SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001:2015- EN LA EMPRESA MAGDANIEL LTDA. EN EL DISTRITO ESPECIAL, TURÍSTICO Y CULTURAL DE RIOHACHA

LUZ DARIS SUAREZ BARROS

UNIVERSIDAD DE LA GUAJIRA
FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
PROGRAMA DE MAESTRÍAS EN ADMINISTRACIÓN DE EMPRESAS
RIOHACHA, AGOSTO 2021

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001:2015 - EN LA EMPRESA MAGDANIEL LTDA. EN EL DISTRITO ESPECIAL, TURÍSTICO Y CULTURAL DE RIOHACHA

LUZ DARIS SUAREZ BARROS

Trabajo presentado como requisito para optar al título de Magister en Administración de Empresas

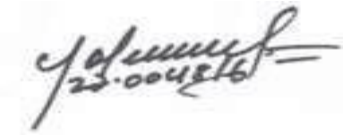
Director
YOLEIDA VEGA MENDOZA
Magister en Gerencia de Proyectos de Investigación y Desarrollo

UNIVERSIDAD DE LA GUAJIRA
FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
PROGRAMA DE MAESTRÍAS EN ADMINISTRACIÓN DE EMPRESAS
RIOHACHA, AGOSTO 2021

CERTIFICACIÓN DEL DIRECTOR

Yo, **YOLEIDA VEGA MENDOZA** identificado con la cédula de ciudadanía No. 27.004.816, expedida en Riohacha, La Guajira, por medio del presente hago constar que el trabajo de grado, presentado por el señorita **LUZ DARIS SUAREZ BARROS**, identificado con la cédula de ciudadanía No. 1.118.823.778, expedida en Riohacha, La Guajira, titulado **Sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda., en el Distrito Turístico, Especial y Cultural de Riohacha**, para optar al título de Magister en Administración de Empresas, reúne los requisitos y méritos suficientes para ser sometido a consideración del jurado evaluador que se designe, para su posterior sustentación en presentación pública.

Dado en el Distrito Turístico, Especial y Cultural de Riohacha, Departamento de La Guajira, el 31 de agosto de 2021.



_____

YOLEIDA VEGA MENDOZA
Director del Trabajo de Grado

CERTIFICACIÓN ANTIPLAGIO

Como director de este trabajo de grado como requisito para optar por título de Magister en Administración de Empresas, presentado por **LUZ DARIS SUAREZ BARROS**, identificado con la cédula de ciudadanía No. 1.118.823.778, con el trabajo titulado **Sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda., en el Distrito Turístico Especial y Cultural de Riohacha**, afirmo haber revisado el informe arrojado por el software anti plagio «Turnitin» con un 12% de coincidencias con otros trabajos y que las fuentes utilizadas detectadas por el mismo en el trabajo en mención, se encuentran debidamente citadas de acuerdo a las normas APA vigentes, por lo que el proyecto de investigación es de su total autoría.

Dado en el Distrito Turístico, Especial y Cultural de Riohacha, Departamento de La Guajira, el 31 de agosto de 2021.

_____

YOLEIDA VEGA MENDOZA
Director del Trabajo de Grado

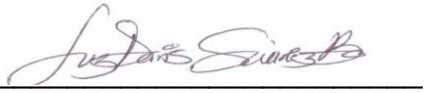
DECLARATORIA DE AUTENTICIDAD

Yo, **Luz Daris Suarez Barros**, estudiante del Programa de Maestría en Administración de Empresas de la Universidad de La Guajira, identificado con cédula de ciudadanía No. 1.118.823.778, expedida en Riohacha, La Guajira, autor(a) del trabajo de grado titulado: **Sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.;** declaro bajo la gravedad del juramento que:

a) El presente trabajo de grado es de mi autoría;
b) He respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesis no ha sido plagiada parcial ni totalmente;
c) La tesis no ha sido auto plagiada; es decir, no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional;
d) Los datos presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presenten en la tesis se constituirán en aportes a la realidad investigada.

De identificarse la presencia de fraude (datos falsos), plagio (información sin citar a autores), auto plagio (presentar como nuevo algún trabajo de investigación propio que ya ha sido publicado), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad de La Guajira y el país.

Dado en el Distrito Especial, Turístico y Cultural de Riohacha, Departamento de La Guajira, el 31 de agosto de 2021.



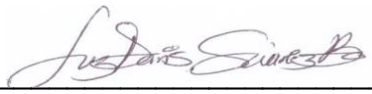
LUZ DARIS SUAREZ BARROS

DERECHOS DE AUTOR

Yo, **LUZ DARIS SUAREZ BARROS**, identificado con cédula de ciudadanía No. 1.118.823.778, expedida en Riohacha, La Guajira autor(a) del trabajo de grado titulado: **Sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.**, autorizo a la Universidad de La Guajira, para que haga de esta tesis un documento disponible para su lectura, consulta y aporte a los procesos de investigación, según las normas de la institución.

Cedo los derechos en línea patrimoniales de mi tesis, con fines de difusión pública, además apruebo la reproducción de esta tesis, dentro de las regulaciones de la Universidad, siempre y cuando respeten mis derechos de autor (a).

Dado en el Distrito Especial, Turístico y Cultural de Riohacha, Departamento de La Guajira, el 31 de agosto de 2021.



LUZ DARIS SUAREZ BARROS

DEDICATORIA

Esta tesis se la dedico principalmente a Dios, al creador de todas las cosas, por ser el inspirador y mi fortaleza, para continuar en este proceso de obtener uno de los anhelos deseado en mi vida.

A mis padres, quienes me dieron vida, educación, apoyo y consejos. Además, me enseñaron a formarme con buenos sentimientos, hábitos y valores, lo cual me han ayudado a seguir adelante en los momentos más difíciles y a convertirme en lo que hoy soy.

A mis hermanos, por estar siempre presente, acompañándome y por el apoyo moral en cada momento de mi vida.

A mi novio, por todo su amor, apoyo y compresión a lo largo de esta etapa.

A todos mis seres queridos, que aportaron su granito de arena a través de su apoyo para el cumplimiento de este trabajo con éxito, en especial a aquellos que me abrieron las puertas y compartieron sus conocimientos. ¡Gracias!.

Para ellos es esta dedicatoria de tesis, pues es a ellos a quienes se las debo por su apoyo incondicional.

Luz Daris Suarez Barros

AGRADECIMIENTOS

A ti, Dios de mis padres, te alabo y te doy gracias. Me has dado sabiduría y poder, me has dado a conocer lo que pedimos. Daniel 20:23.

De tu mano señor, todo es posible para el que cree. La realidad, es el mayor sueño hecho realidad.

A mis padres, hermanos y familia, que siempre han estado presente apoyándome en cada etapa, proceso y momento de mi vida.

A la Universidad de la Guajira, como institución de Educación superior estatal, por permitirme hacer parte de ella.

A mi directora de tesis, por su colaboración gracias a su ayuda, entrega y múltiples correcciones, se pudieron romper las barreras, para llevar a cabo esta investigación.
A mi asesora de tesis por el tiempo, dedicación y apoyo, para que yo pudiera elaborar esta investigación.

Y por último a mis amigos y todas aquellas personas, que de una u otra manera hicieron parte de este largo proceso, para que hoy sea una realidad.

Luz Daris Suarez Barros

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

LISTA DE ANEXOS

SUÁREZ BARROS, Luz Daris, Sistema de Gestión de Seguridad de la Información bajo ISO / IEC 27001: 2015 en Magdaniel Ltda., Universidad de La Guajira, Programa de Maestría en Administración de Empresas, Riohacha, La Guajira.

RESUMEN

La presente investigación se titula Sistema de Gestión de Seguridad de la Información bajo la Norma ISO/IEC 27001:2015, en la empresa Magdaniel Ltda., en el Distrito Especial, Turístico y Cultural de Riohacha. Tiene como objetivo analizar el SGSI bajo la norma ISO 27001:2015, con el tratamiento de dimensiones enfocadas en las políticas de seguridad, seguridad física y del entorno y los activos de la información.

El estudio se encuentra soportado principalmente por la Norma ISO 27001 del 2015, enfocado metodológicamente en nivel cuantitativo de tipo aplicada, explicativa y transversal, basada en el diseño de campo, no experimental; contando con una población de estudio de 6 trabajadores de la empresa. El instrumento de medición de la variable fue el cuestionario con escala de Likert conformada por 20 afirmaciones el cual fue sujeto a la validación por expertos, a través de una prueba piloto obteniendo una confiabilidad del 0,967% por el coeficiente Alfa Crombach. El instrumento fue aplicado a la totalidad de la población de estudio logrando obtener resultados que fueron analizados por medio de pruebas estadísticas descriptivas.

Las conclusiones y recomendaciones descritas en la investigación se encuentran dirigidas a la mejora continua de los procesos dentro de la empresa puesto que es de suma importancia contar con los recursos basados en tecnología y seguridad; por lo tanto, los lineamientos establecidos bajo la norma ISO 27001:2015 permite la implementación de un sistema de gestión en seguridad de la información para asegurar y analizar los procesos en referencia al acceso del entorno, así mismo, mitigar los riesgos a los que se encuentra expuesto la empresa y sus activos.

Palabras claves: Sistema de gestión de seguridad de la información, políticas, acceso, seguridad física, activos.

SUAREZ BARROS, Luz Daris, Information Security Management System under ISO / IEC 27001: 2015- in Magdaniel Ltd., University of La Guajira, Master's Program in Business Administration, Riohacha, La Guajira.

ABSTRACT

This research is entitled Information Security Management System under the ISO / IEC 27001: 2015 Standard, in the company Magdaniel Ltda., In the Special, Tourist and Cultural District of Riohacha. Its objective is to analyze the ISMS under the ISO 27001: 2015 standard, with the treatment of dimensions focused on security policies, physical and environmental security and information assets.

The study is mainly supported by the ISO 27001 Standard of 2015, methodologically focused on a quantitative level of applied, explanatory and cross-sectional type, based on the field design, not experimental; counting on a study population of 6 company workers. The variable measurement instrument was the Likert scale questionnaire made up of 20 statements which was subject to validation by experts, through a pilot test, obtaining a reliability of 0.967% by the Alpha Crombach coefficient. The instrument was applied to the entire study population, obtaining results that were analyzed by means of descriptive statistical tests.

The conclusions and recommendations described in the research are aimed at the continuous improvement of the processes within the company since it is extremely important to have resources based on technology and security; Therefore, the guidelines established under the ISO 27001: 2015 standard allow the implementation of an information security management system to ensure and analyze the processes in reference to access to the environment, as well as mitigate the risks to which the company and its assets are exposed.

Keywords: Information security management system, policies, access, physical security, assets.

INTRODUCCIÓN

Actualmente, tanto las personas como las empresas, están continuamente captando una serie de datos que permiten el análisis de aspectos para el mejoramiento continuo y conocimiento del ambiente a nivel organizacional. Por ello, en el área de sistemas o manejo de datos, son constituidos actualmente como el término de información, donde el manejo del mismo conlleva a la toma decisiones acertadas. Por ello, la información disponible y accesible a tiempo y en la cantidad precisa es un factor clave para toda organización (Devece, Guira & Lapiedra, 2011).

En este orden de ideas, la información manejada dentro de las organizaciones y/o personas es de suma importancia y considerada como un activo valioso el cual debe ser protegido de agentes que lo afecten tanto a nivel interno como externo, es así como el estudio realizado por Benavides y Blandón (2017) en la Universidad de Manizales, sustentan que el avance tecnológico hoy en día desarrolla nuevos riesgos dentro de la seguridad para el manejo de la información, por el cual se lleva a cabo la aplicación de prácticas inclinadas a la adaptación de métodos para preservar privacidad, honestidad y reserva en todo aquello que se encuentre relacionado con la organización.

Frente a lo anteriormente descrito, es necesario que las organizaciones manejen apropiadamente los recursos haciendo posible el cumplimiento de los objetivos planteados dentro del sistema de gestión de seguridad de la información. De esta manera, salvaguardar y asegurar los activos de la información, están representando en un gran reto para las compañías de hoy.

En este orden, Velásquez (2015) afirma acerca de la importancia que toda organización independientemente de su naturaleza o tamaño, crea conciencia en

la complejidad de amenazas, viéndose representando en todo aquello que se encuentre dirigido en la generación de altos costos económicos, legales, afectación de imagen e incluso la continuidad de la existencia en el mercado.

De esta manera, cada día se hace complejo asegurar y administrar la seguridad en la información, permitiendo que haga parte de los planes estratégicos en las empresas, donde la designación de responsabilidades es importante para el fortalecimiento de las actividades en cada área, por el cual, la toma de decisiones en la protección de la información debe de estar dirigida a la detención de riesgos que puedan afectar el libre desarrollo de los procesos.

Es así, como la presente tesis realizó el análisis del SGSI basado en la norma ISO/IEC 27001:2015, permitiendo conocer el estado del funcionamiento actual en la empresa Magdaniel Ltda., en referencia a la protección de la información propia de la organización, teniendo en cuenta criterios específicos que puedan evidenciar el desempeño de los requisitos exigidos, los cuales deben ser alineados a lo requerido; y de esta manera describir los parámetros que garanticen la confidencialidad, integridad y disponibilidad de la información en la empresa.

Por lo anterior, el trabajo se encuentra estructurado en el desarrollo de cuatro capítulos, encontrándose estructurado para su mayor comprensión, dando inicio con el capítulo uno, comprendido por el problema de investigación dando a conocer el planteamiento del problema, seguido de los objetivos, justificación y delimitación de la investigación; el segundo capítulo consta del desarrollo del marco referencial el cual permite la descripción de los antecedentes relacionado con la variable de estudio, un marco conceptual, legal e institucional, seguido la sistematización de la variable descrito por el cuadro de operacionalización dando a conocer las dimensiones e indicadores de estudio.

Seguidamente, el tercer capítulo relaciona todo lo referente al marco metodológico, el cual determina el tipo, diseño y fuentes de recolección de

información; así mismo, se da a conocer la población de estudio, técnica e instrumentos; cálculo de validez y confiabilidad en la aplicación del instrumento; por último, el cuarto capítulo establece el análisis de los derivaciones obtenidas por medio de la aplicación de pruebas estadísticas, para la formulación de lineamientos estratégicos, recomendaciones y conclusiones para futuras investigaciones.

1. PROBLEMA DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

Las transformaciones constantes generadas en el mundo moderno llevan consigo un incesante cambio en el desarrollo; el crecimiento de la economía, el alto manejo de información y entre otros aspectos, los cuales traen consigo altos porcentajes de amenazas que deben ser atacadas de una forma veraz, ya que por esas inminencias no se debe de dejar a un lado el propósito de expandirse y la posibilidad de innovación.

Es así, como la tecnología en el transcurrir de los años está haciendo parte del diario vivir del ser humano realizando cambios significativos en la sociedad y organizaciones, permitiendo el crecimiento e innovación en cada proceso ya sea personal o a nivel empresarial generando avances significativos contribuyendo de manera positiva en los procesos, aunque en ocasiones por factores internos y externos afectan de manera negativa, conllevando a la descripción de procedimientos estructurados que permitan la minimización de los riesgos tecnológicos, por ello, Camelo (2010) hace conocer que los distintos procesos deben ser realizado por el personal calificado para la realización de tareas, donde se pueda controlar los riesgos relacionados con la perdida de información, accesos indebidos, falta de implementación de políticas entre otros.

Por lo anterior, es de importancia mencionar que la tecnología es una herramienta indispensable en los procesos productivos de una organización independientemente de la actividad de económica ejercida, debido a que es de suma importancia proteger la información considerada de gran valor, en cada proceso y la sistematización de las bases de datos manejadas en la organización.

En cualquier entorno priman características específicas, las cuales se deben tener en cuenta para adoptar medidas que originen estrategias importantes las cuales permitan actuar frente a cualquier situación no deseada, contrarrestando todo aquello desencadenado en el área de tecnología, es por ello, donde la mayoría de las organizaciones consideran la posibilidad de establecer sistemas de protección para la información que ellos manejan, para no dejar desprotegidos los aspectos importantes mitigando así aquellos riesgos que se desprenden en ese medio.

Con el transcurrir del tiempo, el uso de la tecnología se ha transformado como una necesidad que permite mantener las compañías o las mismas personas en su diario vivir, conllevado a un mesurable despliego de inquietudes desarrolladas a medida que se estén ejecutando tareas a través del uso de la informática o todo lo que gire en torno a la misma, creando de esta forma la necesidad de proteger la información manejada para evitar posibles daños y pérdidas incalculables.

Por tal motivo, se permite resaltar que la tecnología ha permitido estar en niveles altos de conocimiento, debido a la facilidad para la ejecución de tareas, la accesibilidad de información y la comunicación entre persona y/o empresas, pero es de mencionar que también existe un lado negativo de toda la situación, el cual va encaminado a la manipulación de información muchas veces de personas inescrupulosas, dedicadas en la mayor parte del tiempo a obtener información para cometer actos ilícitos.

En el desarrollo de actividades dentro de una compañía la utilización de mecanismo de sistemas e informática poseen ciertas características que deben de ser manejadas de la forma adecuada, según los aportes de Alvarez & Perez (2004), quienes sustentan que “el amplio grado de integración de las redes, comunicación y sistemas demanda transformaciones en la práctica de la disciplina orientada a ejercer un control superior mediante la auditoria y/o control”.

Así mismo, en la investigación realizada por Landeta (2011), da a conocer que a través de la aplicación de métodos de medición para estudios de mercado, permitió prever y dar a conocer que se pueden tomar decisiones por medio de la incertidumbre, el cual fue aplicado en Cuba debido al surgimiento de la necesidad de crear una oficina el cual le permitiría proteger todas las redes informáticas enfocado en la prevención, evaluación y dar respuestas a las acciones internas o externas relacionadas al funcionamiento de las tecnologías de la informática y las comunicaciones.

Es por esto, que la mejor forma de prevenir en las empresas es implementar sistemas de gestión enfocado en la seguridad de la información cuyo propósito es administrar los recursos y optimizar los procesos, basados en la importancia de la protección de la información, afirmación dada por el Equipo Global de Investigación a Análisis en Latinoamérica sustentada en la revista Vanguardia (Ruiz, 2018). Es necesario la implementación de mecanismos que permitan proteger las informaciones de las empresas, los sistemas y estructura tecnológica, con el objetivo de resguardarse de para que sea expuesta inadecuadamente.

La implementación de normas basadas en la seguridad de la información ha trascendido desde el año 1901, el cual permitió la normalización a nivel mundial a través de la primera entidad conocida como British Standards Institution (BSI, organización británica equivalente a AENOR en España) ISO 27001 (2006). A partir de entonces se generaron evoluciones para la conservación de la información, la primera norma fue enfocada al código de buenas prácticas conocida como BS 7799, desde entonces fueron dando origen a nuevas normas que conllevaran al mejoramiento de una tras otra.

Es decir, la norma anteriormente mencionada fue publicada en el año 1998 en segunda versión de BS-7799 estableciendo específicamente todo lo relacionado al Sistema de Gestión en Seguridad de la Información; desde entonces, ha venido evolucionando, llegando al año 2006 para la publicación de la

ISO 27001/2005, centrada específicamente en la gestión de los riesgos presentada en el manejo de las informaciones dentro de las empresas.

Por consiguiente, los constantes cambios y preocupaciones generadas en las organizaciones por el manejo constante de información y la incertidumbre de saber la existencia de ciertos grados de error considerados como contraproducente para la organización, se van generando a medida del tiempo y según la necesidad, la actualización de la norma ISO 27001. Actualmente, su última actualización fue generada en el año 2015 donde se afianzan las pautas para llevar a cabo la implementación de un adecuado sistema de gestión de seguridad de la información, incorporando novedades que han permitido establecer los estándares para evaluar los riesgos.

Es de esta manera, que la aplicabilidad de procedimientos permite la conservación de información llevando consigo la importación de conocimientos que grandes organizaciones la requieren y se ha creado en base a una necesidad, es por ello, a nivel mundial, se encuentran en la aplicación constante y modernas tecnologías permitiendo estar a la vanguardia con la incorporación de métodos efectivos interviniendo en las estructuras de la tecnología, sosteniendo las transformaciones y el trabajo en equipo las cuales son fundamental dentro de la aplicación de nuevos procesos. Desde el surgimiento de esa necesidad se fue dando origen a las normas para la protección de la información y hacer conocer la existencia de procedimientos, los cuales deben de cumplirse para el mejoramiento de los procesos.

Por lo anterior, los estudios realizados en el Centro de Información y Gestión Tecnológica de Santiago de Cuba sustentan que: “Cuba realiza grandes esfuerzos e invierte considerables recursos, para llevar la informatización a todos los niveles de la sociedad, con el objetivo de mejorar la rapidez del acceso a la información y su organización de una manera adecuada, además, de garantizar la preparación” (Díaz -Ricardo, Pérez del Cerro, & Proenza-Pupo, 2014).

También las grandes compañías a nivel mundial les inquietan las amenazas que existen a nivel virtual, establecen mecanismos los cuales deben de contribuir al aseguramiento de la información manejada internamente. Es por esto donde las compañías de seguridad informática afirman: “los ciberdelincuentes seguirán infectando los sistemas con amenazas para ganar dinero de manera ilegal” (Ruiz, 2018). Por ello, la aplicación de sistemas de seguridad en la información ha trascendido en muchos países donde las grandes compañías a través de la evolución han permitido sustentar lineamientos coadyuvando a la formación de nuevos métodos permitiendo proteger la información, el cual existen normas amparando este tipo de situación y llevar el cumplimiento adecuado de las normas, por ello, poco a poco algunos países han tomado conciencia frente a esta posición.

