de 2022]. Disponible en https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html?dt=1662229753673.

CEUPE. Política de seguridad de la información y SGSI. [sitio web]. [Consultado: 21 de agosto de 2022]. Disponible en https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html?dt=1662229753673.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1377. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Derogado Parcialmente por el Decreto 1081 de 2015. Santa Fe de Bogotá, D.C.: Diario Oficial. Nro. 48834 del 27 de junio de 2013. [Consultado: agosto 22 de 2022]. Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.:
Diario Oficial. 2009. nro. 47223. p. 1-4. [Consultado: agosto 22 de 2022]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (23, diciembre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. Nro. 48587 de octubre 18 de 2012. [Consultado: agosto 16 de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CONCATEL. Ventajas de la implantación de un SGSI. [Blog]. Barcelona, España. 2022. [Consultado: 31 de agosto de 2022]. Disponible en: https://sii-concatel.com/ventajas-de-la-implantacion-de-un-sgsi/#:~:text=Los%20SGSI%20mejoran%20la%20credibilidad,que%20almacena%20y%2Fo%20transmite.

DA SILVA, Douglas. ¿Qué es la seguridad de la información? [En línea]. (18 de septiembre de 2023). [Consultado: 17 de abril de 2024]. Disponible en: https://www.zendesk.com.mx/blog/que-es-seguridad-de-informacion/.

GÓMEZ, F. (2020). “La Importancia de implementar un SGSI en nuestra organización”. [Internet]. Disponible en https://www.safesociety.co/blogitem/4/la-importancia-de-implementar-un-sgsi-en-nuestra-organizacion.

ISO 27001:2022. Norma ISO 27001:2022 [sitio web]. Madrid España. [Consultado: 30 de agosto de 2022]. Disponible en: https://normaiso27001:2022.es/.

ISO. ISO/CEI 27001:2022:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. [sitio web]. Octubre del 2013. Chile. [Consultado: 20 de agosto de 2022]. Disponible en https://www.iso.org/standard/54534.html.

LAOYAN, Sarah. Cómo implementar el análisis de brechas para alcanzar los objetivos de negocios. [En línea]. Asana en Español. (17 de mayo de 2022). [Consultado: 28 de agosto de 2022]. Disponible en: https://asana.com/es/resources/gap-analysis.

MARTELO, Raúl J; MADERA, Jhonny E y BETIN, Andrés D. Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información tecnológica. [En línea]. 2015, vol.26, n.2 [citado el 10-08-2022], pp.129-134. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642015000200015&lng=en&nrm=iso. ISSN 0718-0764. http://dx.doi.org/10.4067/S0718-07642015000200015.

MINGUEZA, Sergio. Marco teórico: definición, estructura y ejemplos. [en línea]. (31 de enero de 2023). [Consultado: 17 de abril de 2024]. Disponible en: https://expertouniversitario.es/blog/marco-teorico/#toc_Que_es_un_marco_teorico.

OCAMPO WILCHES, Ana Cristina. Papel de la teoría en la investigación. [en línea]. (Septiembre de 2023). [Consultado: 17 de abril de 2024]. Disponible en: https://www.researchgate.net/publication/374248226_Papel_de_la_teoria_en_la_investigacion.

ORTIZ BUITRON, Vanessa Catherine. Diseño de las políticas de seguridad de la información en la compañía de seguros S.A**.** [en línea], Trabajo de grado para optar al título especialista en seguridad informática. Bogotá. D.C, Colombia: Institución. Universidad Católica de Colombia. Facultad de Ingeniería (2021). (p.33). [Consultado: 17 abril 2024]. Disponible en: https://repository.ucatolica.edu.co/server/api/core/bitstreams/671c379e-57cf-4b0b-93d1-eccb021944e5/content

OSTEC. ISO 27002: Buenas prácticas para gestión de la seguridad de la información. [sitio web]. Ubarão, Brasil. Business Security; [Consultado: 22 de agosto de 2022]. Disponible en: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/.

RUÍZ TAPIA, Juan Alberto; ESTRADA GUTIÉRREZ, César Enrique y SÁNCHEZ PAZ, Ma. de la Luz. Propuesta de un Modelo de un Sistema de Gestión de Calidad en Seguridad de la Información basado en la norma ISO 27001:2013 para Instituciones Educativas. En: Revista de Investigación Latinoamericana en Competitividad Organizacional. Editorial RILCO. (febrero 2020). Volumen Nro. 5. [Consultado: 15 de agosto de 2022]. Disponible en https://www.eumed.net/rev/rilco/05/gestion-instituciones.pdf.