Es así, como los planteamientos en la informática han permitido analizar las debilidades en la administración de la información teniendo en cuenta la ISO/IEC 27001:2015, teniendo en cuenta que los sistemas cumplen con objetivos enfocados en preservar la información en una empresa; así mismo, se genera la aplicabilidad de nuevo método de investigación para obtener conocimiento valido y confiable para el área de sistemas dentro de la entidad.

Diferentes investigadores realizan aportes con base en las experiencias obtenidas con la implementación de la ISO 27001, entre ellos, Gomez & Alvarez (2012) sustentan dentro de su proyecto de investigación, el cual lo llevó a cabo por medio de la Universidad de España, da a conocer lo siguiente: “la implementación de un buen sistema de gestión obtiene un estado de seguridad y permite la mitigación de los riesgos soportando a un mejoramiento continuo.”

Realizando el análisis de lo anteriormente descrito, para una en una empresa es importante la existencia de un SGSI, con el propósito de identificar los peligros y gestionar los controles para los mismos; como se ha venido mencionado, la NTC ISO/IEC 27001:2015 define la gestión de riesgos como “ las actividades

coordinadas para dirigir y controlar una organización en relación con el riesgo", así mismo, describe el SGSI como aquel procesos dirigido a la conservación de la confidencialidad, integridad y disponibilidad de la información. Al obtener claridad de los conceptos, se hace mención a la exigencia de hacer necesario en las empresas la existencia de personas autorizadas para tener acceso a la información debido al requerimiento de obtener protección de información sea pública o privada.

Por ello, en Latinoamérica y el Caribe, las empresas se encuentran en el constante movimiento y búsqueda de proteger la información de sus empresas, conllevando a la tarea de estar innovando y estar atentos a los cambios ejercidos en la sociedad, por el continuo afán de querer estar a la vanguardia de la tecnología, donde las pequeñas y medianas empresas (pymes) afrontan una problemática grande, donde la mayoría no consignan los recursos necesarios para contrarrestar la ausencia de seguridad y prevención de los riesgos en los activos, generando al final en muchas ocasiones perdidas incalculables.

Por tanto, las organizaciones se han visto en la tarea de adquirir mecanismos de protección informática debido a los sistemas implementados en sus procesos, en algunos casos se generan ciertas fallas, siendo necesario el contar con procesos estructurados y personal especializado y capacitado para manejar los incidentes de seguridad de información (Camelo, 2010). Por lo tanto, dar cumplimiento a los tres enfoques establecidos por la norma generan ventajas que pueden ser competitivas desde el mejoramiento de la imagen corporativa hasta beneficios financieros.

En el departamento de La Guajira, exactamente en el distrito de Riohacha se encuentran conformadas varias empresas ofreciendo variedad de servicios según la necesidad surgida y de tal forma la aplicación de tecnología, independientemente de su actividad económica, los cuales buscan el mejoramiento de la condiciones y servicios de sus clientes y/o usuarios. Con el

transcurrir de los últimos años se ha visto obligado a crear barreras que permitan proteger la información de sus empresas y de las personas.

De acuerdo con lo anterior, de manera puntual las empresas dedicadas al diseño, construcción e interventoras de obras civiles y arquitectónicas brindan las soluciones apropiadas para todo tipo de personas ya se natural o empresarial, por el cual, no son ajenas a los problemas de seguridad de la información por el cual atraviesan las mayorías de las empresas a nivel nacional y mundial. En este sentido, los problemas en los cuales se encuentran hacen referencia a cada una de las características giradas en torno a la tecnología subestimada por medio de la existencia de fallas en los procedimientos sin tener la mínima precaución de salvaguardar la información interna y externa de la empresa.

Independientemente de la manera como es recibida la información, esta debe ser guardada y conservada de la manera más adecuada posible a través de mecanismos de protección; sin embargo, la existencia de fallas en los procesos hace que se genere inestabilidad y limitaciones en los procedimientos requeridos en el ámbito de seguridad para la conservación de la información, por lo tanto las decisiones tomadas por gerencia son de suma importancia para la aplicación adecuada de un sistema que conserve los activos más importante de las empresas.

Igualmente, los problemas que se han generado en los procesos se encuentran vinculados específicamente con la pérdida de información, el cual se considera como la catástrofe a nivel informático. Por tanto, es de gran importancia la aplicabilidad de las políticas de seguridad debido a que su inexistencia a conlleva a la generación de falencias tanto en los documentos generados a diario como para el personal que hace parte de la organización.

La ISO/IEC 27001:2015, recomienda llevar a cabo la implementación de un sistema que conlleve a la gestión adecuada para la generación de seguridad en la información, permitiendo analizar los riesgos generados durante el proceso para

llevar a cabo la identificación y posteriormente tomar las acciones correctivas para todo aquello que se encuentre en peligro dentro de la organización.

La falta de lineamientos enfocados a la seguridad permite la ausencia de control, desinterés del personal de trabajo y la no apropiación de mecanismos para evitar daños a la compañía y ausencia en el mercado, por la deserción de compromiso con la organización y manipulación de información de una manera desconsiderada, dan origen a perjuicios grandes e incalculables totalmente para la empresa a nivel interno y externo, por ello, en estos momentos se puede sustentar en estos momentos la empresa se encuentra dispuesta frente a cualquier amenaza.

Por lo anteriormente expuesto, Magdaniel Ltda., es una empresa dedicada al diseño, construcción e interventorías de obras civiles y arquitectónicas, brindando soluciones apropiadas a sus interesados en el Departamento de La Guajira. En la ejecución de sus actividades recolecta información valiosa tanto para sus clientes como para la organización, por el cual posee cierta estructura informática que permite la interconexión entre cada una de las áreas que la conforman dentro del proceso de transmitir la información relacionada con su actividad económica.

La empresa a través de sus actividades realizadas almacena información valiosa, el cual cuenta con accesos indebido en determinadas redes por el uso de distintos puntos de redes sociales, requiriendo de esta manera fortalecer los elementos que conforman el sistema para la seguridad de la información, detectando fallas relacionadas con la implementación de políticas de seguridad, así mismo, las estrategias de protección d los activos dentro del entorno de la empresa.

En base a lo anterior, es importante analizar las condiciones de la organización, para lograr minimizar los riesgos físicos de la información dentro de los procesos que la relacionan a través del procesamiento, almacenamiento y distribución, concernientes en la utilización de los servicios prestados a los

usuarios, por el cual, la ejecución de la norma ISO/IEC 27001:2015 permite la aplicación de controles dirigidos a garantizar la confidencialidad, integridad y disponibilidad de la información con que cuenta la empresa.

Es importante resaltar que la empresa Magdaniel Ltda., en cierto tiempo llevo a cabo el inicio de la implementación de ciertos parámetros que relaciona al sistema de gestión en seguridad de la información, por motivos de factores internos actualmente no se le ha dado continuidad al proceso por motivos de establecer los lineamientos adecuados basados en la norma y el personal idóneo para llevar a cabo la continuidad del proceso. Por lo tanto, la ISO/IEC 27001:2015 a través de su aplicación demuestra el enfoque hacia una mejora continua, analizando cada elemento que interviene en el proceso de mejoramiento y salvaguardar la información de la empresa.

En consecuencia, con el desarrollo de esta investigación se realizó el análisis del sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda., el cual se pretende con los resultados obtenidos sustentar posiciones que coadyuven al mejoramiento de las funciones y desarrollo de la empresa.

1.1.1. Formulación del problema

Teniendo en cuenta los aspectos mencionados en el planteamiento del problema, se desarrolla el siguiente interrogante que permite estructurar la investigación de la siguiente manera:

¿Cómo está conformado el sistema de gestión de seguridad de la información bajo las normas ISO/IEC 27001:2015 en la empresa Magdaniel Ltda., en el Distrito Especial Turístico y Cultural de Riohacha?

1.1.2. Sistematización del problema

En base a la formulación del interrogante, conlleva a la descripción de las subsiguientes interrogaciones:

- ¿Cuáles son las políticas de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.?
- ¿Cómo es la seguridad física y del entorno de la información bajo la norma ISO/IEC 27001:2015, en la empresa Magdaniel Ltda.?
- ¿Cuáles son los activos de información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.?
- ¿Cómo proponer lineamientos estratégicos para el sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015, empresa Magdaniel Ltda., en el Distrito Turístico y Cultural de Riohacha?

1.2. OBJETIVOS DE LA INVESTIGACIÓN

1.2.1. Objetivo general

Analizar el sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda., en el Distrito Especial, Turístico y Cultural de Riohacha.

1.2.2. Objetivos específicos

- Determinar las políticas de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.
- Definir la seguridad física y del entorno de la información bajo la norma ISO/IEC 27001:2015, en la empresa Magdaniel Ltda.

- Identificar los activos de información, bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.

- Proponer lineamientos estratégicos para el sistema de gestión de seguridad de la información, bajo la norma ISO7/IEC 27001:2015, en la empresa Magdaniel Ltda., en el Distrito Especial Turístico y Cultural de Riohacha

1.3. **JUSTIFICACIÓN DE LA INVESTIGACIÓN**

La importancia de la aplicación de los sistemas de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015, se demuestra su importancia para llevar a cabo su implementación adecuada en la empresa Magdaniel Ltda., permitiendo así conocer las políticas establecidas para el manejo adecuado de la información, evidenciando métodos dirigidos a la seguridad física y de toda la organización, con el fin de salvaguardar la información confidencial de la empresa y de los clientes, dado que teniendo en cuenta los acelerados avances de la tecnología cada vez más los sistemas de información son más vulnerables y podrían ponen en riesgo la estabilidad de la misma.

En este sentido, la empresa Magdaniel bajo la aplicación de la norma permitió manejar la información como el eje principal, por tal motivo es deber de la empresa avalar la confiabilidad, integridad y reserva de la información; por lo tanto, el dirigente es conocedor que la seguridad determinada en la empresa actualmente es restringida e escasa, por ello, se requiere en el desarrollo de esta investigación analizar el estado actual en la compañía.

Por tanto, basado en la seguridad de la información, se permite ofrecer alto nivel en la prestación de servicios basados en la disposición, funcionalidad y habilidad en el manejo de la seguridad, siendo así, la implementación se inclina a la minimización de costos a la organización. Las descripciones anteriormente mencionadas, genera la necesidad de realizar la investigación y dar posibles soluciones a la situación actualmente presentada en la empresa, a través de

interrogantes surgidos por la ejecución de los procesos ejecutados para el manejo y protección de información.

La relevancia social de la presente investigación se encuentra enfocada en ofrecer beneficios para los clientes que hacen parte de ella, puesto que es de suma relevancia proteger la información que se obtiene de cada uno, preservando de tal manera la confidencialidad en el momento de suministrar los datos y minimización de las amenazas en torno a la integridad de los clientes en el momento que dan a conocer información valiosa, lo que permitirá afianzar la relación entre clientes y empresa, obteniendo así mejores resultados-

En cuanto a la justificación teórica, las ideas expresadas por los autores citados en el trabajo como: Díaz - Ricardo, Pérez del Cerro, Proenza-Pupo, Camelo, entre otros investigadores, son tenidas en cuenta como bases teoricas fundamentales para aplicación de todo lo relacionado a las técnicas de seguridad. sistemas de gestión de la seguridad de la información (Sgsi) el cual orienta la perspectiva de este estudio, identificando las dimensiones relacionadas al sistema de información con el objetivo de brindar lineamientos que conlleven a alcanzar el éxito de la empresa, contando con los conceptos suficientes y necesarios para que sea tomado como antecedente investigativo en nuevos trabajos.

La importancia práctica de este proyecto radica en el análisis realizado a la administración sobre el manejo de la información bajo la norma ISO/IEC 27001:2015-sistema de gestión de seguridad de la información en la empresa Magdaniel Ltda., lo cual permitirá incluir mejoras en aquellas variables deficientes, esto implica que en el momento de poner en práctica este trabajo se ejecutarán procesos que permitan proteger toda la información y mayor eficiencia en los procesos.

Por último, esta investigación también adquirirá relevancia metodológica, debido a la adquisición de oportunidad de hacer un estudio serio con la aportación de instrumentos válidos y confiables para llevar a cabo el desarrollo del proyecto

debido a que se encontrará basado en fundamentos teóricos y aplicación de instrumentos que permitirán establecer la confianza y validez de la investigación.

1.4. DELIMITACIÓN DE LA INVESTIGACIÓN

1.4.1. Delimitación temática

La investigación se realizó basados en elementos relacionados con el sistema de información, basándose en la norma ISO 27001:2015 para la obtención de pautas necesarias en el mejoramiento de los procesos dentro del sistema de gestión. De esta manera, el estudio se encontró enmarcado dentro de la línea de ciencia, tecnología e innovación, teniendo en cuenta primeramente los parámetros necesarios para la ejecución de un sistema de gestión en seguridad de la información, por tanto, los soportes teóricos se realizaron con alguno de los siguientes autores:

ISO27001 (2013), Gomez & Alvarez (2012), Correa y Cabezas (2014) MinAmbiente, (2014), MinTic (2016), Ochoa (2016) Peltier (2014), Gomez & Alvarez (2012), Hodeghatta & Nayak (2014), entre otros.

1.4.2. Delimitación espacial o geográfica

La presente investigación se desarrolló en la República de Colombia, en el Departamento de La Guajira, específicamente en la ciudad de Riohacha Distrito Especial, Turístico y Cultural, concretamente en la Empresa Magdaniel Ltda., ubicada en la Calle 13 # 15-91 de esta ciudad.

1.4.3. Delimitación temporal o histórica

La investigación se desarrolló con información recolectada en el segundo semestre del año 2019.

2. MARCO REFERENCIAL

2.1. MARCO TEÓRICO

2.1.1. Antecedentes investigativos

Hacer referencia a parte de antecedentes investigativos conlleva a la descripción de estudios realizados que se encuentran relacionados con la variable en investigación, por ello, en el desarrollo de este ítem sirvieron de base monografías a nivel de maestría y doctorado, los cuales fueron soportes en el cumplimiento de los objetivos estipulado los cuales son descritos a continuación:

Inicialmente, se tiene en cuenta el estudio realizado por Rivas (2017), con el trabajo de investigación titulado *Diagnóstico y plan de acción para la implementación del marco de negocio para el gobierno y gestión de tecnologías de la información (cobit5.0) aplicado a la universidad técnica de Machala*, para optar por el título de Magister en Gestión Estratégica de Tecnologías de la información en la ciudad de Cuenca. El propósito del estudio está orientado en definir un plan de acción de las actividades desarrolladas para la implementación de procesos basados en el diagnóstico inicial en Cobit 5.0. Las dimensiones investigadas lograron establecer planes de acción que conllevaron a la implementación de procesos prioritarios por medio de Cobit 5.0. El sustento teórico estuvo dado por autores como: Putri & Surendro (2015); Network (2011); Bayas (2014); Machado, Sobral & Junior (2014), entre otros.

Metodológicamente en esta investigación, se planteó lineamientos a través del marco de trabajo de Cobit 5.0, basada en tipo de estudio descriptivo y de campo, donde el sujeto de estudio fue de 51 trabajadores al cual se aplicó el cuestionario, así mismo, teniendo en cuenta la observación directa, con el cual se recolecto información para dar un diagnostico basado en seguridad de la

información, siendo estos resultados tabulados fundadas en las dimensiones de política de seguridad, confiabilidad, seguridad de la información, acceso y otros aspectos que conllevaron a la validación obteniendo una confiabilidad del 96% en el coeficiente de Alpha Crombach.

De los resultados obtenidos se demuestra la aplicabilidad de la cascada de metas otorgada por Cobit 5.0, el cual dentro del proceso escoge las preocupaciones de las partes interesadas, posteriormente el proceso es aplicado a las actividades prioritarias, por ende en la Universidad Técnica de Machala en la aplicabilidad del proceso se demostró el cumplimiento de la capacidad de los procesos implementados, a su vez, la valoración y el proceso catalizador se encuentran dentro de los márgenes establecidos.

Las conclusiones de la investigación están dirigidas principalmente en el éxito obtenido con la implantación de procesos a través de Cobit 5.0, logrando analizar las inquietudes generadas en la organización para la toma de acciones que sean ejecutadas a través de actividades que conlleven al mejoramiento continuo de los procesos, por lo cual, la empresa estima las posibilidades de implementar un sistema acorde a las insuficiencias generadas y de esta manera minimizar las posibilidades de exposición de toda esa información importante.

La investigación sirvió como referencia para la compilación teórica en sistemas de información, a su vez en la revisión de antecedentes se extrajo conceptos relacionados con constructos referenciales en seguridad de la información, donde el desarrollo de los lineamientos giró en torno a la tecnología e información pretendiendo obtener aspectos importantes para suministrar información en futuras investigaciones.

Siguiendo en la misma línea de investigación, se analizó el trabajo de Guamán (2015), titulado *Diseño de un sistema de gestión de seguridad de la información para instituciones militares: Escuela Politécnica Nacional*, tesis para la obtención del título de Magister en Gestión de las Comunicaciones y Tecnologías

de la Información, en la ciudad Quito, Ecuador. El proyecto de investigación estuvo orientado al diseño del sistema de gestión de seguridad de la información para instituciones militares, la incorporación de nuevas tecnologías y contribución en la modernización de las instituciones militares. Las dimensiones están encaminadas a la evaluación, estudio y diseño de un SGSI. Las bases teóricas están fundamentadas en: ISO/IEC 27001:2009; ISO/IEC 27001:2005; Hernández (2003); entre otros que sirvieron de apoyo en el desarrollo de la investigación.

A nivel metodológico se trató de una investigación con enfoque cualitativo, de tipo descriptivo, donde el sujeto de estudio fue de 51 empleados que hacen parte del área de tecnológica de la organización, utilizando como técnica la encuesta recolectando información de manera directa; el instrumento aplicado se encontró relacionado con el cuestionario con 69 preguntas cerradas dirigido al personal de la empresa, el cual fue sometido a validación por 5 expertos, obteniendo una validez del 96% de confiabilidad de Alfa de Cronbrach.

Los resultados de la investigación conllevaron a la caracterización de los riesgos, amenazas y vulnerabilidades basadas en requerimientos necesarios por parte de la empresa, de igual manera se permitió la caracterización de los activos de la informa, también se determinó la factibilidad a nivel operativo, tecnológico y económico para poder implementar o diseñar el sistema de gestión de seguridad de la información en las instituciones militares, asignando responsabilidades y compromisos con el SGSI.

Las conclusiones fueron fomentadas en base a los objetivos de la investigación los cuales permiten sustentar que el resultado es la inexistencia de documentos en base a la seguridad de la información y establecer políticas de seguridad inmersas a un sistema de gestión en seguridad de la información, así mismo, requisitos para acuerdos de confidencialidad y el no cumplimiento acceso de usuarios o clientes a información externa a la dirección de tecnologías.

El aporte investigativo, está encaminado a la relación existente entre las variables de estudio, debido al tratamiento aplicado a la misma servirá como base para la realización de la investigación en proceso así mismo, los aportes bibliográficos y la manera adecuada de aplicar la norma ISO 27001, conllevando a establecer puntos de referencia para otro tipo de investigación enmarcada con la variable de estudio.

Así mismo, se tiene el trabajo investigativo de Suarez (2015), llamado *Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización***,** exigencia para obtener el título de Magister en Seguridad Informática, a través de la Universidad Nacional Abierta y a Distancia en la ciudad de Bogotá, Colombia. El estudio está enfocado en la realización del análisis y diseño del sistema de gestión de seguridad informática en la empresa aseguradora. Las dimensiones del estudio están concernidas en la categorización y análisis de riesgos de los activos de información. Sustentado con aportes de los autores Salcedo (2013), Camelo (2010), Pacheco (2014), Cao (2014), De la Cuesta (2015), La norma ISO 27001:2013, entre otros aportes teóricos.

Metodológicamente hablando, fue una exploración de tipo descriptiva con enfoque cualitativo, basadas en referencias literarias junto a la elaboración de matrices de riesgos para verificar el estado real de la empresa dentro del factor de seguridad en la información, realizando entrevista de tipo abierta a los trabajadores de la empresa. Así mismo, las pruebas estuvieron basadas en el cumplimiento de lo establecido por la norma ISO/ IEC 27001:2013.

En los hallazgos se fundamentaron en los datos aportados por los entrevistados, dando a conocer que la empresa, no dispone de un SGSI, debido a la carencia de personal calificado e idóneo para la asignación de responsabilidades dentro del sistema, donde se demuestra la ausencia de

actividades para la protección de los activos u otros aspectos que deben ser cubiertos por la organización.

La investigación permitió evidenciar que los datos conservados por una empresa son de suma importancia, resaltando así mismo, la designación de políticas, roles y responsabilidades son importante en el aseguramiento del éxito dentro de una estructura organizacional bajo los lineamientos que deben ser dirigidos por la alta gerencia, donde todas las personas que hacen parte de la misma, ya sea a nivel interno como externo deben conocer.

El trabajo relaciona con la investigación en curso debido a su aporte extenso en relación a la aplicabilidad de un SGSI junto a la importancia obtenida del mismo; así mismo, los lineamientos y referencias bibliográficas serán tenidas en cuenta para el desarrollo de lineamientos conllevando a una investigación seria y bajo fundamentos reales, las cuales son tenidas en cuenta para el desarrollo de los aportes teóricos de una manera adecuada.

Seguidamente, la investigación realizada por Berrio (2016), titulada *Metodología para la evaluación del desempeño de controles en sistema de gestión de seguridad de la información sobre la norma ISO /IEC 27001* para obtener el título en Magister en Ingenierías de Sistemas, por medio de la Universidad Nacional de Colombia, en Medellín. El objetivo general de la información consistió en desarrollar la metodología para la evaluación del desempeño de los sistemas de gestión de seguridad de la información basado en la norma ISO/IEC 27001. Dentro de las dimensiones estuvo un modelo de evaluación objetiva por medio del método Delphi, la identificación de controles y metodología de la implementación de un SGSI. El desarrollo de la investigación se basó en fundamentos teóricos de los autores Acevedo (2010); Almenara (2014); Broderick (2006); Cronbach (1951); García (2003), entre otros.

Dentro de los aspectos metodológicos, la investigación se consideró de tipo descriptiva con enfoque cuantitativo, permitiendo la elaboración y evaluación de la

eficacia del SGSI. La población de estudio se encontró constituida por 7 personas a los cuales se les realizó un cuestionario de tipo escala de Likert para la definición de una lista de chequeo con el propósito de evaluar los controles relacionados con el método Delphi, obteniendo una confiabilidad del 97% en el coeficiente Alpha Crombach.

Los resultados arrojaron la forma de implementación de un prototipo a través del método Delphi para la realización de controles de riesgo que presentaba el sistema; dando origen al desarrollo de una aplicación llamada ISOWEB, con la intención de ser una plataforma para el análisis de los riesgos latentes en la organización. La valoración de cada uno de los ítems evaluados por los expertos demuestra la necesidad de la existencia de un método que coadyuve a la protección de los datos sistemáticos de una organización.

Las terminaciones obtenidas en el adelanto de la investigación conllevaron a la efectiva ejecución de un sistema de gestión de seguridad de información, por el cual se contó con expertos, los cuales realizaron el análisis para llevar a cabo el desarrollo de controles de riesgos en una organización. El método Delphi sirvió como herramienta para consolidar la información, principalmente en el proceso del análisis de riesgos para la valoración y clasificación de los controles de seguridad. El SGSI requiere estar a la vanguardia de las innovaciones tecnológicas ya que se debe de presentar herramientas metodológicas para la prevención en detención de riesgos.

Esta investigación ayudo en la compresión del estudio de los riesgos presentados a nivel tecnológico y la importancia de implementar un sistema de gestión en seguridad de la información en una empresa, orientando al conocimiento de herramientas necesarias para establecer controles que conlleven a la minimización de los riesgos, así mismo sirve como aporte para las referencias bibliográficas.

En el mismo sentido, se tiene en cuenta el aporte realizado por Espinosa, García y Giraldo (2016), a través de su trabajo de investigación titulado *Sistema de gestión de seguridad de la información para los tres procesos misionales de la corporación autónoma regional de Risaralda,* en la Universidad Autónoma de Manizales para optar por el título de Magister en Gestión y Desarrollo de Proyectos de Software en la ciudad de Manizales, Colombia. El objetivo de la investigación está encaminada a diseñar y desarrollar un Sistema de Gestión de Seguridad de la Información basados en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013; las dimensiones están direccionadas a la gestión de riesgos, adoptar un modelo de mejoramiento y elaboración de diagnósticos. La investigación se basó en normas relacionadas con la ISO. (2005); ISO/IEC 27000, 27001 y 27002; Peltier, T. (2001) entre otros aportes.

Por lo anterior, la metodología manejada para el alcance de los objetivos fue de tipo descriptiva y transversal, con enfoque cuantitativo, la cual se utiliza para la identificación y valoración de las amenazas en el desarrollo del sistema de gestión en seguridad de la información. La recolección de datos se realizó mediante información obtenida directamente en la empresa; aplicando el instrumento del cuestionario conformada con preguntas cerradas y la técnica de la entrevista. El instrumento se sometió a validez de expertos con una confiabilidad del 97.6% de Alpha Crombach.

Los resultados de la investigación permitieron determinar la situación real en referencia a la seguridad de la información, reconociendo a través del proceso que todas las partes se involucrarán en la implementación del SGSI, de tal manera, por medio del análisis e identificación de riesgos se haya establecido a profundidad los aspectos más vulnerables en la entidad y la búsqueda de la mejor forma de mitigarlos, por medio de herramientas e implementación de un SGSI según la necesidad requerida.

Las conclusiones de la investigación lograron dar a conocer la importancia de implementar un SGSI basada en la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013, lo cual es importante la verificación de los niveles de seguridad de la empresa que conlleven a fortalecer la protección de la base de datos de las personas que hacen parte del proceso misiones en la corporación, verificando así, los niveles de seguridad que se debe de implementar.

Los aportes referenciados para la investigación serán de gran beneficio debido a la utilización de herramientas que conlleven a la mitigación de riesgos en el sistema de información en una organización, estableciendo mecanismos que serán tenidos en cuenta para la investigación debido a que conllevan a establecer lineamientos para el análisis e identificación de los riesgos que se presentan en el desarrollo e implementación del SGSI.

2.1.2. Fundamentos teóricos

Hacer referencia a fundamentos teóricos en una investigación permite el desarrollo de conceptos relacionados con una variable en estudio junto a sus dimensiones e indicadores que la conformen, esto es realizado por medio de bases teóricas sustentadas por constructos que a través de sus postulaciones conllevan a la descripción de conceptos adecuados para la investigación. Por lo tanto, el estudio se está fundamentado en todo lo referenciado al sistema de gestión en seguridad de la información bajo la norma ISO/IEC 27001:2015, en la empresa Magdaniel Ltd., sirviendo de soporte dentro de los resultados obtenidos.

2.1.2.1. Sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015

Dentro del área de informática existen riesgos que han ido evolucionado, por el cual, Gutarra (2016) da a conocer que las organizaciones deben afrontar agresiones relacionadas con la navegación y riesgos de ataque informativo, donde los accesos no autorizados al sistema y aplicaciones para dañar los recursos

informativos, por lo cual deben de existir procedimientos enmarcados o dirigidos a la protección de la información de una empresa u organización.

El SGSI está conceptualizado según Cadme & Duque (2012) para trabajar en diferentes tipos de organización. Dentro del contexto la ISO 27001:2015 establece que el sistema de gestión de seguridad de la información es considerado como el conjunto de lineamientos inclinados la prevención de riesgos que conllevan al desarrollo de peligros relacionados con la pérdida o robo de información dentro o fuera de la organización.

De la misma manera, el Instituto Colombiano de Normas Técnicas y Certificación (2013, pag.4) define el sistema de gestión de seguridad de la información según la Norma ISO/IEC 27001 (2015): “Esta descrita como la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad y fiabilidad”.

Así mismo, Gómez & Álvarez (2012) señalan al SGSI como al aquel conjunto de elementos que conllevan a la protección de todos aquellos activos informáticos pertenecientes a una organización, teniendo en cuenta todos los riesgos existentes dentro del proceso. De esta manera, los objetivos planteados por una empresa dentro de la implementación del sistema deben de atribuir a la aplicación de controles para la mitigación de peligros y de esta manera la implementación arroje resultados satisfactorios.

De igual manera, Moncoyo & Marco (2012) dan a conocer el concepto de Sistema de Gestión de la Seguridad de la Información como aquel esquema integral comprendido por políticas, distribución organizativa, recursos necesarios y procedimientos para la implantación de una buena gestión en todo lo referente a la seguridad en la información dentro de la organización. Mirando de esta forma la posibilidad de reducción de los riesgos que se puedan llegar a generar o implementación de controles en aquellos que ya existen.

De acuerdo con los constructos, se describe que el SGSI dentro de una empresa debe ser utilizado bajo los lineamientos que conlleven al mejoramiento continuo de los procesos y accesos a la información, controlando de esta manera el ingreso de personas estableciendo términos en la autorización, siendo asi (Gómez & Álvarez 2012, ISO 27001, 2015 y Moncoyo & Marco, 2012), se encuentran dentro de la misma línea conceptual sustentando que el sistema de información debe ser la herramienta eficaz dentro de los procesos de la organización.

Es de esclarecer, que los conceptos que giran en torno a seguridad de la información son muy escasos, debido a que todo lo necesario e importante para el desarrollo de cualquier actividad que este enfocado a un sistema de gestión en seguridad de la información se encuentra de la norma ISO/IEC 27001, por lo tanto con su última actualización realizada en el año 2015 se sustenta de manera general, la seguridad de la información como el mecanismo abordado de medidas preventivas que reactiva a las empresas para dar protección a todo tipo de información en el cual no pueda tener acceso los agentes externos.

Actualmente, todo tipo de organización se encuentra en constante vulnerabilidad ante cualquier agente externo que tenga acceso a información que solo le compete como empresa, generando de esta manera riesgos frecuentes a sus sistemas informativos y por lo tanto si no se toman las medidas pertinentes, se convertirá en una amenaza constante.

El sistema de gestión en seguridad de la información (SGSI) establece y gestiona a través del ciclo PHVA (Planear, Hacer, Verificar, Actuar), donde Cadme & Duque (2012) lo definen metodológicamente como el proceso que demuestra el cumplimiento de un ciclo conformado por 4 aspectos inclinados a la medición de acciones descritas por la organización basadas en la ISO 27001:2015 basados en la siguiente definición:

- *Planear*: se describe como la fase inicial de todo proceso; en el caso específico del SGSI permite la descripción de las políticas basadas en la seguridad teniendo claro los objetivos los cuales deben ser medibles por la organización, así mismo, se lleva a cabo la definición de actividades metodológicas para la minimización de riesgos asociados a la protección de la información y/o activos de la empresa.

- *Hacer*: la segunda fase es la implementación de todo aquello que se encuentra planeado en la primera etapa, aplicabilidad de los procedimientos, mediciones, asignación de responsabilidades y seguimiento a las actividades.

- *Verificar*: implica el proceso de corroborar los resultados generados a través de lo anteriormente implementado, si realmente las acciones tomadas dentro del sistema en base a las actividades y los riesgos relacionados son acordes con los objetivos y políticas establecidas para la obtención de resultados positivos.

- *Actuar*: el actuar está relacionado con tomar las acciones correctivas y/o preventivas frente a aquello que no se obtuvieron resultados favorables para la organización en la aplicación del SGSI.

2.1.2.2. Políticas de seguridad

Enfocarse en la definición de políticas de seguridad inclina hacia distintos dentro ámbitos a nivel empresarial, según la necesidad generada o la actividad económica de la empresa; por tanto, el desarrollo de la investigación tiene en cuenta aportes teóricos basados en la seguridad de la información definiendo las necesidades presentadas dentro del grupo de interés.

Frente a esto, Correa y Cabezas (2014) hacen referencia a la política de seguridad como aquella que se encuentra expresada dentro de un pliego la

consignación de reglas para llevar a cabo el desarrollo de un marco bajo actuaciones que conlleven a proteger la información de una empresa, el cual debe ser adaptada bajo las características principales de la organización.

Por su parte, el MinAmbiente (2014) define las politicas de seguridad de la información como aquel mecanismo para la protección de activos pertenecientes a la organización, las cuales deben encontrarse alineadas con los objetivos, para la riesgo minización de riesgos relacionados con perdidas financieras, robos y acceso indebido.

Seguidamente, el Min TIC (2016) establece la política como el conjunto de directrices inclinadas al amparo de los activos de la información en la compañía; donde el propósito debe relacionarse con los objetivos de seguridad, garantizando mejora continua dentro de los procesos para definir, documentar e implementar compromisos basados por la Alta dirección.

Por último, Stewart (2012) instituye la política de seguridad como un "documento que define el alcance de la necesidad de la seguridad para la organización y discute los activos que necesitan protección y el grado para el cual deberían ser las soluciones de seguridad con el fin de proveer la protección necesaria". De esta manera, la política se encuentra reflejadas en la identificación de las áreas críticas representados en los activos para que puedan ser protegidos.

Cada uno los constructos formulan la importancia que tiene el establecer políticas de seguridad en la información dentro de una empresa, debido a la existencia de agentes que pueden atentar contra la integridad y el buen nombre de la empresa. Cada uno de los componentes de la organización debe de tener conocimiento de las políticas, para dar el respectivo cumplimiento de estas.

En síntesis, se establece que las políticas de seguridad de la información son de representación necesaria para el personal vinculado a la empresa, proceso y nivel organizacional en el que se encuentre, debe de tener claridad acerca del

funcionamiento de la empresa y consigo los mecanismos que ayuden a la mitigación de los riesgos que afronte la información de la organización. Por lo tanto, las políticas de seguridad deben de encontrarse relacionada con los objetivos de seguridad para que de esta forma se pueda responder la manera adecuada frente a la situación expuesta.

2.1.2.2.1 Objetivos de seguridad

Cuando los objetivos se encuentran enfocados hacia la seguridad de la información deben de cumplir específicamente con analizar y gestionar los riesgos basados en los procesos ejecutados en una organización los cuales deben ser controlados para que la información no se vea expuesta a cualquier tipo de amenazas generadas interna o externamente. Por lo anterior, existen autores que demuestran sus postulaciones frente a la definición de objetivos de seguridad.

Inicialmente, Mejía & Lopez (2015) mencionan que: “el objetivo de la seguridad se encuentra enfocado en la protección de los datos mismos y tratar de evitar su pérdida y modificación no-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo más requisitos como por ejemplo la autenticidad entre otros”, por tal motivo hace conocer que la seguridad informática, “consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización”

En el mismo sentido, Laudon & Laudon (2012) consideran que los objetivos de la seguridad deben de garantizar la integridad, disponibilidad y confidencialidad de la información de una organización en un sistema. Dentro del mismo punto de vista se encuentra el concepto de Rodriguez (2018), dando a conocer que los objetivos de la seguridad se encuentran enfocados en establecer mecanismos de

control para los datos que se manejan dentro de una entidad, basados en la disponibilidad, confidencialidad e integridad. En la misma línea, la ISO 27001:2015 establece que los objetivos deben de analizar y gestionar los riesgos basados en los procesos que relacionados con la organización sometidos al sistema de información.

Con las postulaciones anteriormente mencionada se demuestra que el objetivo de la seguridad de la información es claro, debido a que los tres autores Laudon & Laudon (2012), Rodriguez (2018), ISO 27001:2015 coinciden en que la información debe ser protegida y cumplir con aspectos relacionados con la integridad, disponibilidad y confidencialidad, fijando posición en referencia a los procedimientos que deben llevarse a cabo para el cumplimiento de los objetivos en el entorno donde se desarrollan la actividades y se maneja la información de la empresa.

Teniendo claro el concepto de objetivo de la seguridad se concluye que es considerado como el conjunto de herramientas que deben de proteger la información de una empresa mediante mecanismos interactuados con la política de seguridad; el cual debe de encontrarse enfocado establecer medidas que conlleven al mejoramiento continuo de los procesos permitiendo que los objetivos sean alcanzables y medibles para cada uno de los miembros de la organización.

Los objetivos de la información cuentan con las siguientes características para una adecuada implementación dentro de la organización, los cuales se deben de encontrar basados en la ISO 27001:2015. Debido a que el sistema de gestión de la seguridad de la información en el establecimiento de sus políticas debe de cumplir con ciertos objetivos los cuales presentan características fundamentales comprendidas en diversos aspectos el cual tiene como finalidad la protección de la información y evitar ponerla en riesgo, por lo cual Cadme & Duque (2012) describen tres aspectos importantes dentro de la ISO 27001:2015

Confidencialidad: es el proceso en el cual se garantiza la seguridad de una información en el momento que es suministrada, impidiendo la divulgación a personas u organizaciones sin autorización; buscando con ello que solo puedan acceder ciertas personas o la gerencia.

Integridad: es el procedimiento implementado por las empresas para la conservación de todos los datos que se encuentra relacionados con los usuarios, buscando la conservación y evitar el manejo inapropiado por parte de personas inescrupulosas.

Disponibilidad: es aquella descrita como la condición para acceder a información importante para la organización a través de la utilización de herramientas y equipos adecuados que conlleven a garantizar la optimización de los procesos previniendo los ataques a nivel informático.

2.1.2.2.2 Roles y responsabilidades

Las responsabilidades de seguridad de la información para los diferentes cargos que hacen parte de la organización, deben de estar sometidos a procesos, mejoramiento continuo y capaz de dar cumplimiento de las normas o políticas de la empresa. Por tanto, es de gran importancia conocer los diferentes fundamentos teóricos relacionados la seguridad en el recurso humano.

Al respecto, Rodriguez (2018) establece que una de las principales claves de seguridad la determina los niveles de control de acceso en los recursos humanos, debido a que en la base de datos se almacena toda la información de los empleados, por lo tanto los niveles de control no solo deben de efectuarse en el momento de ingreso del personal sino también de los acceso por fuera de la aplicación, por el cual las herramientas de programación con conexión a las bases de datos y herramientas deben de definir los perfiles de acceso los cuales son restringidos y con auditoría activada para hacer trazabilidad en los procesos.

Seguidamente, dentro de la ISO 27001:2015 hace referencia a las responsabilidades como aquellos lineamientos para asegurar que el sistema de gestión de seguridad de la información cumpla con todos los requisitos, permitiendo ser monitoreado por personas designadas para ejecutar las funciones y ser informado a la alta dirección. Es por tanto, que la organización debe incluir discreciones de seguridad de la información a través del mandato en los recursos humanos, donde la seguridad debe de contar con la elección, compromiso, capacitación de empleados y salida de la empresa.

Según Laudon & Laudon (2012) el objetivo de la seguridad de recursos humanos busca que los empleados, contratistas y terceros entiendan sus responsabilidades y la conveniencia para los roles desempeñados, para recudir así el riesgo de robo, fraude o el mal uso de las instalaciones, explicando antes de realizar el trabajo las responsabilidades frente a esta y firmando una constancia de sus responsabilidades.

Los conceptos relacionados con los roles y responsabilidades frente aún sistema de gestión de la seguridad de la información se encuentran ligados en cada una de las postulaciones de los autores, donde el objetivo principal es proteger la información y llevar a cabo el desarrollo de procedimientos con el recurso humano que permita proteger la información, por medio de controles desde su inicio hasta la finalización del contrato del empleado.

Por ello, se puede decir que la seguridad en los recursos humanos permite el desarrollo de procesos los cuales intervienen desde el momento de ingreso del personal, garantizando la protección de la información de la empresa por medio de procedimientos y confidencialidad, debido a que la información suministrada hace parte de la empresa y por lo tanto debe de ser tratada de la manera adecuada. Por lo tanto, según la ISO 27001:2015 las características de la seguridad de los recursos humano se encuentran basadas en tres fases, las cuales se describen a continuación.

Selección y contratación: para el manejo de la información en una organización se debe de tener en cuenta aspectos relacionados con la designación de responsabilidades, compromiso de confidencialidad, protección de datos, antecedentes, tratamiento adecuado de la información.

Formación de empleados: los empleados deben recibir formación, educación, motivación y conciencia sobre las instrucciones de seguridad y el correcto uso de los recursos de la información. La designación de compromisos recae sobre la organización donde la norma ISO 27001:2015 describe el liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información.

Documentar los roles y responsabilidades: Es de gran importancia documentar los roles y responsabilidades de cada una de las personas que hacen parte de la organización y tienen acceso a información importante, por el cual se debe inicialmente llevar a cabo la descripción de trabajo enfocado directamente en el diseño del organigrama o política de Seguridad de la Información, junto a los procedimientos, planes y otros documentos que designe las funciones dentro de la implementación del sistema bajo la norma ISO 27001:2015.

2.1.2.2.3 Control de acceso

Los controles de acceso ofrecen la posibilidad de establecer mecanismos para la protección de un recurso especifico, por lo cual dentro de un sistema informativo hace parte importante puesto que permite la aplicación de métodos para la mitigación de cualquier riesgo informático o sabotaje en la información de una empresa, por lo tanto, existen postulaciones en referencia al concepto de los cuales se citan los que se encuentran vinculados con la investigación.

Con respecto a lo anterior, García & Alegre (2011) expresa que el acceso son sistemas de contraseñas para entrar a un equipo informático, evitando el ingreso de personas no autorizadas para la información. En el mismo sentido, Laudon & Laudon (2012) dan a conocer que el control de acceso consiste en la

verificación de si una entidad, persona u ordenador solicitando acceso a un recurso tiene los derechos necesarios para hacerlo.

En la misma línea de idea, Peltier (2014) da a conocer que los controles de acceso ofrecen la posibilidad de acceder a los recursos físicos o lógicos de una organización de una manera segura. Para Cadme & Duque (2012), el control de acceso lo determina como el sitio donde deben de estar protegidos de los accesos no autorizados, a través de la aplicación de registros y sistemas tecnológicos. A través de la norma ISO 27001:2015 se establece sistemas de control de acceso que garanticen la manera segura en que se debe de guardar la información, permitiendo ser monitoreados y protección de los recursos y/o activos de la organización.

Los aportes de los autores referenciados anteriormente coinciden en que a través de mecanismos de protección de la información se puede garantizar la protección de todos los activos de la empresa, debido a que la implementación de un sistema de gestión de la información reúne características para la adecuada accesibilidad de la información con controles para que solo personal autorizado pueda ingresar a la información.

De esta manera, se fija posición con García & Alegre (2011), para la presente investigación, debido a que la definición relacionada con el control de acceso sustentado por el anterior autor, conlleva a la realización de cierto analisis para diseñar estrategias que conlleven al aseguramiento de la información en la empresa, para evitar o minimizar cualquier tipo de riesgo generado, el cual puede ser abarcado desde establecer contraseñas y acceso a personal autorizado por la organización.

En otras palabras, los controles de acceso se pueden definir entonces como el dispositivo que tiene como objetivo impedir el ingreso de personal no autorizado logrando establecer mecanismos de protección a la información de la organización; permitiendo actuar de manera eficaz, aprobando o negar el paso a

personas a zonas restringidas de la empresa, con el propósito de hacer frente a las amenazas generadas sobre la información de la empresa.