SEMIC EFFECTIVE IT SOLUTIONS. ¿Por qué necesitamos un SGSI? [blog]. Madrid, España. 22 de octubre del 2018. [Consultado: 01 de septiembre de 2022]. Disponible en https://www.semic.es/es/content/por-que-necesitamos-un-sgsi.

Sisteseg.com. Seguridad de la información ISO 27001:2013. [sitio web]; [Consultado: 28 de agosto de 2022]. Disponible en: https://www.sisteseg.com/informatica.html.

UNIVERSITAT OBERTA DE CATALUNYA. Principales novedades de la norma ISO /IEC 27002:2013. [Blog]. 4 de julio 2021. España. [Consultado: 22 de agosto de 2022]. Disponible en https://blogs.x.uoc.edu/calidad-iso/principales-novedades-de-la-norma-iso-iec-270022013/.

ANEXOS

ANEXO 1. Cuestionario aplicado área de Sistemas

	**GESTION DE INFORMACION Y COMUNICACIÓN**	**CODIGO: FGI-025**
		VERSION: 1
	ENCUESTA SGSI TIPO CUALITATIVO	**FECHA: NOV 2021**
		PAGINA 1 DE 1

CUESTIONARIO ÁREA SISTEMAS

Cargo: _____ Fecha: _____

N°	Pregunta
1	¿La organización cuenta con un Manual de Política de Seguridad de la Información?
2	¿Cada cuánto se actualiza el Manual de Política de Seguridad de la Información?
3	¿El Manual de Política de Seguridad de la Información es socializado a todo el personal?
4	¿Se cuenta con un área o responsable de seguridad de la información?
5	¿La organización tiene implementada herramientas de seguridad?
6	¿Se tiene documentados instructivos y procedimientos propios del área?
7	¿Cada cuánto se actualiza los instructivos y procedimientos?
8	¿Se cuenta con el apoyo y participación de la Gerencia?
9	¿El personal recibe capacitación en temas de seguridad de la información?
10	¿Se tiene definido perfiles y roles de usuarios?
11	¿Se tiene clasificada la información?
12	¿La organización tiene implementadas políticas y controles de seguridad?
13	¿Se cuenta con mecanismos de autenticación?
14	¿Se gestiona contraseña personaliza para cada uno de los usuarios?
15	¿Cómo está conformada la infraestructura tecnológica de la organización?
16	¿Se cuenta con un antivirus y que protección brinda al sistema?
17	¿Con qué periodicidad se realiza mantenimiento a los equipos tecnológicos?
18	¿La organización tiene control de inventarios tecnológicos?
19	¿Con qué periodicidad se realiza los respaldos de información?
20	¿La organización ha presentado algún caso de incidentes de seguridad?
21	¿Qué medidas se tienen en caso de ataque al sistema de información?

ANEXO 2. Cuestionario aplicado a otras áreas

	**GESTION DE INFORMACION Y COMUNICACIÓN**	**CODIGO: FGI-026**
		VERSION: 1
	ENCUESTA SGSI TIPO CUALITATIVO	**FECHA: NOV 2021**
		PAGINA 1 DE 1

CUESTIONARIO OTROS PROCESOS

Cargo:_____ Fecha: _____

N°	**Pregunta**
1	¿Qué conoce acerca del tema de Seguridad de la información?
2	¿Cada cuánto se actualiza los instructivos y procedimientos?
3	¿La organización cuenta con un área o responsable de seguridad de la información?
4	¿Identifica los activos de información que posee el área a que pertenece?
5	¿El personal recibe capacitación en temas de seguridad de la información?
6	¿Se gestiona contraseña personaliza para cada uno de los usuarios?
7	¿Con qué periodicidad se realiza mantenimiento a los equipos tecnológicos?
8	¿Con qué periodicidad se realiza los respaldos de información?
9	¿La organización ha presentado algún caso de incidentes de seguridad?
10	¿Qué medidas se tienen en caso de ataque al sistema de información?