Las características de los controles de acceso se encuentran basados según la norma ISO 27001: 2015 son aquellas que permiten establecer mecanismos para que las funciones del sistema informativo sean ejecutadas de una manera eficaz, mostrando seguridad en cada procedimiento que se realiza en una organización donde se lleve a cabo la implementación o desarrollo de un sistema de gestión de la seguridad en la información, por lo tanto, se dispone de las siguientes características.

- Instituir políticas para intervenir en el acceso a la información, el cual debe ser documentado a través de obligaciones de la organización y la seguridad de acceso.
- Controlar el ingreso establece un registro de usuarios el cual consiste en la existencia formal del ingreso y/o anulación de interesados con el fin de otorgar y anular el acceso a todos los sistemas de información.
- Restringiendo y controlando la asignación y uso de privilegios
- Establecer uso de contraseñas a través de un proceso normal de gestión
- Establece controles de acceso a las redes evitando los no autorizado, especificando aquellos que si deben de ingresas u obtener alguna información.

2.1.2.3. Seguridad física y del entorno

La seguridad para la información ha crecido mucho en los últimos años, donde las diferentes compañías del mundo están buscando siempre la protección de su información, por el cual, Cadme & Duque (2012), en su investigación describen la importancia de proteger la información de todo tipo de riesgos que constantemente

atentan contra una organización, colocando en peligro aquello que es valioso y que puede ser divulgado de la manera inadecuada.

Según la ISO 27001:2015, la seguridad de la información en el entorno consiste en asegurar que los recursos del Sistema de Información de una compañía sean utilizados apropiadamente y el acceso de información se encuentre disponible controlando las modificaciones posibles por parte de las personas calificadas.

En el mismo orden de ideas, Peltier (2014) señala la seguridad de la información como aquella que se encuentra orientada a proteger una serie de atributos relacionados principalmente con la confidencialidad, integridad y disponibilidad; por lo tanto se debe de evitar las amenazas en las categorías que puedan afectar a las organizaciones, con el propósito de disuadir y prevenir cualquier daño en el ambiente físico.

Por último, Ochoa (2016) aseguran que la seguridad física y del entorno se refiere a la prevención y protección, a través de ciertos mecanismos para evitar que de manera accidental o intencional la transferencia, modificación, fusión o destrucción no autorizada de la información, debido al uso anormal de la información conllevando a la violación de privacidad. Los factores que interceden dentro de la seguridad del entorno logran la determinación de aspectos en el desarrollo adecuado de las actividades relacionada con la seguridad.

De esta manera, los aportes anteriormente descritos conllevan a que exista relación entre cada uno, debido a la similitud encontrada entre cada concepto de seguridad de la información. Es de esclarecer que cada aporte está relacionado con ISO/IEC 27001:2015, ya que la norma es específica en sustentar los términos enfocados al sistema de gestión de seguridad de la información, es así como los autores sustentan sus posiciones.

Se sustenta entonces la seguridad física y del entorno como el mecanismo que debe ser aplicado de forma efectiva para proteger o generar privacidad en la información requerida, manejada a través de la tecnología, en poder evitar que la información no se divulgada, robada, borrada o saboteada, el cual conlleva a la afectación de la disponibilidad y el riesgo generado en una u organización, el cual no es positivo en muchos de los casos.

Las características de la seguridad física y del entorno se encuentran específicamente en poder manipular con gran habilidad la seguridad de la información dentro de las compañías, permitiendo ayudar en la minimización de los riesgos a través del conocimiento y administración de los mismos, que violen la seguridad de la información, por lo tanto, la existencia de dispositivos para verificar los niveles de servicios requeridos.

2.1.2.3.1 Sistemas de protección

Los sistemas de protección pueden ser manejados en cualquier ámbito, pero específicamente en dentro de la protección de un sistema informático, debe de cumplir ciertas características que contribuyan al mejoramiento y minimización de los riesgos existente en la información que posee una organización, por lo cual postulaciones frente al concepto del sistema de protección son descrito a través de distintos constructos.

Inicialmente, Peltier (2014) sustenta que los sistemas de protección relacionados con la información permiten contrarrestar las amenazas o aquello que pueda afectar a la organización. De igual manera, García & Alegre (2011) señalan al sistema de protección como el método implementado por una empresa para evitar accidentes de todo tipo y de tal manera minimizar los posibles riesgos en la infraestructura, equipos o información, los cuales pueden ser causados por incendios, fallas eléctricas o cualquier otro riesgo.

De igual manera la ISO 27001 (2013) dice que los sistemas de protección son utilizando a través de la implementación de barreras físicas y mecanismos de control, empezando a proteger físicamente de las amenazas físicas las cuales pueden ser provocadas por el hombre de forma accidental o voluntaria o bien de factores naturales. En las amenazas provocadas por el ser humano se encuentran las tipo accidentales, como barrado accidental, olvido de la clave. Las deliberadas: como robo de la clave, borrado deliberado de la información, robo de datos confidenciales y dentro de las provocadas por factores naturales se encuentran los incendios e inundaciones.

Es de precisar, cada uno de los autores sustentados mantiene relación en los conceptos dando a conocer que los sistemas de protección cumplen con el objetivo de establecer mecanismos en la protección de la información de una organización frente a las amenazas generadas tanto a nivel interno como externo, el cual puede conllevar a la pérdida total o parcial de los activos, siendo estos de suma importancia a través de aspectos relacionados con los lineamientos estipulados en la norma ISO 27001 (2015).

En síntesis, se define sistemas de protección como aquel diseño que conlleve al aseguramiento de todos los aspectos de la empresa, así mismo la reacción frente a un acto inesperado, por lo cual se debe de estar preparado y proteger todos los activos de la organización, este tipo de sistemas garantizan en gran parte el funcionamiento continuo de los procesos, donde cada uno de las personas que hacen parte de la organización debe tener claridad acerca de los sistemas de protección utilizados para salvaguardar la información.

Por lo tanto, las características de los sistemas de protección se encuentran relacionados estrictamente con la prevención a áreas no autorizadas, daños a la infraestructura, instalaciones o de la información. Por lo cual, su participación se encuentra relacionada con procedimientos estipulados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2016) enfocados en

el control de acceso fisico, protección de activos, retiro de activos y mantenimiento de equipos.

2.1.2.3.2 Áreas seguras

Las áreas seguras se encuentran definidas en distinto ámbito debido a su amplia aplicabilidad, específicamente en la implementación de un sistema de gestión basado en la información, se maneja en un contexto que conlleva a la protección de los datos e información, así mismo el acceso a las distintas estructuras físicas que contiene la organización.

El concepto relacionado con área segura se sustentó inicialmente con la ISO 27001:2015, como aquel sitio donde se maneja información sensible o valiosos equipos informáticos, es decir, el refugio con los que alcanzar los objetivos de la organización. Por lo tanto, dentro del contexto de seguridad se entiende como el sitio donde se alberga cada uno de los servicios que ofrece la organización.

El concepto proporcionado por Camelo (2010), da a conocer que las áreas seguras tienen como objetivo evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización, a través de controles de acceso adecuados por medio de la protección de las áreas. Para el MinTIC (2016), es interpretado como aquel proceso en que la organización define el lugar que debe de cumplir con características específicas que ofrezcan seguridad a los empleados de la organización para la protección de cada uno de los activos que hacen parte del mismo.

Después de los conceptos anteriormente emitidos por cada uno de los autores se establece relación por parte de los constructos puesto que el objetivo final de las áreas seguras, es estipular entorno seguro de la organización para la protección de las instalaciones y de la información, contra cualquier daño o sabotaje, el cual se debe de implementar mecanismos para que los perímetros sean protegidos.

De acuerdo con lo anterior, se fija posición en el concepto emitido por la ISO 27001:2015, determinando de que las áreas seguras conllevan al desarrollo de las actividades de una manera segura donde la información manejada por la empresa debe ser considerada como aquel activo valioso junto con los equipos y todo lo que conforma el entorno, los cuales logran que la organización permite alcanzar los objetivos propuesto.

Al respecto se puede considerar entonces que el concepto de área segura se encuentra totalmente relacionado con aquello que se desea proteger dentro de un entorno en específico, donde personas ajenas a la organización no puedan tener acceso a la información o activos de propiedad privada, definiendo de tal manera el control de acceso con equipos que permitan la realización de la actividad de la mejor manera.

Según la ISO 27001:2015 las características con el cual debe de contar un área segura, es a través de ciertos lineamientos, que se encuentran descritos a continuación: Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado. Trabajo en áreas seguras: se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

Es de esta manera que se debe tener aspectos seguros para la garantía de las áreas, en primer lugar, es necesario que el perímetro debe de adaptarse al contenido del Sistema de Gestión de Seguridad de la Información según la ISO 27001: 2015. Como segundo requisito deben de tenerse en cuenta las seis caras de los tres últimos perímetros, los cuales deben de tener la misma fuerza. Estos se utilizan muy poco para tener paredes solidas si se puede acceder a la habitación a través de un falso techo.

2.1.2.3.3 Valoración de riesgo

Un riesgo puede causar un incidente no deseado que puede generar daño a la organización y sus activos, es decir es una situación en el cual una persona puede hacer algo indeseable o una ocurrencia natural. Por lo tanto, es de suma importancia llevar a cabo la valoración de las amenazas que enfrentan los sistemas informativos o la información importante de una empresa. Inicialmente se tiene el concepto emitido por el Departamento de Seguridad de Informática en la Universidad de Lujan (2014), considera la existencia de aspectos que permiten la valoración de riesgo dentro de una empresa las cuales se obtiene un nivel de daño clasificado de esta manera: nivel de daño (baja, mediana, alta).

De igual manera, Kim & Salomón (2011) consideran que es el potencial donde un intruso o evento explote una vulnerabilidad específica, con la probabilidad que pueda ocasionar un resultado indeseable para la organización o para un activo en específico. Son acciones que puedan causar daño, destrucción, alteración, pérdida o relevancia de activos que podrían impedir su acceso o prevenir su mantenimiento.

Dentro de la misma perspectiva Doria (2014) aporta que es aquel potencial donde un inoportuno o acontecimiento no esperado genere debilidad, con la posibilidad de generar resultado indeseable para la compañía o en un activo específico. Son acciones que puedan causar daño, destrucción, alteración, pérdida o relevancia de activos los cuales podrían impedir su acceso o prevenir su mantenimiento.

Así mismo, MinTIC (2016) considera que el punto esencial para la valoración de los riesgos es permitir determinar primero quien va a sufrir el daño, debido a que el comportamiento y decisiones de la organización deben ser dirigidos por una conciencia responsable para evitar un daño de mayor magnitud. Estimar la magnitud de daño generalmente es una tarea muy compleja. La manera más fácil es expresarlo de manera cualitativa, lo que significa que aparte del daño

económico, también se considera otros valores como daños materiales, imagen, emocionales, entre otros.

Las postulaciones anteriormente mencionadas conllevan a establecer analogías y diferencias debido a que en primera posición López considera que la valoración de las amenazas es muy compleja y debe de ser tratado de forma independiente según sea el tipo de amenaza el cual está afectando; esta posición es contrarrestada frente a las posiciones de los estudios realizados en la universidad de Lujan y Doria (2014) junto al aporte del MinTic (2016), manifiestan que la valoración de las amenazas deben de ser representadas de una manera donde se obtengan resultados favorables para la organización a través de la identificación de las amenazas que conlleven a darle un valor que identifique los niveles en los cuales se encuentran expuestos.

Por lo anterior, la postulación emitida por Doria (2014) logra determinar que todos los procesos se encuentran sometidos a la generación de algún tipo de riesgo, por lo cual es de suma importancia establecer herramientas y estrategias que conlleven a la valoración y mitigación del riesgo, conociendo de la manera apropiada todo aquello que pueda generar perdida en la empresa, evidenciando la forma de contrarrestar los riesgos para obtener resultados positivos en la conservación de la información.

Cada uno de los constructos mantienen posiciones diferentes para valor un riesgo, pero la finalidad de todos los postulados es establecer el grado de amenazas que se encuentra atentando contra la organización para establecer los controles pertinentes. Por lo tanto, se puede establecer que la valoración de riesgos es una herramienta capaz de identificar cual es el grado de la amenaza que afecta a la organización, identificada en los recursos tangibles e intangibles. Conllevando a dar posibles soluciones y establecer mecanismos basados en normas para contrarrestar aquello que no está siendo beneficioso para la

organización, entre los cuales podemos encontrar las amenazas relacionadas con sabotaje, virus informáticos, robo de información, fraudes, entre otros.

2.1.2.3.4 Análisis de riesgo

Cada día va en aumento los casos relacionados con incidentes relacionados con la seguridad en los sistemas de información de una organización comprometiendo de manera directa los activos; por tal motivo se debe de estar alerta y saber implementar de forma adecuada sistemas de seguridad que permitan realizar el análisis respectivo de los riesgos desarrollados en la empresa. El análisis de riesgo tiene como objetivo la calcular e identificar los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

Por tanto, Doria (2014) expresa que “los riesgos se calculan de la combinación de los valores de los activos que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad de que las amenazas y vulnerabilidades puedan causar un incidente”. El análisis de riesgos establece la existencia o no de controles que ayuden a la minimización o eliminación de la probabilidad de la ocurrencia de la vulnerabilidad.

Seguidamente, Gomez (2013) estipula que existen múltiples metodologías para llevar a cabo el proceso de análisis, evaluación y gestión de riesgos informáticos, cada uno con su particularidad y dirigidos a ciertas situaciones. Este tipo de análisis permite estudiar las causas de las amenazas generadas; por ello el análisis de riesgo se considera como la herramienta de gestión en estudios financieros y en la seguridad para la identificación de los riesgos. Dentro de la administración de riesgos el análisis de riesgo es la identificación, evaluación y toma de decisiones para reducir el riesgo a un nivel aceptable.

Ahora bien, para ISO 27001 (2015), el proceso de análisis de riesgos lo considera como el más importante de la gestión de la seguridad de la información de una organización, debido a que desde ahí parte la gestión de los riesgos,

considerándose como aquella que permite tomar la decisión de eliminarlos, ignorarlos, mitigarlos y controlarlos. Considerando que el análisis de riesgo en la información es considerado como un elemento que forma parte del programa de gestión de continuidad de negocio.

Las definiciones anteriormente descritas, permiten establecer la similitud entre cada punto de vista sustentada por cada otro, estableciendo que el análisis de riesgos a nivel informático es el mecanismo necesario para la identificación previa de los riesgos generados, capacidad de respuesta para la ejecución de planes que permitan eliminar o sustituir los riesgos encontrados. Los autores exponen que la implementación adecuada del sistema de información permite salvaguardar la integridad y el buen nombre de la organización.

De esta manera, se resalta el concepto emitido por Doria (2014), el cual permite que en la presente investigación se tenga en cuenta las características que enrolan al análisis de riesgo, conllevando a la descripción adecuada de los activos que representa la empresa, para luego ser valorados los riesgos generados en la manipulación de la información, reduciendo el nivel de impacto en la confidencialidad, integridad y disponibilidad de la información.

En este mismo sentido, se puede definir entonces que el análisis de riesgos es el proceso lógico y por etapas el cual permitirá la aplicación de métodos adecuado en los hallazgos encontrados, para posteriormente realizar la ejecución de procedimientos y tratar los riesgos priorizando aquello que se encuentren afectando a la empresa a nivel interno y/o externo. Para llevar a cabo el análisis de riesgo se debe de contar con las siguientes características definidas por la ISO 27001 (2015) para que el análisis de estos sea ejecutado y verificado de la forma adecuada, teniendo en cuenta, la identificación de las amenazas, vulnerabilidades, controle y activos, determinación de impactos y probabilidad a través del tratamiento de los riesgos.

De esta manera, existen metodologías para poder analizar el riesgo, generando de esta manera, distintas alternativas para que una organización pueda proteger todo lo referente a sus activos informáticos, entre los cuales podemos encontrar: ITIL, COBIT 5, ISO 31000 e ISO 27001, las anteriormente mencionadas son normativas que establecen principios para ejercer control, monitoreo y protección de todo lo que es importante para las empresas.

2.1.2.4. Activos de la información

Las organizaciones hoy día buscan la forma de satisfacer sus necesidades y por ende proteger todo aquello que hace parte de esta, por ello es utilizado el término activo el cual puede ser tangible o intangible según sea la necesidad generada. En el ámbito de seguridad de la información se busca proteger todo aquello que pueda ser atacado de una forma negativa. Por lo tanto, el término de activo de seguridad será sustentado por autores para la validación de su aplicación.

En primera instancia, la norma ISO 27001 (2015) establece que los activos de información es el recurso del sistema de seguridad de la información necesario para que la empresa funcione y consiga los objetivos propuestos en la alta dirección. Los activos se encuentran directa e indirectamente relacionados con las demás entidades de la organización. Seguidamente, basándose en la ISO 27001, MinTic (2016) manifiesta que los activos de información son ficheros, bases de datos, contratos, acuerdos, documentación del sistema software, equipos de comunicaciones, servicios informáticos, entre otros que generalmente generan utilidades y un valor agregado a la organización por el cual se debe de proteger a través de mecanismos eficientes conllevando a resultados positivos.

Por último, Hodeghatta & Nayak (2014) lo consideran como aquel recurso importante para una compañía por el cual debe ser protegido frente a cualquier riesgo que sea generado durante el tratamiento de datos, así mismo, lo describen como aquel aspecto interno y externo que contengan lo realmente valioso que debe ser manipulado por personal calificado.

Con las sustentaciones anteriores, se dan a conocer las semejanzas presentadas entre cada postulación de cada autor, los cuales sostienen que los activos de las organizaciones son aquellos que le dan un valor agregado a la organización y sus procesos, por el cual deben de ser protegidos de la forma adecuada y todo lo concerniente a la parte tecnológica o información de la empresa.

Los activos de información son parte fundamental dentro del funcionamiento organizacional de la empresa, los cuales deben ser considerados como aquel producto que debe de ser tratado y protegido, por medio de la aplicación de mecanismo que pretendan optimizar los procesos evitando que personas o factores inherentes a proceso realicen actuaciones inadecuadas. Por lo tanto, bajo la norma ISO 27001 (2015) los activos presentan características que pueden diferir en el estado, es decir, en la confidencialidad, integridad y disponibilidad, por el cual se pretende sustentar las siguientes características a nivel de activos de información.

2.1.2.4.1 Propiedad de los activos

Hablar de propiedad de los activos hace referencia a una descripción de puntos principales para la clasificación de la información de la empresa, buscando consigo el funcionamiento adecuado de los procesos y dar cumplimiento a lo estipulado en la norma. Por lo cual, la ISO 27001 (2015) considera que las propiedades son todo lo relacionado a los activos asociados dentro del servicio de procesamiento de información designada por la organización.

A través de la MinTIC (2016) describe que las propiedades de los activos se encuentran representadas en la confidencialidad entre las personas, empresa o los procedimientos no autorizados, definiendo cada una de las características que maneje la empresa. Así mismo, Cárdenas (2018) manifiesta que la información y los activos que se encuentren asociados a ella junto al procesamiento generado,

son designados por la organización determinando de tal manera quienes intervienen en el proceso e interactúan con los activos.

Se dice entonces, que cada una de las postulaciones anteriores presenta analogías debido a que cohiciden en que la propiedad de los activos son considerados como aquellas características que logran representar a la empresa y que son designados por la misma, los cuales deben contener cierta protección para la mitigación de riesgos que originen pérdida en la información y fallas en los procesos, por ello es importante la organización en la interacción de los activos.

Por lo tanto, se fija posición en lo emitido por ISO 27001 (2015), debido a que puede ser muy útil asignar a un grupo de activos que trabajen juntos para realizar una función particular. En este caso, el propietario del servicio es responsable de la entrega del servicio, en la que se incluyen todas las funciones de los activos a los cuales provee. De esta manera, las tareas realizadas por rutina tienen que estar delegadas, como las de un vigilante que se ocupa de un activo en una base diaria, aunque la responsabilidad siempre será del propietario del activo.

De esta manera, se considera la propiedad de los activos como aquellos pertenecientes a una organización contando con personas o capital humano idóneo para asegurar la información y todo aquello que se encuentre asociado. Así mismo, defienden y revisan de forma periódica las restricciones en el acceso y las clasificaciones, dentro del proceso el manejo de los activos y propiedades asignadas con responsabilidades dentro del proceso de negocios, estableciendo un conjunto de actividades, mitigación y definición de datos.

2.1.2.4.2 Inventario de activos

Se ha venido manifestando la importancia que tiene los activos dentro de los procesos designados por una organización, lo cual conlleva a establecer parámetros para su fácil identificación y designación de responsabilidades para su

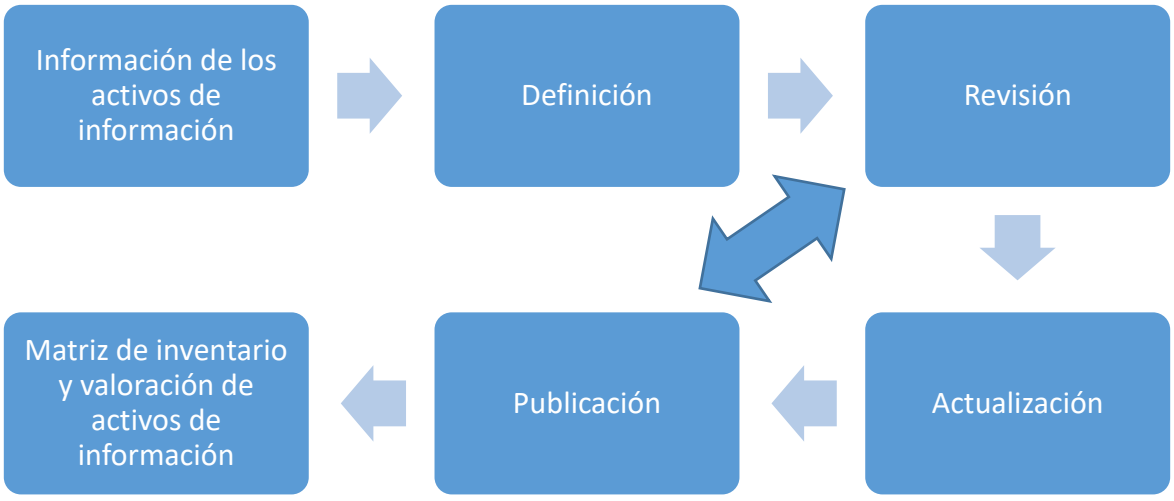
adecuado manejo, es por ello, que el proceso de inventario de los activos implica la aplicación de herramientas para su procesamiento referenciado en la valoración, identificación y clasificación.

A través de lo anteriormente expuesto, la ISO 27001 (2013) define que todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes. La identificación del inventario de activos de información permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

Cárdenas (2018) considera que la realización de un inventario de activos, se debe primeramente tener identificado y posteriormente elaborar y mantener la información importante y adecuada para la empresa en referencia a los activos manejados, indicando el grado de protección por medio de la integridad, disponibilidad y confidencialidad. La última versión de la norma ISO (2015) define, al igual que los anteriores autores, las propiedades de los activos, concluyendo que todo debe encontrarse definido y designado dentro de laorganziación.

Las actividades a realizar para obtener un inventario de activos son: definición, revisión, actualización y publicación, las cuales se reflejan documentalmente en la matriz de inventario y clasificación de activos de información. Así mismo, las características de los activos se encuentran representadas en los siguientes aspectos para hacer valedero su cumplimiento, el cual es descrito a través del MinTIC (2016) basados en la ISO 27001 para establecer de una manera lógica y eficiente el Sistema de Gestión de Seguridad de la Información.

Ilustración 1. Proceso de inventario de los activos



Fuente. Adaptación del Ministerio de tecnología de información y comunicación 2013

2.2. MARCO CONCEPTUAL

La investigación permitió establecer definiciones acerca de términos desarrollados en el documento, determinando su importancia se lleva a cabo el tratamiento adecuado, por el cual se sustenta a continuación conceptos considerados como significativos para el estudio.

Amenazas: son representadas como el riesgo para los activos en la seguridad de la información en general, las cuales pueden ser persistidas al interior o exterior de la organización (Hodeghatta & Nayak, 2014, pág. 31).

Autenticidad: Característica fundamental para una empresa donde la seguridad en la información permite la protección de la identidad de los usuarios o información que caracteriza a la organización (Hodeghatta & Nayak, 2014, pág. 52)

Confidencialidad: Es el proceso inclinado hacia la generación de métodos para la restricción en el acceso a la información, para que no sea divulgada de la manera inequívoca (Hodeghatta & Nayak. 2014, pág. 52)

Disponibilidad: Garantiza el ejercicio del uso adecuado del servicio cuando es solicitado por personas que requieren información (ISO 27001: 2015).

Integridad. Salvaguardar el acceso que conlleve a la restricción o manipulación indebida, modificación o destrucción de la información manteniendo la autenticidad (Hodeghatta & Nayak, 2014, pág. 52)

Vulnerabilidad: es la debilidad del sistema, aplicación o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema (ISO 27001, 2015).

Seguridad: la seguridad debe ser descifrada como el estado subjetivo que permite percibir el desplazamiento dentro de un espacio exento de riesgos reales o potenciales (ISO 27001, 2015).

2.3. MARCO LEGAL

Tabla 1. Matriz legal

Tipo	Nombre	Descripción
Norma	ISO 27001: 2015	Implementación del sistema de gestión en seguridad de la información.
Ley	527 de 1999	Reglamenta el acceso y uso de los mensajes de datos, comercio electrónico, firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley	962 de 2005	Facilitar las relaciones de los particulares con la administración pública.
Ley	1151 de 2007 art 6	Especifica la intención del estado en promover la implementación progresiva del software en las entidades públicas y la inclusión digital
Ley Estatuaria	1266 de 2008	Disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
Ley	1273 de 2009	Dicta disposiciones para preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones
Ley	1450 de 2011 art. 227	Administración de bases de datos de acceso permanente, seguro y confiable
Ley	1450 de 2011 art.	Uso de las tecnologías y comunicaciones ofrecer una oportuna, eficiente y

	232	eficaz prestación de servicio en la gestión de las entidades
Ley	1450 de 2011 art. 230	Establece el cumplimiento de la estrategia de gobierno en línea que será liderada por el Min TIC
Ley	1581 de 2012	Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones
Decreto	1151 de 2008	Reglamenta los lineamientos de gobierno en línea y empieza a implementar la ley anti- trámites.
Decreto	1747 de 2000 art 9	La entidad deberá contar con un equipo de personas, una infraestructura física y tecnológica y unos procedimientos y sistemas de seguridad.
Decreto	2693 de 2012	Definir lo lineamientos, plazos términos para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

2.4. MARCO INSTITUCIONAL

1. Información organizacional

Tabla 2. Información de la empresa

Razón social	Empresa Magdaniel Ltda.
Actividad económica	Diseño y construcción de proyectos arquitectónicos
Sector económico	Sector de la construcción
Tipo de empresa	Empresa privada
Dirección comercial	Calle 13 No. 15-35

Fuente: Suarez, (2019).

2. Reseña Histórica

En el año de 1993, los señores Manuel Magdaniel Pabón y Delay Magdaniel Hernández, Arquitecto e Ingeniero, decidieron asociarse y crearon la Empresa Magdaniel Ltda., la cual en sus inicios se dedicaba a hacer cálculos estructurales y diseños arquitectónicos dados la especialidad de sus socios. Al poco tiempo incursionan en el campo de la contratación en construcción de obras civiles, lo que hacen con mucho éxito.

A raíz de esto, deciden ampliar sus horizontes, participando en licitaciones de todo tipo de obras civiles y de servicios generales. Las labores de prestación de servicios fueron reguladas, en su inicio, el 29 de marzo de 1993 por Escritura Pública No. 398, otorgada en la Notaria Única de Riohacha, inscrita en la Cámara de Comercio el 2 de abril de 1993, bajo el número 1538 del libro IX, se constituyó

la persona jurídica: Magdaniel Ltda. La empresa Magdaniel Ltda., cuenta con una amplia experiencia en la realización de trabajos relacionados con el área de las ingenierías en cuanto a la consultoría y construcción de obras civiles y arquitectónicas con gran reconocimiento en sus proyectos en el Departamento de La Guajira.

Esta experiencia especifica en la prestación de servicios es superior a los dieciséis años, destacándose el significativo crecimiento que ha experimentado en el gremio de los proveedores de servicio en la región principalmente en obras civiles y electromecánicas (edificaciones, colegios, redes hidrosanitario, corredores viales, escenarios deportivos, entre otros), Fundación Cerrejón, Coorpoguajira, Gobernación de La Guajira, Chevron, Alcaldía de Barrancas, Hospital Nuestra Señora del Perpetuo Socorro, Alcaldía de Riohacha, Universidad de la Guajira, INVIAS, entre otras instituciones. Las actividades de prestación de servicios cuentan con el apoyo de los profesionales vinculados a la organización con más de 20 años en el desarrollo de este tipo de proyectos y prestación de servicios, así como personal calificado en varias disciplinas.

3. Plan estratégico de la organización

Misión: Magdaniel Ltda., es una compañía dedicada al diseño, construcción e interventoras de obras civiles y arquitectónicas, brindando soluciones apropiadas a sus clientes en el Departamento de La Guajira; para ello contamos con el compromiso y la competencia de talento humano, el mejoramiento continuo de los procesos y la calidad de nuestro servicio al cliente.

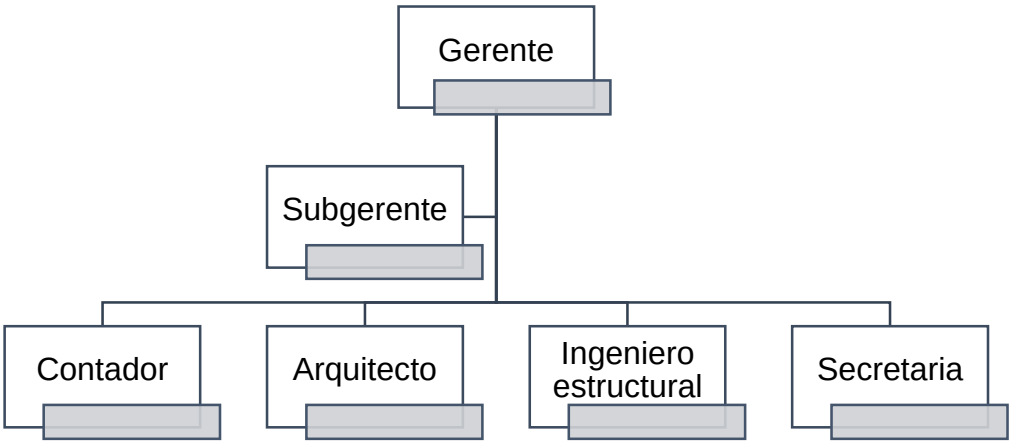
Visión: Magdaniel Ltda. En el año 2021 será reconocida en el departamento de La Guajira por el cumplimiento de los compromisos contractuales y calidad en la prestación de los servicios de Diseño, Construcción e Interventoras de Obras Civiles y Arquitectónicas e incursionará en el sector de la construcción de viviendas. Para cumplir con este propósito se fundamentará en el mejoramiento continuo de la eficacia de nuestro Sistema de Gestión de Calidad, la satisfacción

de las necesidades de los clientes, el fortalecimiento de la competencia del personal, el incremento de la eficiencia administrativa.

4. Organización de la empresa

La organización de la empresa se encuentra estructuralmente identificada dentro de la jerarquía vertical, puesto que es direccionada de arriba hacia abajo siguiendo líneas de mando para la designación de actividades en cada área, definido a nivel general por 7 colaboradores en total.

5.1. Estructura organizacional



Fuente. Suarez (2019), basada en la información de la empresa.

5- Personal

El personal es el conjunto de individuos que conforman a una organización trabajando hacia el cumplimiento de unos objetivos, los cuales ejecutando procesos propios de la actividad económica. De esta manera, en la empresa Magdaniel Ltda., se encuentra conformada por 7 personas designadas con funciones específicas para el cumplimiento de tareas dentro del nivel organizativo, por lo cual en la tabla 3 se describe el personal que conforma a la empresa

Tabla 3. Descripción del personal

CARGO	TOTAL
Gerente	1
Subgerente	1
Contador	1
Ingeniero estructural	1
Arquitecto	2
Secretaria	1
Total	**7**

Fuente. Suarez (2019), basada en la información de la empresa.

2.5. SISTEMA DE VARIABLES

2.5.1. Conceptualización de la variable

En este punto de la investigación conceptualizar la variable de investigación permite llevar a cabo la descomposición en forma ordenada de todos los componentes de estudios, es decir, describir la manera en que se encuentra conformada la variable de estudio, el cual está basada en dimensiones e indicadores los cuales son analizados a través de los objetivos del estudio, por lo tanto, se describe a continuación el concepto de la variable en tratamiento.

Sistema de Gestión de Seguridad de la Información, bajo la norma ISO7/IEC 27001:2015. Se encuentra definida como la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad y fiabilidad.

2.5.2. Operacionalización de la variable

Llevar a cabo el proceso de operacionalizar la variable de investigación se permite a través del diseño de una matriz teniendo en cuenta las dimensiones e indicadores por medio de métodos medibles. En este caso, la variable de investigación está conformada la variable Sistema de Gestión de Seguridad de la Información consta de tres dimensiones y nueve indicadores, donde inicialmente

se despliega la dimensión política de seguridad, el cual consta de los indicadores: objetivos de seguridad, roles y responsabilidades y control de acceso. Seguidamente se encuentra la dimensión seguridad física y del entorno, del cual hace parte los sistemas de protección, áreas seguras, valoración de riesgo y análisis de riesgo. Por último, la dimensión activos de la información comprendida por la propiedad de los activos e inventario de activos.

Tabla 4. Matriz de operacionalización

Objetivo general: Analizar el sistema de gestión de seguridad de la información, bajo la norma ISO7/IEC 27001:2015, en la empresa Magdaniel Ltda., en el Distrito Especial Turístico y Cultural de Riohacha.

Variable	Objetivos específicos	Dimensión	Indicadores
Sistema de Gestión de Seguridad de la Información, bajo la norma ISO7/IEC 27001:2015	Determinar las políticas de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.	Políticas de seguridad. Rojas (2014), MinAmbiente (2014), MinTic (2016).	Objetivos de seguridad
			Roles y responsabilidades
			Control de acceso
	Definir la seguridad física y del entorno de la información bajo la norma ISO /IEC 27001:2015 en la empresa Magdaniel Ltda.	Seguridad física y del entorno ISO27001 (2013), Ochoa (2016), Peltier (2014)	Sistemas de protección
			Áreas seguras
			Valoración de riesgo
			Análisis de riesgo
	Identificar los activos de información, bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.	Activos de la información ISO27001 (2013), Gómez & Álvarez (2012), Hodeghatta & Nayak (2014)	Propiedad de los activos
			Inventario de activos
	Proponer lineamientos para el sistema de gestión de seguridad de la información, bajo la norma ISO7/IEC 27001: 2015, en la empresa Magdaniel Ltda., en el distrito turístico y cultural de Riohacha.	Este objetivo no se operacionaliza. Será alcanzado con el desarrollo de los objetivos anteriores.	

Fuente. Suarez (2019)

3. MARCO METODOLÓGICO

El desarrollo del capítulo tres en el trabajo de investigación permitió la reunión de características para la obtención de resultados, a través del diseño y tipo de estudio, con la variable definida relacionada con el sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015. Obteniendo una población de estudio para comprobar la confiabilidad del instrumento aplicado y análisis de los datos obtenidos por la investigación. Demostrando a través de la teoría de Balestrini (2016) como los metodos de las diversas búsquedas, tecnicas basadas en teorias y mecanismos que conllevan a obtener resultados en entornos reales. Por tanto, la investigación tendrá el adecuado desarrollo alcanzar los objetivos inicialmente planteados.

3.1. ENFOQUE METODOLÓGICO

Dentro de la investigación el enfoque metodológico permitió a través de la variable de estudio relacionada en el segundo capítulo de la presente investigación, por medio de la determinación de los objetivos, plantear estrategias que abordan la investigación el cual se encontrará relacionada con un enfoque cuantitativo, donde a través de sus características que podrán ser aplicada para obtener los resultados adecuados.

La presente investigación tuvo un enfoque cuantitativo, el cual según Bonilla (2011) está definido como aquel proceso de interpretación de resultados numéricos a través de la utilización de estadísticas descriptiva, apoyados en la utilización de instrumentos para el análisis de comportamientos de un grupo en específico. Por otra parte, se cuenta con el aporte de Tamayo y Tamayo (2014), quienes manifiestan que el enfoque cuantitativo investiga el cumplimiento a través instrumentos estadísticos, teniendo en cuenta que es un proceso estructurado

mediante un patrón preciso y predecible que relaciona y conecta sistemáticamente unas etapas con otras.

Las características relacionadas con el enfoque cuantitativo, según Niño (2014), son aquellas que permiten controlar y predecir la realidad, estableciendo las variables, buscando siempre comprobar la hipótesis, predominando siempre el método deductivo con el propósito fundamental de medir magnitudes exigiendo una confiabilidad y validez en la medición, considerando así la generalidad en los resultados y conclusiones.

Por consiguiente, la investigación ocupa un enfoque cuantitativo debido a que los datos obtenidos son procesados a través de procedimientos estadísticos con el fin de verificar y comprobar hipótesis que tienen como soporte teorías por medio de estudios muéstrales representativos, específicamente en el análisis del sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015- en la empresa Magdaniel Ltda.

3.2. TIPO DE ESTUDIO

Referirse al tipo de estudio de una investigación permite identificar los lineamientos que determinan criterios enfocados con el objeto de estudio, nivel de conocimiento y alcance temporal, logrando que el investigador tenga claridad sobre aquello que desea obtener y la manera en que debe ejecutar la investigación. Por consiguiente, la presente investigación está direccionada en el tipo de investigación aplicada, con nivel explicativo y de alcance transversal.

Inicialmente, Bonilla (2011) señala que una investigación es aplicada cuando se tiene fundamentos en los descubrimientos y aportes teóricos, donde el mayor interés se encuentra relacionado con la práctica y la utilización de conocimientos, buscando de tal forma confrontar las teorías con la realidad. En el mismo sentido, Niño (2014) considera que una investigación aplicada siempre se encuentra en la

búsqueda dar soluciones a un problema en específico de forma práctica acudiendo de tal manera a la aplicabilidad de las ciencias y/o teorías.

Las características de este tipo de investigación son señaladas por el autor Bonilla (2011), las cuales son consideradas como aquellas que cumplen una dependencia en relación a los descubrimientos y aportaciones a nivel básico y/o teórico, orientado principalmente a la planificación de métodos para la obtención de resultados en base a los problemas planteados. Por lo tanto, teniendo en cuenta las consideraciones anteriores la presente investigación, siendo aplicada permitió la aplicación y recolección de los datos necesarios logrando establecer mecanismos y estrategias para dar cumplimiento a los objetivos planteados basados en el sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001 en la empresa Magdaniel Ltda.

En el mismo orden, se hace conocer que la investigación obtuvo un estudio de tipo explicativo; para Niño (2014), es visto como el casi que el objetivo final, la meta o la exigencia, ya que busca respuesta a una pregunta fundamental, por el deseo de conocer y saber del ser humano. Por otra parte, Arias (2016) da a conocer que la investigación de tipo explicativa busca las relaciones entre el porque de los hechos ocurridos, asi mismo se encuentra enfocado en la preocupación de analizar las causas mediante la comprobación de las hipotesis, el cual a través de los resultados obtenidos el nivel de conocimiento permite ser mejor considerado.

El tipo de estudio explicativo presenta características que hacen ser representativa en su aplicación, por el cual Mendez (2013) considera que las carácterísticas se enfocan principalmente en la observación y descripción de las fuentes generadoras de nuevos conocimientos permitiendo al investigador ir un poco más allá de su búsqueda mediante la interrelación de los factores de estudio en la formulación de alternativas para el problema.

A través de los conceptos anteriormente emitidos, se estableció actividades que coadyudarón a la generación de eventos logrando describir y explorar sobre la problemática generada, especificamente en la empresa Magdaniel en el ánalisis del sistema de gestion de la información bajo la norma ISO 27001, donde se obtuvieron los datos necesarios a través de la búsqueda de razones para proceder a la valoración del comportamiento de la variable y entender las causas generadas.

El alcance temporal de la investigación es importante relacionar el tiempo, teniendo presente la representación de momentos en que es obtenida la información. En ese orden, se describe la investigación de tipo transversal; definida por Bonilla (2011) como aquella que permite recoger información en base a una población en específica desarrollado en un momento determinado. De igual manera, Bernal (2010) señala que la investigación transversal es aquella en donde se obtiene información directamente de la población o muestra objeto de estudio, lo cual se presenta una única vez en un momento determinado.

De esta manera, se pueden enmarcan las caracteristicas definidas por Bonilla (2011), donde principalmente este tipo de investigación permite la recoleccion de datos de estudio de la variable en un solo momento, para luego describir el comportamiento de la misma, estableciendo su relación con el medio donde es investigado de tal manera que permita obtener resultados que conlleven a los resultados. Por consiguiente, el desarrollo de la investigación permitió la definición de objetivos a cumplir, teniendo en cuenta los aportes teóricos sustentados por los autores relacionados con la variable de estudio Sistema de Gestión de la información bajo la norma ISO 27001, el cual se procedió a la recolección de datos en la empresa Magdaniel Ltda., en un tiempo determinado, con el propósito centrado en analizar la variable y su incidencia.

3.3. DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación se encuentra estrechamente relacionada con el orden desarrollado en la investigación, es decir, se deben de establecer estrategias para que sean implementadas en el proceso el cual se encuentra dividido por etapas, permitiendo constatar los hechos con las teorías, determinando a través de las estrategias las operaciones necesarias para la realización de la investigación y su ejecución final; en este caso en específico, se cuenta con el diseño de investigación de tipo no experimental y de campo.

Inicialmente, se describe el diseño no experimental a través de la postulación de Palella & Martins (2012) definido como el proceso realizado sin llevar a cabo alteraciones sobre la variable en investigación, dentro de un tiempo real es analizado el comportameinto para posteriormente ser examinadas. De igual manera, Hernández, Fernández & Baptista (2014) hacen referencia a la investigación no experimental como aquella en que no es manipulada la variable de una forma deliberada y solo se observan los fenomenos en su contexto original para analizarlos.

Las características enmarcadas en el diseño no experimental están descritas por Bonilla (2011) no requieren de la manipulación debido a que todos los hechos ocurridos son estudiados en su ambiente natural, donde el procedimiento es indicado para las investigaciones de carácter social a los que deja en libertad de actuar de manera espontánea bajo condiciones de observación.

En función de lo anteriormente expuesto, la investigación se llevó a cabo en un tiempo en específico, donde se acudió a la empresa Magdaniel Ltda., y se localizaron a los trabajadores en general llevando a cabo la aplicación del instrumento para la evaluación de la variable de estudio relacionada con el sistema de gestión en la información bajo la norma ISO 27001 del 2015, analizando cada uno de los indicadores para establecer comparaciones y el comportamiento de estas.