ANEXO 3. Resultados cuestionario aplicado área de sistemas

1. Cargo que desempeña	Coordinador de sistemas	Técnico de sistemas	TECNICO DE SISTEMAS	Ingeniero de sistemas
2. ¿La organización cuenta con un Manual de Política de Seguridad de la Información?	No	No cuenta	NO TIENE	No se ha documentado
3. ¿Cada cuánto se actualiza el Manual de Política de Seguridad de la Información?	No existe un manual	No	NO	No sé tiene
4. ¿El Manual de Política de Seguridad de la Información es socializado a todo el personal?	No existe un manual	No	NO	No sé tiene
5. ¿Se cuenta con un área o responsable de seguridad de la información?	Área de sistemas	Coordinador	SISTEMAS	Si el área de sistemas
6. ¿La organización tiene implementada herramientas de seguridad?	Se cuenta con un antivirus ESET, la cual se actualiza anualmente.	Cuenta con claves de acceso y antivirus	CUENTA CON ANTIVIRUS ESET	Si un antivirus y contraseñas en los equipos
7. ¿Se tiene documentados instructivos y procedimientos propios del área?	Se tiene procedimientos de mantenimiento de equipos	No	NO	Si, procedimientos de mantenimiento de equipos
8. ¿Cada cuánto se actualiza los instructivos y procedimientos?	Se actualiza cuando se requiere.	No	NO, SE DEBEN IMPLEMENTAR	Lo realiza el coordinador
9. ¿Se cuenta con el apoyo y participación de la Gerencia?	Si	Si	SI	Si
10. ¿El personal recibe capacitación en temas de seguridad de la información?	No	No	NO	No
11. ¿Se tiene definido perfiles y roles de usuarios?	Si	Si	SI	Si
12. ¿Se tiene clasificada la información?	Si, en cuatro categorías: confidencial, restringido, uso interno y público.	No	SI, EN INFORMACION PRIVADA Y PUBLICA	Si, privado y de uso público
13. ¿La organización tiene implementadas políticas y controles de seguridad?	Se asigna un usuario y contraseña	Si	POLITICAS NO TIENE IMPLEMENTADAS Y CONTROLES SI	Se tienen solo controles de seguridad
14. ¿Se cuenta con mecanismos de autenticación?	Se cuenta con un usuario y contraseña personal	Se tiene usuario y contraseña por trabajador	SE ASIGNA UN USUARIO Y CONTRASEÑA	Si, se asigna usuario y contraseña

ANEXO 4. (continuación)

15. ¿Se gestiona contraseña personaliza para cada uno de los usuarios?	El usuario tiene autorización para gestionar la contraseña de ingreso al sistema.	Si	SI	Si
16. ¿Cómo está conformada la infraestructura tecnológica de la organización?	Se cuenta con un servidor y 10 equipos conectados a través de una red LAN.	Equipos y un servidor	UN SERVIDOR, EQUIPOS	Se cuenta con 10 computadores y un servidor
17+. ¿Se cuenta con un antivirus y que protección brinda al sistema?	Si, antivirus ESET	Si	SI ANTIVIRUS ESET	Si
18. ¿Con qué periodicidad se realiza mantenimiento a los equipos tecnológicos?	Se realiza mantenimiento dependiendo de la necesidad que se genera.	Si, cuando lo soliciten las áreas	CUANDO LO PIDAN	Cuando las áreas lo soliciten, se debe realizar un cronograma
19. ¿La organización tiene control de inventarios tecnológicos?	Se lleva un inventario de activos registrado en la contabilidad	No	NO	El inventario lo maneja el área de contabilidad
20. ¿Con qué periodicidad se realiza los respaldos de información?	Mensualmente	Mensual	MENSUAL	Una vez al mes
21. ¿La organización ha presentado algún caso de incidentes de seguridad?	No	No	NO	No se ha presentado
22. ¿Qué medidas se tienen en caso de ataque al sistema de información?	Se cuenta con antivirus, control de ingreso al servidor y copias de seguridad	Copias de seguridad	ANTIVIRUS, COPIAS DE SEGURIDAD	Copias de seguridad, antivirus ESET y asignación usuario y contraseña

ANEXO 5. Resultados cuestionario aplicado otros procesos

1. Cargo que desempeña	Jefe de ventas	Contadora	Gerente	Jefe talento humano
2. ¿Qué conoce acerca del tema de Seguridad de la información?	Copias de seguridad que se realiza en el pc	Son las herramientas que tiene la organización para proteger la información	Es muy importante realizar copias de seguridad de la información y contar con un buen antivirus	Son todas las medidas que debe tomar la organización para proteger la información
3. ¿Cada cuánto se actualiza los instructivos y procedimientos?	No los conozco	Cada año	Anualmente	Falta documentarlos, no se tienen.
4. ¿La organización cuenta con un área o responsable de seguridad de la información?	Sistemas	Coordinador de sistemas	Área de sistemas	Sistemas
5. ¿Identifica los activos de información que posee el área a que pertenece?	Computador	Computador, impresora, programa contable tns	Computador, teléfono, impresora	Computador, impresora, teléfono
6. ¿El personal recibe capacitación en temas de seguridad de la información?	No	No	Capacitación virtual	No
7. ¿Se gestiona contraseña personaliza para cada uno de los usuarios?	Si	Si	Si	Si
8. ¿Con qué periodicidad se realiza mantenimiento a los equipos tecnológicos?	Cuando se solicita	Anualmente	Cada seis meses	Cuando se requiere
9. ¿Con qué periodicidad se realiza los respaldos de información?	Diariamente	Diariamente	Mensual	Mensual
10. ¿La organización ha presentado algún caso de incidentes de seguridad?	Nunca	No	Nunca	No
11. ¿Qué medidas se tienen en caso de ataque al sistema de información?	Copias de seguridad	Backup diario y antivirus	Backup	Antivirus y copias de seguridad

ANEXO 6. Selección Controles ISO 27002:2013

Controles	Descripción	Tipo de Activos					
		Comunicaciones	Datos	Hardware	Servicios	Software	Soporte
5.	**POLITICAS DE SEGURIDAD.**						
5.1	**Directrices de la Dirección en seguridad de la información.**						
5.1.1	Conjunto de políticas para la seguridad de la información.	X	X	X	X	X	X
5.1.2	Revisión de las políticas para la seguridad de la información.	X	X	X	X	X	X
6.	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.**						
6.1	**Organización interna.**						
6.1.1	Asignación de responsabilidades para la seguridad de la información.	X	X	X	X	X	X
6.1.2	Segregación de tareas.	X	X	X	X	X	X
6.1.3	Contacto con las autoridades.				X		X
6.1.4	Contacto con grupos de interés especial.	X	X	X	X	X	X
6.2	**Dispositivos para movilidad y teletrabajo.**						
6.2.1	Política de uso de dispositivos para movilidad.	X		X			
6.2.2	Teletrabajo.	X		X			
7.	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**						
7.1	**Antes de la contratación.**						
7.1.1	Investigación de antecedentes.						X
7.1.2	Términos y condiciones de contratación.						X
7.2	**Durante la contratación.**						
7.2.1	Responsabilidades de gestión.						X
7.2.2	Concienciación, educación y capacitación en seguridad de la información						X
7.2.3	Proceso disciplinario.						X
7.3	**Cese o cambio de puesto de trabajo.**						
7.3.1	Cese o cambio de puesto de trabajo.						X
8.	**GESTIÓN DE ACTIVOS.**						
8.1	**Responsabilidad sobre los activos.**						
8.1.1	Inventario de activos.	X	X	X	X	X	X
8.1.2	Propiedad de los activos.	X	X	X	X	X	X
8.1.3	Uso aceptable de los activos.	X	X	X	X	X	X

ANEXO 5. (continuación)