Por otro lado, la investigación de campo es considerada por Palella & Martins (2012) como aquella que reside en la obtención de fundamentos solamente de la realidad, sin manipular o controlar la variable. En el mismo sentido, Arias (2016) define la investigación de campo como el proceso de recolectar información en una población en especifíca. Asi mismo, considera que dentro de la investigación se debe de tener en cuenta lo datos secundarios los cuales proceden de fuentes bibliográficas que permite la elaboración del marco teórico.

Las características del diseño de campo, según Bonilla (2011), enrrolan principalmente la experticia del investigador y la creatividad en el acopio de la información cerciorandose de las verdaderas condiciones en que se obtienen los datos, las cuales deben ser recaudadas directamente de la fuente para proporcionar mayor confianza en el conjunto de la información obtenida, logrando comparar resultados entre la realidad y lo esperado.

En el desarrollo de la presente investigación se obtuvo información directamente de la fuente, especificamente en la empresa Magdaniel Ltda., el cual permitió recolectar información suministrada por los trabajadores con la aplicación del instrumento cuestionario, recolectando los datos necesarios en la totalidad de la población por medio de las variables y dimensiones descritas en el estudio.

3.4. FUENTES DE RECOLECCIÓN DE DATOS

Las fuentes de recolección de datos indican el lugar, objeto o persona de donde se obtendrá la información pertinente para la investigación, donde es importante la comprensión de los hechos obtenidos a través de fuentes primarias y secundarias, las cuales deben de encontrarse totalmente relacionadas con los indicadores. Por lo cual, Sabino (2013) establece que son los métodos o estrategias que han de servir para la ejecución del trabajo, donde se hace necesario abordar las formas y procedimientos concretos que permita recolectar y organizar las informaciones que sean necesarias.

Por otra parte, Niño (2014) sustenta que el proceso de recolección de datos depende en gran medida, no solamente de las técnicas escogidas, sino tambien del problema, el objetivo, la muestra seleccionada, la hipotesis y la variable escogida junto a sus dimensiones e indicadores, para que la búsqueda de la información conlleve al cumplimiento de los objetivos y el desarrollo de la investigación de manera óptima.

Con las postulaciones anteriormente mencionadas, en el desarrollo de la presente investigación las fuentes de recolección de datos para la investigación relacionada con el objetivo de analizar el sistema de gestión de seguridad de la información, bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda., serán tomadas en base a la recolección de información primaria e información secundaria.

3.4.1. Información primaria

Las fuentes de información primaria permiten al investigador recolectar la información necesaria en el objeto de estudio, el cual debe suministrar los necesarios para su posible interpretación, con el uso adecuado de técnicas o instrumentos para la extracción suficiente de la información relacionada con la variable de estudio.

Es, por lo tanto, que Niño (2014) describe a la información primaria como aquella que el investigador extrae en contacto directo de la realidad. De igual manera, Sabino (2013) considera que los datos primarios son aquellos donde el investigador los extrae directamente de la realidad, recolectándolos con sus propios instrumentos, es decir, son los datos que el investigador recoge en contacto con los hechos que investiga.

De acuerdo con Méndez (2013), la principal característica de las fuentes primarias de información es que todo lo que se necesita para la investigación es recolectada directamente del objeto de estudio, lo cual implica definir unas

técnicas e instrumentos adecuados para tal fin. De la misma manera, permite determinar el objeto de investigación, donde es necesario seleccionar la unidad a la cual se aplicará el instrumento.

La fuente de información primaria utilizada para esta investigación se basó principalmente en la aplicación del instrumento conocido como cuestionario, el cual permitió el análisis de la variable relacionada con el sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015. Esta técnica de recolección de datos se consideró como método confiable para obtener resultados en el desarrollo de la investigación.

3.4.2. Información secundaria

Las fuentes secundarias hacen referencia a todo lo referenciado a textos, libros, tesis, artículos, entre otros mecanismos que permiten afianzar los conocimientos y resultados obtenidos a través de las fuentes secundarias primarias. Es por ello, que se considera importante dentro del proceso pues sirve de apoyo en todo lo referente a la parte teórica, ampliando de tal manera el contenido de la información en referencia a la variable en estudio.

De esta manera, Sabino (2013) establece que las informaciones secundarias son búsquedas que provienen también de una relación con la práctica, pero que ya han sido procesados por otros investigadores. Así mismo, Niño (2014) define los datos secundarios a través la obtención de ciertas mediciones para una adecuada intervención, es decir, han sido ya recogidos y tratados por otras personas y se hallan de alguna manera almacenados.

De esta manera, las características de este tipo de fuente se encuentran definidas por Bonilla (2011), como aquellas que permiten explorar o emprender un proceso investigativo conduciendo al logro de objetivos significativos, que conllevan a la solución de un problema, a través de la revisión documental en

forma escrita bien sea con palabras o imágenes, logrando encontrar información preciada sobre el tema investigado.

Por lo tanto, la investigación se basó en la recolección de información por medio de la utilización de las fuentes secundarias proveniente de fuentes bibliograficas, como libros, tesis, documentos oficiales, artículos, asesorías de expertos y director de tesis con información referente a la variable de estudio sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015.

3.5. POBLACIÓN

La identificación de la población es base fundamental en la investigación debido a que se permite centrar el estudio en un punto específico, para la validación de lo anterior se tiene la teoría sustentada por Balestrin (2016), el cual define a la población como un conjunto finito de personas, casos o elementos que presentan características en común. De igual manera, Hernández, et at (2014), dan a conocer que la población es un conjunto de características similares dentro del fenómeno a estudiar, obteniendo de allí los datos necesarios para la investigación.

Las características que debe de cumplir una población de estudio según Tamayo y Tamayo (2014) es que debe reunir elementos similares para la realizacción del estudio, logrando establecer la totalidad del fenomeno investigado, donde las unidades de la población cuenta con particularidades en común siendo estás observables, las cuales deben estar relacionadas con la unidad de estudio junto a todo los posibles puntos a investigar.

Por lo tanto, teniendo en cuenta lo anteriormente expuesto, la población de estudio se encuentró enfocada en los trabajadores de la empresa Magdaniel Ltda., logrando analizar el sistema de gestión de la información bajo la norma ISO 27001:2015, detallada en una totalidad de 7 trabajadores, donde el recuento de individuos se realizó a través de un censo poblacional el cual tiene como objetivo

determinar el número de personas que conforman el grupo de trabajo. De igual manera, se determinó que no es necesario realizar muestreo, ni aplicación de formulas ya que el número de individuos dentro del estudio no excede las 100 unidades.

3.6. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

La recolección de la información es un proceso planeado paso a paso, para que de forma coherente se puedan obtener resultados que contribuyan favorablemente al logro de los objetivos propuestos. Si en el proceso investigativo, la obtención y recolección de la información no se realiza siguiendo un proceso ordenado y coherente, que acceda a evaluar la confiabilidad y validez tanto del proceso mismo como de la información recolectada, ésta no será relevante y por lo tanto no podrá reflejar la realidad social que se pretende describir, por lo cual se utilizó como técnica la encuesta y el instrumento fue el cuestionario, teniendo en cuenta que la presente investigación tiene un enfoque cuantitativo.

Para la validación de lo anteriormente mencionado, se tiene el aporte realizado por Hurtado (2012), indicando que la recoleccion de información permite dar respuesta al enuciado o pregunta de investigación, en consecuencia para alcanzar tanto el objetivo general como los especificos, haciendo referencia a modos especificos de realizar las cosas paso a paso en el desarrollo del metodo a utilizar. De igual manera, Arias (2016) señala que la técnica de recolección de datos representa el conjunto de procedimientos utilizado para la obtención de información en el logro de los objetivos de la investigación.

Teniendo claro los conceptos relacionados con las técnicas e instrumentos de recolección de datos, en la presente investigación se tuvo en cuenta la aplicación del cuestionario, el cual fue aplicado de la manera apropiada sin ningún tipo de manipulación para no presentar falla en el proceso o alteraciones en los resultados que pudieron haber afectado la investigación, es así como se obtuvieron los resultados apropiados para alcanzar los objetivos propuestos.

De esta manera, se define el cuestionario según Bonilla (2011) como aquel que puede suministrarse en forma impresa o virtual, donde el investigador consigna una serie de preguntas que demandan del investigado una serie de respuestas necesaria para el trabajo sobre el cual está indagando. El cuestionario de la presente investigación fue diseñado para una encuesta, el cual contó con unas características que permitieron obtener mejores resultados en la investigación. Las preguntas del instrumento del cuestionario estuvieron diseñadas a través de la escala o gradación, según Bonilla (2011), “son aquellas que permiten medir las variables de estudio” (p.209). Por lo tanto, se tuvo en cuenta la escala de Likert para la medición del grado de interés o actitud de una persona respecto a una variable.

Las afirmaciones presentadas en el instrumento estuvieron establecidas por categorías, las cuales son cinco (5) alternativas de respuesta donde el sujeto debe de elegir y marcar solo una opción distribuida de la siguiente manera: Totalmente de acuerdo (5) De acuerdo (4) Neutral (3) En desacuerdo (2) Totalmente en desacuerdo (1). Se llevó a cabo el proceso de calcular la puntuación de la escala de Likert, los cuales son sumados los valores alcanzados en cada afirmación.

El resultado de la puntuación pudo considerarse alto o bajo según el número de afirmaciones obtenidas. Igualmente, cuando el formato es diligenciado por varias personas, el resultado de la puntuación será igual a la suma de los promedios de cada alternativa o afirmación. Este instrumento fue aplicado en los trabajadores de las distintas áreas de la empresa Magdaniel Ltda.

Tabla 5. Valores Escala de Likert

ALTERNATIVAS DE RESPUESTAS	CODIFICACIÓN
Totalmente de acuerdo (**TD**)	5
De acuerdo (**DA**)	4
Neutral (**N**)	3
En desacuerdo (**ED**)	2
Totalmente en desacuerdo (**TD**)	1

Fuente: Suarez, (2019).

3.7. VALIDEZ Y CONFIABILIDAD DE LA INVESTIGACIÓN

3.7.1. Validez del instrumento

La selección o el diseño de un instrumento son importantes para el desarrollo de la investigación, donde se puede cerciorar que ciertamente se encuentra midiendo las características del objeto de estudio. Por lo cual, la validez, para Sabino (2013), indica la capacidad de la escala para medir las cualidades para las cuales ha sido construida y no otras parecidas. Una escala confusa no puede tener validez, lo mismo que en una escala que esté midiendo, a la vez e indiscriminadamente, distintas variables superpuestas. De igual manera, Bonilla (2011) señala que la validez permite la evaluación de cada uno de los indicadores que contiene el instrumento con el cual se pretende medir las variables de investigación.

Bajo las postulaciones anteriores, la validez del instrumento presenta características necesarias para su respectivo funcionamiento y aplicación. Por lo tanto, Bonilla (2011) expresa que, para llevar a cabo la validez del instrumento a aplicar, el cuestionario debe presentar una redacción coherente, clara y directa, de igual manera debe ser sometida a expertos conocedores del tema para su adecuado estudio y determinar si el instrumento realmente permite explicar el hecho o la realidad que se desea conocer.

3.7.1.1. Validez de contenido

Para determinar la validez del instrumento, se recurrió a juicio de cinco expertos con conocimiento en las temáticas abordas relacionadas con la variable de estudio sistema de gestión de la seguridad de la información bajo la norma ISO 27001:2015, los cuales evaluaron cada uno de los ítems y aportaron al mismo

tiempo sugerencias relacionadas con el mejoramiento de la redacción de algunos ítems y actualización de bibliografía. Los criterios de cada experto se encuentran referenciados en la tabla 6.

Por lo anteriormente descrito, el grado de investigación permitió llevar a cabo el proceso de validación del instrumento teniendo en cuenta el criterio de cinco (5) expertos en el área, los cuales cuentan con formación de alto nivel en maestría y doctorado, donde el formato de validación (ver anexo A) presenta una serie de ítems con criterios a evaluar basados en los objetivos específicos, conllevando a la descripción de unos indicadores que permitieron formular afirmaciones para la creación del instrumento aplicado en la población de estudio.

Tabla 6. Resultados de la validación

Expertos	Observaciones	Criterios
1	Validado sin observaciones	Aprobado
2	Valido con correcciones. Anexar un ítem más	Aprobado
3	Valido con correcciones. Anexar dos afirmaciones en relación al indicador de objetivos de seguridad.	Aprobado
4	Valido con correcciones. Mejorar la redacción	Aprobado
5	Valido con correcciones. Mejorar la redacción	Aprobado

Fuente: Suarez, (2019).

3.7.1.2. Validez de criterio

La validez de criterio es el procedimiento que hace referencia al grado de eficacia con que se puede predecir sobre el comportamiento de las variables de estudio. De esta manera, se establece a través de las calificaciones dadas por los expertos, por medio de la verificación del instrumento a aplicar en la investigación, por lo tanto, a través del software estadístico SPSS se calcula el Alfa Crombach, el cual estableció la validez del instrumento siendo en su aplicación sea aplicado apropiado y confiable. Por lo tanto, a través de los datos obtenidos por parte de los expertos y la utilización del SPSS 22.0, se establece que la validez de criterio se

encuentra representa en un 0.967%, desarrollado a través de 20 elementos que conforma el instrumento.

3.7.2. Confiabilidad del instrumento

Un instrumento es confiable cuando ofrece las garantías de que puede ser aplicada a un grupo de individuos, donde según Sabino (2013) la confiabilidad es una medida de consistencia de la escala que nos evalúa su capacidad para discriminar en forma constante entre un valor y otro. Así mismo, Bonilla (2011) determina que para el investigador es importante que el instrumento sea confiable puesto que permite obtener resultados y seguridad en su aplicación. Las características se encuentran principalmente, según Bonilla (2011), en aplicar el instrumento a un número determinado que tengan las mismas características de los elementos de la muestra o población identificada, con el propósito de hacer ajustes en la redacción, lenguaje utilizado, orden de las preguntas, cuyo resultado permite la confiabilidad.

Para el cálculo de la confiabilidad en la presente investigación se tuvo en cuenta el coeficiente de Alfa Crombach, el cual maneja escala de 0 a 1 a través de un cuestionario de 20 preguntas, es de precisar que el coeficiente de confiabilidad expresa la relación entre la varianza de error, la varianza verdadera y el resultado observado; cuando la varianza de error de un instrumento de medición es alta, el coeficiente de confiabilidad va a ser cercano a 1, esto indica que el instrumento es más confiable, la interpretación del coeficiente de confiabilidad o coeficiente Alfa depende de los propósitos planteados en la medida. El coeficiente de alfa de Cronbach para la presente investigación se calculó aplicando la siguiente ecuación:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

Dónde:

α : coeficiente Alpha Cronbach

K: número de ítems

∑ Vi: sumatoria de la varianza de los puntajes de cada ítem

Vt: la varianza de los puntajes totales.

Tabla 7. Escala de interpretación de Alpha de Cronbrach

Escala	Magnitud
0.81 a 1.00	Muy alto
0.61 a 0.80	Alto
0.41 a 0.60	Moderado
0.21 a 0.40	Bajo
0.001 a 0.20	Muy bajo

Fuente: Hernández, et at (2014)

Por lo tanto, el alfa obtenida a través de la aplicación de los resultados obtenidos de la prueba piloto correspondiente a un total de 5 personas; se obtuvo un porcentaje de 0.967, dando a conocer por medio de la interpretación del coeficiente que se encuentra dentro de una magnitud muy alta, donde demuestra que es de alta confiabilidad el instrumento aplicado en la investigación.

3.8. PROCEDIMIENTO DE LA INVESTIGACIÓN

La investigación se encuentra demarcada en ciertos lineamientos donde se debe de exponer el procedimiento para llevar a cabo el cumplimiento de los objetivos propuestos. En la actualidad existen modelos de la secuencia del proceso de investigación, por lo tanto, las postulaciones de Hernández, et at (2014), señalan que "*los autores que han publicado libros sobre el proceso de investigación científica aplicado a diversas disciplinas y áreas del conocimiento abarcan las mismas etapas".* Además, agrega que los pasos o etapas del proceso de investigación científica tienen un orden para realizarse

Teniendo en cuenta lo anterior, la investigación se centra en el desarrollo por medio de procedimientos y cumplimiento de requisitos mínimos donde se tuvo en cuenta la variable de investigación sistema de gestión de seguridad de la información bajo la norma ISO 27001:2015. Por lo tanto, el procedimiento metodológico consistió en pasos para la correspondiente planificación y ejecución de la investigación en la empresa Magdaniel Ltda., según el autor se tiene en cuenta los siguientes pasos:

El proceso de la investigación inició en concebir la idea que conllevo al desarrollo del planteamiento del problema, el cual permitió establecer los objetivos, a través de la realización de la formulación del problema junto a la justificación para dar conocimiento de su viabilidad. Se prosigue a la elaboración del marco teórico a través de la recopilación de literatura; describiendo los antecedentes basados en otras investigaciones relacionados con la variable de estudio, así mismo, se describen los fundamentos teóricos donde con el apoyo de autores se describe a nivel conceptual todo lo relacionado a las variables, dimensiones e indicadores; así mismo se define el tipo de investigación para el análisis de las variables para que puedan ser definidas conceptual y operacionalmente.

Luego, se desarrolla el marco metodológico, seleccionando el enfoque, tipo de estudio, diseño y fuentes de recolección de datos, así mismo, determina la población para llevar a cabo la recolección de datos con la elaboración del instrumento, logrando determinar la validez y confiabilidad con la aplicación del mismo. Después se debe establecer un análisis de los datos obtenidos por medio de pruebas estadísticas, donde al final se debe de elaborar los lineamientos estratégicos, junto a conclusiones y recomendaciones para futuras investigaciones.

3.9. ANÁLISIS DE LOS DATOS

La información procesada tiene un valor apreciable puesto que de ella dependerá que se pueda o no resolver las preguntas inicialmente formuladas en la investigación ya que por sí sola no es capaz de arrojar las respuestas para el respectivo análisis e interpretación. Por lo tanto, Sabino (2013) da a conocer que el análisis de datos desde el punto de vista lógico es el análisis de descomponer todas las partes de la investigación con el fin de estudiar y proceder a obtener respuestas lógicas. El procesamiento implica el agrupamiento de los mismos en unidades coherentes con estudio minucioso de sus significados y ser sintetizados en una globalidad mayor.

El análisis de los datos a través de la aplicación del instrumento en la empresa Magdaniel Ltda., por medio de los resultados obtenidos, fueron analizados cada uno de ellos, comprobando los postulados inicialmente descritos. El desarrollo de la tarea analítica dentro del problema planteado, se tomó cada uno de los datos siendo examinados mediante métodos conocidos; debido a que es una investigación cuantitativa; la información resultante fue expresa en forma numérica a través del procesamiento con cuadros, gráficas y medidas en los cuales fueron calculados los porcentajes y presentados de forma conveniente, evaluando de tal forma el comportamiento de la variable sistema de gestión de la información bajo la norma ISO 27001:2015.

Por consiguiente, los datos obtenidos a través del instrumento descrito anteriormente, fueron analizados por medio de la aplicación de las medidas de distribución de frecuencia, tendencia central y dispersión, los cuales se hallaron por medio de la aplicación del paquete estadístico SSPS versión 22.0 y hojas de cálculo de Excel, los resultados obtenidos se analizaron por medio de las tablas de categorización tanto para la media y desviación estándar.

El análisis de los datos en la presente investigación, permitieron principalmente calcular la media arítmetica como medida de tendencia central dentro del promedio estabecido por los 20 ítems del cuestionario, relacionada con la variable de sistema de gestión de seguridad de la información, bajo la norma ISO 27001:2015, evaluada a través del comportamiento de cada uno de los indicadores establecidos. Por lo tanto, el intervalo para la interpretación de la media se encuentra representada en la tabla 9, el cual se estableció un patrón de cumplimiento en referencia a cada indicador.

Tabla 8. Intervalo para la interpretación de la media

Intervalos	Categorías	Interpretación
4,21 – 5,00	Muy alta	El indicador se ubica en una frecuencia muy alta
3,41 – 4,20	Alta	El indicador se ubica en una frecuencia alta
2,61 –3,40	Moderada	El indicador se ubica en una frecuencia moderada
1,81 –2,60	Baja	El indicador se ubica en una frecuencia baja
1,00 –1,80	Muy baja	El indicador se ubica en una frecuencia muy baja

Fuente: Suarez, (2019). Basada en Bonilla (2011)

De igual manera, dentro del proceso de análisis de datos se tiene en cuenta el promedio establecido por la desviación, el cual, al igual que la media es interpretada en base a la dispersión debido a que son directamente proporcional, es decir, cuanto mayor sea la dispersión de los datos obtenidos por la media, mayor será la desviación estándar, de esta manera, los resultados relacionados con la dispersión son comparados por medio de la tabla 10.

Tabla 9. Categoría de análisis para la desviación estándar

Intervalo	Categoría
1,43 – 1,65	Muy alta dispersión – Muy poca confiabilidad
1,20 – 1,42	Alta dispersión – poca confiabilidad
0,97 – 1,19	Moderada dispersión – moderada confiabilidad

0,74 – 0,96	Baja dispersión – alta confiabilidad
0,50 – 0.73	Muy Baja dispersión – muy alta confiabilidad

Fuente: Suarez, (2019).

4. RESULTADOS DE LA INVESTIGACIÓN

Los resultados obtenidos de la presente investigación conforman una de las etapas más significativa en la realización de la investigación, debido a que se reflejan la forma como se comprueban las bases teóricas soporte del estudio y los conceptos metodológicos, con el fin de medir el nivel de coincidencia entre estos, utilizados para dar contestación a los objetivos específicos que orientados en el desarrollo del trabajo y de igual manera el logro del objetivo general.