8.1.4	Devolución de activos.	X	X	X	X	X	X
8.2	**Clasificación de la información.**						
8.2.1	Directrices de clasificación.		X				
8.2.2	Etiquetado y manipulado de la información.		X				
8.2.3	Manipulación de activos.		X				
8.3	**Manejo de los soportes de almacenamiento.**						
8.3.1	Gestión de soportes extraíbles.		X	X			
8.3.2	Eliminación de soportes.		X	X			
8.3.3	Soportes físicos en tránsito.		X	X			
9.	**CONTROL DE ACCESOS.**						
9.1	**Requisitos de negocio para el control de accesos.**						
9.1.1	Política de control de accesos.				X		X
9.1.2	Control de acceso a las redes y servicios asociados.	X					
9.2	**Gestión de acceso de usuario.**						
9.2.1	Gestión de altas/bajas en el registro de usuarios.						X
9.2.2	Gestión de los derechos de acceso asignados a usuarios.						X
9.2.3	Gestión de los derechos de acceso con privilegios especiales.						X
9.2.4	Gestión de información confidencial de autenticación de usuarios.						X
9.2.5	Revisión de los derechos de acceso de los usuarios.						X
9.2.6	Retirada o adaptación de los derechos de acceso						X
9.3	**Responsabilidades del usuario.**						
9.3.1	Uso de información confidencial para la autenticación.						X
9.4	**Control de acceso a sistemas y aplicaciones.**						
9.4.1	Restricción del acceso a la información.					X	X
9.4.2	Procedimientos seguros de inicio de sesión.					X	X
9.4.3	Gestión de contraseñas de usuario.					X	X
9.4.4	Uso de herramientas de administración de sistemas.					X	X
9.4.5	Control de acceso al código fuente de los programas.					X	X
11.	**SEGURIDAD FÍSICA Y AMBIENTAL.**						
11.1	**Áreas seguras.**						
11.1.1	Perímetro de seguridad física.				X		X
11.1.2	Controles físicos de entrada.			X	X		X
11.1.5	El trabajo en áreas seguras.		X				X
11.2	**Seguridad de los equipos.**						
11.2.1	Emplazamiento y protección de equipos.	X					
11.2.2	Instalaciones de suministro.	X		X			

ANEXO 5. (continuación)

11.2.3	Seguridad del cableado.	X		X			
11.2.4	Mantenimiento de los equipos.	X		X			
11.2.5	Salida de activos fuera de las dependencias de la organización.	X		X			
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	X		X			
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	X		X			
11.2.8	Equipo informático de usuario desatendido.	X		X			
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.						X
12.	**SEGURIDAD EN LA OPERATIVA.**						
12.2	**Protección contra código malicioso.**						
12.2.1	Controles contra el código malicioso.		X			X	
12.3	**Copias de seguridad.**						
12.3.1	Copias de seguridad de la información.		X			X	
12.4	**Registro de actividad y supervisión.**						
12.4.1	Registro y gestión de eventos de actividad.		X			X	X
12.4.2	Protección de los registros de información.		X			X	
12.4.3	Registros de actividad del administrador y operador del sistema.		X			X	
12.4.4	Sincronización de relojes.		X	X			
13.	**SEGURIDAD EN LAS TELECOMUNICACIONES.**						
13.1	**Gestión de la seguridad en las redes.**						
13.1.1	Controles de red.	X					
13.1.2	Mecanismos de seguridad asociados a servicios en red.	X					
13.1.3	Segregación de redes.	X					
13.2	**Intercambio de información con partes externas.**						
13.2.1	Políticas y procedimientos de intercambio de información.		X				X
13.2.2	Acuerdos de intercambio.		X				X
13.2.3	Mensajería electrónica.		X				X
13.2.4	Acuerdos de confidencialidad y secreto.		X				X
16.	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**						
16.1	**Gestión de incidentes de seguridad de la información y mejoras.**						
16.1.1	Responsabilidades y procedimientos.		X				X
16.1.2	Notificación de los eventos de seguridad de la información.		X				X
16.1.3	Notificación de puntos débiles de la seguridad.		X				X

ANEXO 5. (continuación)

16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.		X				X
16.1.5	Respuesta a los incidentes de seguridad.		X				X
16.1.6	Aprendizaje de los incidentes de seguridad de la información.		X				X
16.1.7	Recopilación de evidencias.		X				X
17.	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**						
17.1	**Continuidad de la seguridad de la información.**						
17.1.1	Planificación de la continuidad de la seguridad de la información.				X		
17.1.2	Implantación de la continuidad de la seguridad de la información.				X		
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.				X		
18.	**CUMPLIMIENTO.**						
18.1	**Cumplimiento de los requisitos legales y contractuales.**						
18.1.1	Identificación de la legislación aplicable.				X		
18.1.2	Derechos de propiedad intelectual (DPI).		X		X	X	
18.1.3	Protección de los registros de la organización.		X		X		X
18.1.4	Protección de datos y privacidad de la información personal.		X				
18.1.5	Regulación de los controles criptográficos.		X			X	X
18.2	**Revisiones de la seguridad de la información.**						
18.2.1	Revisión independiente de la seguridad de la información.		X	X	X		X
18.2.2	Cumplimiento de las políticas y normas de seguridad.		X				X
18.2.3	Comprobación del cumplimiento.		X	X			X