Este capítulo permite la valoración de los datos obtenidos a través de la utilización de herramientas designada en la investigación relacionada con el Sistema de Seguridad de la Información, bajo la norma ISO 27001:2015 en la empresa Magdaniel. El análisis es establecido a través de la utilización de frecuencia y distribución porcentual de las dimensiones e indicadores consideradas en el proceso, las cuales se utilizaron como referencia para la interpretación de las respuestas obtenidas, con la finalidad de confrontar los con la matriz de caracterización de la media, mediana y moda.

Con la finalidad de analizar los resultados conseguidos, se empleó la estadística descriptiva estableciendo la media aritmética de los datos agrupados por indicador; para conseguir la tendencia manifestada por dichos indicadores se obtiene el cálculo de la dispersión de los datos a través de la desviación estándar. Los cálculos de las estadísticas se evidencian con tablas de forma detallada presentadas en consideración de la variable, dimensiones e indicadores.

4.1. POLÍTICAS DE SEGURIDAD

La empresa Magdaniel dispone de una política de seguridad enfocada en la protección de la información conllevando a la constitución de planes estratégicos

dentro de la organización para salvaguardar los activos junto a todas las partes interesadas. El uso inadecuado de la información de la empresa genera daños en el funcionamiento normal de los procesos, así mismo, se atenta contra la privacidad y confidencialidad de información de los funcionarios, terceros y usuarios en general.

Por lo tanto, todos los colaboradores de la empresa deben de cumplir la presente política en materia de protección de la información de la empresa Magdaniel Ltda., permitiendo garantizar el cumplimiento de los objetivos basados en la confidencialidad, honradez y disposición de la información a través de los roles y responsabilidades asignadas por la organización.

Los trabajadores y/o contratistas pertenecientes a la empresa Magdaniel Ltda., son responsables de la información manejada a nivel interno el cual debe ser protegido para evitar el riesgo de pérdida de la información, accesos o autorizados, uso indebido de la información y divulgación inadecuada bajo ningún casual.

La política de seguridad de la información en base a su situación actual se demuestra a través de la aplicación del instrumento aplicado en la investigación el cual es determinar las políticas de seguridad de la información bajo la norma ISO/IEC 27001:2015 para la empresa Magdaniel Ltda.; la dimensión se encuentra conformada dentro de la matriz de operacionalización por los indicadores objetivos de seguridad, roles y responsabilidades y control de acceso, los cuales son analizados a través de las respuestas obtenidas por los trabajadores de la empresa.

De acuerdo con la tabla 10 se presenta el análisis de los resultados de la frecuencia de la dimensión políticas de seguridad donde el indicador **objetivos de seguridad** donde el 57,14% de los empleados de la empresa Magdaniel respondió estar totalmente de acuerdo con los objetivos; ya que cumplen con lo establecido por la norma para la disposición de garantías enfocadas en la

confidencialidad, integridad y disponibilidad de la información; el 21.43% respondió encontrarse de acuerdo y el 21.43% respondió neutral.

Tabla 10. Indicadores de la dimensión políticas de seguridad

	Objetivos de seguridad		Roles y responsabilidades		Control de acceso	
	FA	**FR**	**FA**	**FR**	**FA**	**FR**
TA	16	57,14	5	35,71	7	50,00
DA	6	21,43	9	64,29	0	0,00
N	6	21,43	0	0,00	2	14,29
D	0	0,00	0	0,00	3	21,43
TD	0	0,00	0	0,00	2	14,29
Suma	28	100,00	14	100,00	14	100,00
Media	4,36		4,36		3,5	
Mediana	5,00		4,00		4,00	
Moda	5,00		4,00		5,00	
D Estándar	0,83		0,50		1,65	

Fuente: Suarez, (2019).

De otra parte, la media del 4.36, indicando que los objetivos de seguridad de la información se dan con una frecuencia muy alta; con relación a la mediana indica que más del cincuenta por ciento de las respuestas tiene un valor igual a 5,00, ubicándose por encima de la media y evidenciando una tendencia hacia las alternativas altas de opinión. La moda muestra que la respuesta con mayor frecuencia es 5; y la desviación estándar muestra un valor equivalente al 0.83% señalando baja dispersión y una alta confiabilidad en las respuestas.

Al respecto, Laudon & Laudon (2012) expresan que los objetivos de seguridad garantizan la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema, con el propósito de mantener un ambiente sano, logrando proteger los activos de la organización, dando uso adecuado a los recursos que hacen parte de la empresa y se encuentran disponibles para los usuarios. Dentro del mismo punto de vista se encuentra el concepto de Rodriguez (2018), quien da a conocer que los objetivos de la seguridad se encuentran enfocados en establecer mecanismos de control para los

datos que se manejan dentro de una entidad, basados en la disponibilidad, confidencialidad e integridad

En relación con los **roles y responsabilidad**, el 64,29% de los empleados respondió estar de acuerdo con la asignación de responsabilidades estipuladas por la norma ISO 27001:2015 para asegurar y dar cumplimiento al sistema de gestión; y el 37,51% restante dice estar totalmente de acuerdo con la implementación adecuada del sistema donde cada trabajador pueda ser monitoreado en la designación de sus actividades.

De acuerdo con el registro, la media indica que el promedio de respuestas positivas sobre los roles y responsabilidades es del 4,36 ubicándola en la categoría muy alta, e indicando que los roles y responsabilidad se ubican en una frecuencia muy alta; la mediana indica que más del cincuenta por ciento de las respuestas es igual o mayor a 4,00, ubicándose por debajo de la media y evidenciando una tendencia hacia las alternativas bajas de opinión. La moda muestra que la respuesta con mayor frecuencia es 4, de acuerdo; la desviación estándar de 0,50, señalando una muy baja dispersión de las respuestas e indicando una muy alta confiabilidad en los roles y responsabilidades de los funcionarios.

El resultado obtenido se encuentra acorde con el concepto emitido por la ISO 27001 (2015), donde las responsabilidades se hacen necesarias para asegurar que el Sistema de Gestión de Seguridad de la Información cumpla con todos los requisitos. Así mismo, las responsabilidades permiten monitorear el desempeño e informar a la alta dirección todo lo relacionado con el comportamiento de las personas que manejan la información dentro de la organización.

Por último, en relación con el **control de acceso**, el 50,00% de los empleados respondió estar totalmente de acuerdo con la implementación de procesos relacionados con la adaptación de contraseñas en los equipos informáticos de esa manera son protegidos contra las personas no autorizadas; el

21,43% está en desacuerdo con el sistema implementado para la protección de la información; el 14,29% muestra estar neutral frente a lo consultado, y el 14,29% está totalmente en desacuerdo con las afirmaciones.

Por tanto, la media indica el promedio de respuestas positivas sobre el control de acceso del 3,5 ubicándola en la categoría alta; la mediana indica que más del cincuenta por ciento de las respuestas es igual a 4,00, ubicándose por encima de la media y evidenciando una tendencia hacia las alternativas altas de opinión. La moda muestra que la respuesta con mayor frecuencia es 5, totalmente de acuerdo; la desviación estándar es de 1,65, señalando una muy alta dispersión en las respuestas.

Por otra parte, el resultado obtenido está en correspondencia con el concepto emitido por García & Alegre (2011), el cual considera que el control de acceso son métodos para ingresar a un dispositivo tecnológico, evitando el ingreso de personas no autorizadas para la información, comprobando la identidad del usuario a través de canales para el ingreso a los recursos físicos, estableciendo medidas de seguridad con el objetivo de proteger acorde al nivel de criticidad.

Por otro lado, se realiza el análisis de la dimensión de los indicadores anteriormente descritos, por lo cual en la tabla 12 se muestra el comportamiento de la dimensión política de seguridad, donde inicialmente está representado por un 50,00% de los empleados de la empresa Magdaniel que respondieron estar totalmente de acuerdo con las políticas establecidas de seguridad de la información, debido a que la empresa da cumplimiento a los objetivos de seguridad, asignación de roles y responsabilidades e implementación de controles a la información; el 26.79% respondió estar de acuerdo con las afirmaciones planteadas; el 14,29% está neutral frente a lo planteado; el 5,36% muestra estar en desacuerdo, y el 3,57% en total desacuerdo.

El promedio de las respuestas arrojó como resultado que el 4.14 de la media ubicándola en la categoría alta; la mediana indica que el cincuenta por ciento de las respuestas tuvo un valor igual a 4,00 asegurando una tendencia baja en las alternativas de repuestas, permitiendo encontrarse por debajo de la media; la moda muestra que la respuesta que más se repite 5, totalmente de acuerdo; la desviación estándar muestra un valor equivalente al 1,09% señalando una moderada dispersión en la respuesta.

Tabla 11. Dimensión política de seguridad

	FA	FR
TA	28	50,00
DA	15	26,79
N	8	14,29
D	3	5,36
TD	2	3,57
Suma	56	100,00
Media	4,14	
Mediana	4,00	
Moda	5,00	
D. Estándar	1,09	

Fuente: Suarez (2019)

Por lo emitido en el Ministerio de Ambiente y Desarrollo Sostenible (2014) las políticas de seguridad de la información como aquel mecanismo para la protección de activos pertenecientes a la organización, las cuales deben encontrarse alineadas con los objetivos, para la minización de riesgos relacionados con perdidas financieras, robos y acceso indebido.

4.2. SEGURIDAD FÍSICA Y DEL ENTORNO

La empresa Magdaniel Ltda., cuenta con características dentro del panorama físico y de su entorno, lo cual está distribuida en zonas según el acceso de personas ya sea autorizado o no; cuenta con zonas para las cajas eléctricas y tableros que suministran energía las cuales son calificadas de alto riesgo por tanto es de acceso limitado. Los equipos de cómputo, equipos de comunicación y

portátiles son registrados de tal manera para la protección de la información por el cual, aquellas personas ajenas a la organización no tienen acceso al recurso informático, de igual manera frente a riesgo generados en el entorno se cuenta con algunos sistemas de alarmas e incendios.

Por lo anterior, se llevó a cabo la aplicación de la encuesta en frente objetivo específico definir la seguridad física y del entorno en el sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015, en la empresa Magdaniel Ltda., a través de los indicadores sistemas de protección, áreas seguras, valoración de riesgo y análisis de riesgo; los cuales se analizan en la tabla 12.

Tabla 12. Indicadores de seguridad física y del entorno

	Sistemas de protección		**Áreas seguras**		**Valoración de riesgo**		**Análisis de Riesgo**	
	FA	**FR**	**FA**	**FR**	**FA**	**FR**	**FA**	**FR**
TA	3	21,43	7	50	6	42,86	3	21,43
DA	5	35,71	1	7,14	1	7,14	2	14,29
N	2	14,29	4	28,57	6	42,86	2	14,29
D	4	28,57	2	14,29	1	7,14	7	50,00
TD	0	0,00	0	0	0	0	0	0
Suma	14	100,00	14	100	14	100	14	100
Media	3,50		3,93		3,86		3,07	
Mediana	4,00		4,50		3,50		2,50	
Moda	4,00		5,00		3,00		2,00	
D Estándar	1,16		1,21		1,10		1,27	

Fuente: Suarez (2019)

De acuerdo a la tabla 12 se presenta el análisis de los resultados de la frecuencia de la dimensión seguridad física y del entorno, donde se observa inicialmente el comportamiento del indicador **sistemas de protección** donde el 35,71% de los trabajadores muestra estar de acuerdo con que la empresa debe de contar con sistemas de protección para evitar cualquier tipo de riesgo informático descritos bajo la norma ISO 27001:2015; el 28,57% dice estar en desacuerdo en que la información se encuentra sometida a riesgos informáticos; el

21,43% muestra estar de acuerdo con las postulaciones presentadas y el 14,29% está neutral frente a lo consultado.

Se debe agregar que la media muestra un promedio de respuestas positivas de 3,50, ubicándola en una categoría alta; la mediana indica que más del cincuenta por ciento de las respuestas es igual a 4,00 ubicándose por debajo de la media y evidenciando una tendencia hacia las alternativas bajas de opinión. La moda muestra que la respuesta con mayor frecuencia fue 4, de acuerdo; la desviación estándar de 1,16 representa una moderada dispersión de las respuestas.

De acuerdo con lo expresado por García & Alegre (2011) al sistema de protección como el método implementado por una empresa para evitar accidentes de todo tipo y de tal manera minimizar los posibles riesgos en la infraestructura, equipos o información, los cuales pueden ser causados por incendios, fallas eléctricas o cualquier otro riesgo.

El segundo indicador está relacionado con las **áreas seguras**, muestra que el 50,00% de los trabajadores encuestados están totalmente de acuerdo, que la empresa dispone de áreas seguras para el personal no autorizado; el 28,57% considera estar neutral, dado que la información manejada en la empresa se encuentra protegida contra daños e interferencias; el 14,29% muestra estar en desacuerdo con los procedimientos implementados para establecer áreas seguras y el 7,14% está de acuerdo con las afirmaciones.

De igual manera, en la tabla 12 se muestra que el promedio de respuestas positivas de la media sobre el indicador de áreas segura es del 3,93 ubicándola en la categoría alta; la mediana indica que más del cincuenta por ciento de las repuesta es mayor a 4, situada por encima de la media y evidenciando una tendencia alta de opinión. La moda muestra que la respuesta con mayor frecuencia es 5, totalmente de acuerdo; la desviación estándar de 1,21 señala una alta dispersión de las respuestas.

De acuerdo al concepto emitido por la ISO 27001 (2015) las áreas seguras son aquellas como aquel sitio donde se maneja información sensible o valiosos equipos informáticos, es decir, el refugio con los que alcanzar los objetivos de la organización. Por lo tanto, dentro del contexto de seguridad se entiende como el sitio donde se alberga cada uno de los servicios que ofrece la organización, así mismo, contando con sistemas de monitoreo constante en el control del personal basados en la seguridad, a través de los recursos tecnológicos suministrados por la alta gerencia los cuales están descritos en los software para antivirus, controles de acceso a personal autorizado, implementación de protocolos y almacenamientos en lugares seguros.

Seguidamente, el indicador **valoración de riesgo** muestra que el 42,86% de los trabajadores están totalmente de acuerdo con la identificación de los riesgos que puedan causar daño e impiden el acceso de la información en la empresa relacionados con el fraude, robo de información y falta de continuidad de lla empresa; el 42,86% muestra estar neutral frente a las exposiciones de ocurrencias de eventos no deseados sobre el sistema de información de la empresa; el 7,14% está de acuerdo con las afirmaciones y el 7,14% restante muestra estar en desacuerdo.

Así mismo, en la tabla se indica que el promedio de respuestas positivas de la media sobre la valoración de riesgo es del 3,86 ubicándola en la categoría alta; la mediana indica que más del cincuenta por ciento son mayores a 3,00, ubicándose por debajo de la media y evidenciando una tendencia baja hacia las alternativas de opinión. La moda muestra que la respuesta con mayor frecuencia es 3, neutral; la desviación estándar de 1,10 señala una moderad dispersión entre las respuestas.

En este sentido, Doria (2014) define la valoración de riesgo como aquel potencial donde un inoportuno o acontecimiento no esperado genere debilidad, con la posibilidad de generar resultado indeseable para la compañía o en un

activo específico. Son acciones que puedan causar daño, destrucción, alteración, pérdida o relevancia de activos los cuales podrían impedir su acceso o prevenir su mantenimiento. Actualmente, la empresa muestra la necesidad de dar continuidad apropiada al SGSI debido a la importancia de proteger la información de la empresa y sus clientes.

Por último, el indicador **análisis de riesgo** da a conocer que el 50,00% de los trabajadores encuestados están en desacuerdo con que la empresa realiza el análisis para la identificación de las amenazas dentro del sistema de informativo, así mismo, cuenta con las herramientas de gestión de la seguridad en la información para la identificación de los riesgos. El 21,43% muestra estar totalmente de acuerdo con las afirmaciones. En un porcentaje igual de 14,29% están de acuerdo y neutral frente a lo formulado.

En igual sentido, la tabla muestra los datos representados por la media, el cual indica que el promedio de las respuestas sobre análisis de riesgo es de 3,07 ubicándola en una categoría moderada; la mediana indica que el cincuenta por ciento de las respuestas son superiores a 2,00, evidenciando bajas alternativas de opinión y ubicándose por debajo de la media. La moda muestra que la respuesta con mayor frecuencia es 2, desacuerdo; la desviación estándar de 1,27 señala una alta dispersión entre las respuestas.

Por tanto, Doria (2014) describe el análisis de riesgo permite estudiar las causas de las amenazas generadas; por ello el análisis de riesgo se considera como la herramienta de gestión en estudios financieros y en la seguridad para la identificación de los riesgos. Los riesgos se calculan de la combinación de los valores de los activos que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad de que las amenazas y debilidades puedan causar un incidente; así mismo, el análisis de riesgos establece la existencia o no de

controles que ayuden a la minimización o eliminación de la probabilidad de la ocurrencia de la vulnerabilidad.

Tabla 13. Dimensión seguridad física y del entorno

	FA	**FR**
TA	19	33,93
DA	9	16,07
N	14	25
D	14	25
TD	0	0
Suma	56	100
Media	3,59	
Mediana	3,50	
Moda	5,00	
D Estándar	1,20	

Fuente: Suarez (2019)

El análisis representado en la tabla 13, indica que el 33,93% de los trabajadores están totalmente de acuerdo con que la seguridad física y del entorno el cual es generado a través de la disposición de áreas seguras y sistemas de protección que permiten la protección de los activos de la empresa Magdaniel Ltda.; el 25,00% dice estar neutral frente a las actividades de implementación para la protección de la información; de igual porcentaje del 25,00% muestra que los trabajadores están en desacuerdos con el proceso de análisis de riesgos ejecutados en la empresa y con el 16,07% están de acuerdo con los procesos de la seguridad física en la organización.

Así mismo, se indica que para la media el promedio de respuestas positivas sobre la seguridad física y del entorno es del 3,59 ubicándola en la categoría alta; la mediana indica que más del cincuenta por ciento de las respuestas es mayor a 3,00, mostrando alternativas bajas de opinión y estar por debajo de la media. La moda muestra que la respuesta con más frecuencia fue 5, totalmente de acuerdo; la desviación estándar de 1,20 muestra una alta dispersión entre las respuestas.

Siguiendo con lo establecido por la ISO 27001 (2015) la seguridad de la información en el entorno consiste en asegurar que los recursos del Sistema de Información de una compañía sean utilizados apropiadamente y el acceso de información se encuentre disponible controlando las modificaciones posibles por parte de las personas autorizadas.

4.3. ACTIVOS DE INFORMACIÓN

Hacer referencia a los activos de información en la empresa Magdaniel es todo aquello basado en la descripción de sus actividades, registros, documentos, información de clientes y otros, los cuales deben encontrarse protegidos para un mayor control en los procesos, siendo descritos de la siguiente manera:

Tabla 14. Lista de activos de la empresa Magdaniel Ltda.

Tipo de activo	Nombre de la información	Descripción
Activo de datos	Base de datos	Información sobre las anotaciones de solicitudes e información de clientes y/o proveedores, y otros
Activo de software	Software aplicativo de planos arquitectónicos	Diseño arquitectónico para cualquier tipo de construcción
Activo de Hardware	Equipos de computo	Equipos que permiten el desarrollo de actividades y otras obligaciones que deben desempeñar los trabajadores en la empresa
Activo de red	Red Wif Red LAN	Redes de acceso ya sea de uso inalámbrico para el uso interno de los empleados en la organización
Activos de servicios	Correos electrónicos Página web	Canales de comunicación interno y externo que le permite a la empresa adquirir la información necesaria.

Fuente: Suarez (2019)

Teniendo claro los activos que representan a la empresa se conlleva a la valoración del grado de importancia y criticidad para la empresa Magdaniel Ltda., por el cual se tiene lo siguiente:

Tabla 15. Valoración de los activos de la empresa Magdaniel Ltda.

Aspectos	Criterio	Impacto	Valoración	Escala de valoración
Financiero	Pérdidas económicas	< a 100 millones de pesos	1	Bajo
		Entre 100 y 300 millones de pesos	2	Medio
		>300 millones de pesos	3	Alto
Imagen	Aspectos negativos de imagen de la empresa para clientes internos y externos	Falta de credibilidad	1	Bajo
		Pérdida de clientes potenciales	2	Medio
		Afectación en las ofertas de servicios y obtención de nuevos clientes	3	Alto
Legal	Incumplimiento en los aspectos normativos y legales	Cancelación de contratos con clientes	1	Bajo
		Afectación en los procesos contractuales	2	Medio
		Demandas por incumplimiento en contratos	3	Alto

Fuente: Suarez (2019)

Los resultados de la investigación en base al objetivo específico de la presente dimensión el cual es identificar los activos de información en el sistema de gestión de seguridad de la información, bajo la norma ISO/IEC 27001:2015, el cual se encuentra representado por los indicadores propiedad e inventario de los activos, donde su comportamiento se describe en la siguiente tabla.

Tabla 16. Indicadores de Activos de información

	Propiedad de los activos		Inventario de activos	
	FA	**FR**	**FA**	**FR**
TA	6	42,86	10	71,43
DA	4	28,57	2	14,29
N	0	0,00	0	0
D	4	28,57	2	14,29
TD	0	0,00	0	0
Suma	14	100,00	14	100
Media	3,86		4,43	
Mediana	4,00		5,00	

Moda	5,00	5,00
D Estándar	1,29	1,09

Fuente: Suarez (2019)

El análisis de los resultados de la frecuencia de los indicadores de la dimensión activos de información se observa que el indicador **propiedad de los activos**, está representado inicialmente con el 42,86% de los trabajadores encuestados los cuales están totalmente de acuerdo con que la empresa cuenta con la definición de los activos dentro procesamiento de la información, el cual es designada por la organización; el 28,57% dice estar de acuerdo con las afirmaciones antes mencionada, en igual porcentaje de 28,57% dice estar en desacuerdo con los procedimientos aplicados en la propiedad de los activos.

Prosiguiendo, la media indica que el promedio de respuestas positivas sobre la propiedad de los activos es de 3,86 ubicándola en la categoría alta; la mediana muestra que más del cincuenta por ciento de las respuestas es igual a 4,00, con una tendencia hacia las alternativas altas de opinión y ubicarse por encima de la media. La moda muestra que la respuesta con más frecuencia es 5, totalmente de acuerdo; la desviación estándar de 1,29, señala una alta dispersión entre las respuestas.

Por otra parte, de acuerdo a la definición planteada por la ISO 27001 (2015) la propiedad de los activos es toda la información y activos asociados con los servicios de procesamiento de información deben ser "propiedad" de una parte designada de la organización**,** dentro del proceso que conlleve a la gestión de tecnología según su criticidad y protección, teniendo aspectos importantes relacionados con los aspectos financieros, legales y de imagen, los cuales deben verse materializado en la confidencialidad, integridad y disponibilidad de la información.

Referente al indicador **inventario de activos**, el 71,43% de los trabajadores encuestados manifiestan estar totalmente de acuerdo con los procesos de inventarios de activos realizados por la empresa; considerados de tal manera como parte importante de la misma; el 14,29% está de acuerdo con las afirmaciones planteadas y el 14,29% restante en desacuerdo con los procesos realizados en la empresa relacionado con los activos de información.

De esta manera, la media indica que el promedio de respuestas positivas sobre el inventario de activos es del 4,43 ubicándola en la categoría muy alta; la mediana indica que más del cincuenta por ciento de las respuestas es igual a 5,00, ubicándose por encima de la media y evidenciando una tendencia hacia las alternativas altas de opinión. La moda muestra que la respuesta con más frecuencia es 5, totalmente de acuerdo; la desviación estándar de 1,09 mostrando una moderada dispersión entre las respuestas.

Para la ISO 27001 (2015) el proceso relacionado con el inventario de activos hace referencia, a todos los activos que deben estar claramente identificados, los cuales son sometidos a un proceso descriptivos, a través de la clasificación que contiene parámetros para determinar el grado de cada activo, por medio de la recopilación de información adecuada de todo aquello que hace parte de la organización.

Por otra parte, de acuerdo con los registros de la tabla 17, el 57,14% de los trabajadores está totalmente de acuerdo con que los activos de la información son considerados parte importante de la empresa a través de la implementación de procedimientos para la descripción y conocimiento de los activos dentro del entorno, el 21,43% está de acuerdo con las afirmaciones realizadas y el 21,43% restante se mostró en desacuerdo con algunos procedimientos relacionados con el inventario de activos.

Tabla 17. Dimensión Activos de la información

	Activos de la Información	
	FA	**FR**
TA	16	57,14
DA	6	21,43
N	0	0
D	6	21,43
TD	0	0
Suma	28	100
Media	4,14	
Mediana	5,00	
Moda	5,00	
D Estándar	1,21	

Fuente: Suarez (2019)

Así mismo, la tabla manifiesta indica el comportamiento de la media donde el promedio de respuestas positivas sobre los activos de la información es del 4,14 ubicándola en la categoría alta; la mediana indica que más del cincuenta por ciento de las respuestas es igual a 5,00, ubicándose por encima de la media y evidenciando una tendencia hacia las alternativas altas de opinión. La moda muestra que la respuesta con mayor frecuencia fue 5, totalmente de acuerdo; la desviación estándar de 1,21 muestra una alta dispersión entre las respuestas.

Siguiendo con lo establecido por la norma ISO 27001 (2015) establece que los activos de información es el recurso del sistema de seguridad de la información necesario para que la empresa funcione y consiga los objetivos propuestos en la alta dirección. Los activos se encuentran directa e indirectamente relacionados con las demás entidades de la organización.

Tabla 18. Variable sistema de gestión de seguridad de la información

	FA	**FR**
TA	63	45,00
DA	30	21,43
N	22	15,71
D	23	16,43
TD	2	1,43

Suma	140	100,00
Media	3,92	
Mediana	4,00	
Moda	5,00	
D Estándar	1,18	

Fuente: Suarez (2019)

Los resultados del análisis de frecuencia de la variable sistema de gestión de seguridad de la información, señalaron que el 45,00% de los trabajadores encuestados manifestó estar totalmente de acuerdo con los procedimientos para el administración de la información y cumplimiento de las políticas establecidas por la ISO 27001:2015; el 21,43% indicó estar de acuerdo con los roles y responsabilidades asignadas en el entorno físico conllevando a la protección de la información; el 15,71% muestra estar neutral frente a las afirmaciones realizadas; el 16,43% están en desacuerdo con el análisis de riesgos ejecutado por la empresa, el cual hace vulnerable a los activos y el 1,43% restante se muestra en total desacuerdo.

En este mismo sentido, la media muestra que el promedio de contestaciones positivas sobre el sistema de gestión de la información es del 3,92 ubicándola en una categoría alta; la mediana indica que más del cincuenta por ciento de las respuestas es mayor a 4, ubicándose por encima de la media y evidenciando una tendencia hacia las alternativas altas de opinión. La moda muestra que la respuesta con mayor frecuencia es 5, totalmente de acuerdo; la desviación estándar de 1,18 señala una moderada dispersión entre las respuestas.

De esta manera, Gómez & Álvarez (2012), señalan al SGSI como aquel conjunto de elementos que conllevan a la protección de todos aquellos activos informáticos pertenecientes a una organización, teniendo en cuenta todos los riesgos existentes dentro del proceso. De esta manera, los objetivos planteados por una empresa dentro de la implementación del sistema deben de atribuir a la aplicación de controles para la mitigación de peligros y de esta manera la implementación arroje resultados satisfactorios.

4.4. LINEAMIENTOS ESTRATÉGICOS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El desarrollo investigativo complementa el trabajo con la resolución del objetivo número cuatro, el cual establece proponer lineamientos estratégicos para el SGSI bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda., enfocado en los trabajadores que son autorizados en el manejo adecuado de la información dentro del entorno de la compañía. Estos lineamientos son formulados de acuerdo con los resultados obtenidos en función a los encuestados.

4.4.1. Introducción

El SGSI cuenta con la capacidad de proveer a la organización la seguridad pertinente para la protección de sus activos, gestionando de manera eficiente los riesgos generados por cualquier tipo de proceso que pueda transgredir en contra de la seguridad de la información, por lo tanto, este tipo de sistema genera la confianza suficiente donde las artes interesadas generen crecimiento y sostenibilidad en los procesos de la organización.

Para las organizaciones hoy en día es importante la ejecución de un adecuado sistema de gestión de seguridad de la información, el cual le permite contar con una guía de seguridad alineado a las necesidades y objetivos de la empresa, encontrándose compuesto por la estructura organizacional que conlleva a la designación de roles y responsabilidades para la gestión segura de salvaguardar la información de la compañía.

Es necesario entonces que la empresa Magdaniel Ltda., mediante la gestión e implementación adecuada del SGSI permita fortalecer de manera integral a los trabajadores por medio de la disponibilidad, honestidad y confiabilidad de la información que conlleve a fomentar la cultura apropiada para la seguridad de la información. Desde esta perspectiva, se formulan los siguientes lineamientos encaminados a mejorar el sistema en la empresa en mención.

4.4.2. Objetivo

Formular lineamientos estratégicos para mejorar el sistema de gestión de seguridad de la información, bajo la norma ISO7/IEC 27001:2015, en la empresa Magdaniel Ltda.

4.4.3. Objetivos específicos

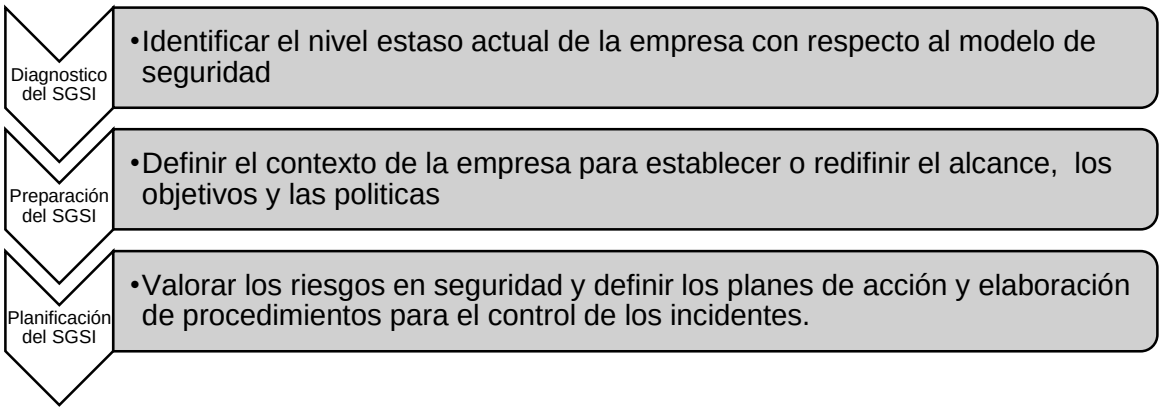
- Fortalecer las fases para la ejecución adecuada del SGSI en la empresa Magdaniel Ltda.
- Definir metodología para identificar y clasificar los activos de la información, para su valoración y tratamiento.

4.4.4. Justificación

Formular lineamientos estratégicos para la presente investigación desarrollar distintas fases para el mejoramiento de los procesos del SGSI en la empresa Magdaniel, en el Distrito de Riohacha, lo cual, estará contemplada en una serie de actividades que conllevaran al alcance de los objetivos específicos propuestos en el presente trabajo de investigación. Cada uno de los puntos propuestos relacionara distintos elementos para el desarrollo adecuado de las actividades enmarcadas en la ejecución y mejoramiento del sistema en la empresa, por lo tanto, cada uno de los puntos está direccionada a la ejecución de acciones descritas en la norma

Lineamiento estratégico 1. Establecer las fases para la implementación adecuada del SGSI

Ilustración 2. Fases del sistema de gestión de la seguridad de la información



Fuente: Suarez (2019). Basado en la ISO 27001:2015

Los requerimientos establecidos bajo la norma ISO 27001:2015, conlleva a la ejecución de ciertos lineamientos para el adelanto adecuado del sistema de seguridad. Por lo cual, dentro del contexto de seguridad es importante tener claro las fases necesarias para el funcionamiento óptimo de los procesos o actividades generadas, las cuales son generadas a través del diagnóstico, preparación y planificación, donde cada una ella logra analizar los detalles a mejorar en el sistema de gestión, debido a que cada una cumple con funciones y actividades en específico.

Etapa 1. Diagnóstico: esta etapa comprende todo lo relacionado al proceso de identificación del nivel en el cual se encuentra el sistema de gestión de la empresa, teniendo en cuenta las especificaciones que plantea ISO 27001:2015, de tal manera se obtenga la información necesaria que conlleve a su debido tratamiento, el mecanismo a utilizar para obtener la información es la siguiente:

- Diligenciamiento de formatos para establecer el grado de desempeño de la empresa relacionado con la aplicación de los lineamientos de ISO 27001:2015.
- Organizar toda la documentación importante de la empresa, relacionadas con la designación de roles y responsabilidades, políticas y funciones.

- Valorar e identificar activos en la empresa con puntajes designados, para el conocimiento previo para salvaguardar información.
- Especificar el nivel de cumplimiento y riesgo a través del formato estipulado por la ISO 27001:2015.

Etapa 2. Preparación del SGSI. La norma ISO 27001:2015 da a conocer los factores internos y externos que puedan afectar de manera positiva o negativa la información de la empresa y la empresa misma. Es por ello, que esta fase le permite a la organización determinar los factores pertinentes para el adecuado funcionamiento del sistema de gestión. Para ello se debe realizar las siguientes actividades:

- Realización de asesoría y capacitaciones para la adecuada ejecución y funcionamiento del sistema de gestión.
- Revisar y actualizar la matriz de riesgo, la cual permite la identificación, implementación y administración del sistema de riesgo de la empresa.
- Promover los recursos tecnológicos para garantizar la confiabilidad, disponibilidad e integridad de la información, los cuales determinaran el monitoreo y evaluación de la empresa.
- Aseguramiento de los activos de información para garantizar la mejora continua.
- Adecuar las políticas y objetivos de seguridad según el alcance de la empresa, así mismo divulgar a todas las partes interesadas y su respectivo cumplimiento.

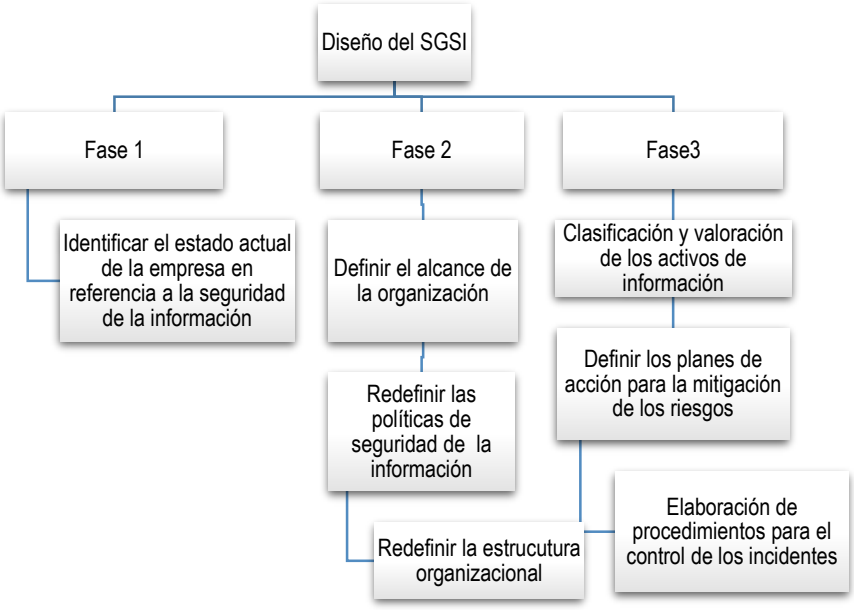
Etapa 3. Planificación del SGSSI. La parte de planificación permite la realización de las actividades pertinentes dentro del sistema, asegurando que se cumple a cabalidad los objetivos propuestos, conocer los riesgos y falencias

presentadas en el proceso y poder mitigar o anular la existencia de los mismos. Las actividades basadas en esta etapa son las siguientes:

- Clasificación de los activos, valoración de los riesgos y nivel de criticidad de la empresa, basado en los anexos estipulados por la ISO 27001:2015.
- Elaboración de matriz con la descripción de los activos,
- Estatutos para la confiabilidad de datos
- Elaboración de procedimientos a través de los datos suministrados por la evaluación inicial.

Los responsables en cada una de las etapas del sistema son: la alta dirección y colaboradores designados en cada una de las actividades, designando roles y responsabilidades dentro del sistema. Para llevar a cabo el desarrollo de las fases de manera adecuada, se describen actividades relacionadas para su mejor diseño en la empresa, y se obtengan resultados positivos en el proceso de mejoramiento, por lo tanto, se tiene el siguiente esquema.

Ilustración 3. Fases para el diseño del SSGI



Fuente: Suarez (2019). Basado en la ISO 27001:2015

Lineamiento estratégico 2. Especificar el sistema para la caracterización y categorización de los activos de la información, que conlleve a la valoración y tratamiento de riesgos de seguridad establecidas a través del planteamiento de enfoques para la identificación de los riesgos por medio de procesos de identificación, de esta manera se establece en la tabla 19 las codificaciones que determinadas dentro del ámbito informático para la identificación del riesgo, de igual manera se describe puntualmente el paso a paso para la identificación valoración de activos y peligros.

Identificar y Valorar Activos de Información

- Describir los activos de información para determinar el tipo
- Identificar los dueños de los riesgos y los responsables.
- Establecer el porcentaje de criticidad y el nivel de criticidad del activo
- Determinar la evaluación de riegos

Identificar y Valoración de Riesgos

- Identificación de peligros y debilidades
- Examinar el peligro
- Elaborar matriz de peligro
- Evaluación de controles
- Establecer planes de tratamiento de riesgos

Tabla 19. Codificación de los riesgos

R1	Acceso no autorizado
R2	Ataques externos
R3	Cambios de privilegio

R4	Pérdidas naturales
R5	Circulación de la información
R6	Falta del dirigente
R7	Establecimiento de software no facultado
R8	Apropiación no calificada de información
R9	Obstáculo en los productos
R10	Reforma sin permiso
R11	Hurto de dispositivos
R12	Uso inadecuado del sistema
R13	Abuso de privilegios

Fuente: Basado en la ISO 27001:2015

El mecanismo para la identificación de amenazas y los riesgos de la empresa se debe de elaborar una lista general de todo aquello que pueda afectar a la empresa, teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información.

- Caracterización de las debilidades las cuales se encuentran asociadas a los peligros de los activos de la información
- Valora los controles, a través de listas de chequeo permitiendo la evaluación de los controles a implementar.
- Periodicidad de revisión de las matrices de riesgos, las cuales deben ser revisadas y actualizadas mínimas una vez al año, según los hechos generados.
- Adiestramiento en seguridad de la información, a través de planes periódicos.

CONCLUSIONES

A continuación, se establecen las conclusiones a partir de la comparación de los resultados de la investigación y las bases teóricas que soportan el estudio, los cuales se fundan en forma de síntesis sobre las consideraciones más relevantes originadas del análisis de los datos para sustentar las premisas propuestas, logrando la argumentación de los objetivos que orientaron este trabajo.

De acuerdo al primer objetivo específico, determinar las políticas de seguridad, se evidenció que dentro de la empresa se llevan a cabo actividades relacionadas con el cumplimiento de los objetivos, disponiendo de las garantías necesarias para la conservación de la información y manejo por parte de los colaboradores, conllevando a la protección y administración de los recursos que suministra la empresa. Así mismo, se da a conocer la importancia de la designación de roles y responsabilidades en la manipulación de información, aprovechando los recursos que brinda el entorno los cuales son designados a través de los niveles operativos y directivos.

De esta manera, las respuestas de los trabajadores de la empresa Magdaniel consideran la importancia de los sistemas de protección que ayuden a minimizar cualquier tipo de riesgo específicamente para la seguridad de la información, conllevando a la protección de aquello que reside en las bases de datos de la organización. Por lo tanto, cada perspectiva de los trabajadores permitió determinar la importancia que tienen las políticas de seguridad en la información, pues logran acatar en gran porcentaje lo referente a la confidencialidad, integridad y disponibilidad de la información.

En relación al segundo objetivo específico, definir la seguridad física y del entorno, se evidenció que la empresa se encuentra ausente en la gestión de

estudios financieros y sistemas de protección para la evaluación de los peligros de los activos representados en la compañía; así mismo, existen debilidades relacionadas con la determinación de áreas segura y desconocimiento de procesos para la protección de la información, aunque se emiten en ocasiones los procedimientos adecuados relacionados en el paso de personas no capacitada en la manipulación de la información.

Por lo tanto, teniendo en cuenta la perspectiva de los trabajadores se considera que la valoración de riesgo en la empresa estimula en ocasiones al estudio de aquellos peligros que logren causar daño en los activos de la organización, determinando la opción de tratamiento estableciendo medidas y controles, por medio del diagnóstico realizado generando seguridad en los procesos.

En referencia al tercer objetivo específico, identificar los activos de la información, la empresa cuenta con procesos que permiten la descripción de la propiedad de los activos presentes, el cual es promovido por la valoración realizada a través de la gestión de los recursos, donde todo tipo de aspectos ligados al sistema de información son analizados en la ejecución de las actividades.

Por lo tanto, de acuerdo a la opinión de los trabajadores el inventario de los activos realizado dentro de la empresa cumple con las expectativas necesarias en el desarrollo de actividades adecuadas en la protección de los elementos importante de la organización, principalmente la información, donde este tipo de procesos les permite identificar los riesgos a través de procesos tecnológicos que conlleven a la toma de decisiones dentro del entorno. Logrando a su vez establecer que en ocasiones no se cumple con los procedimientos correspondientes en el conocimiento y tratamiento de los activos de la empresa, debido a la importancia de establecer seguridad y administración constante.

Para el cuarto objetivo específico, proponer lineamientos para mejorar sistema de gestión de seguridad de la información, bajo la norma ISO7/IEC 27001:2015, en la empresa Magdaniel Ltda., está dirigido a los trabajadores y altos directivos que tienen constante manipulación de la información relacionada con la empresa, con la finalidad de proporcionar las bases de formación que motiven a la cultura de generar seguridad dentro de la empresa.

Finalmente, se concluye que la variable sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015, haciendo referencia a la dimensión políticas de seguridad el nivel de cumplimiento es el adecuado bajo lo establecido por la norma; en la seguridad física y del entorno, no se dispone de áreas totalmente seguras, donde el adelanto de actividades y manejo de los activos de la información de la empresa no están seguros y con ello conllevan a la afectación de los procesos; el abandono de controles conlleva a la generación de niveles altos de vulnerabilidad de los activos dentro de la categorización de los riesgos, por lo cual implica a la empresa a la realización de esfuerzos para el cumplimiento de los controles y mitigación de las amenazas y riesgos existentes.

Además, teniendo en cuenta las debilidades encontradas se formularon lineamientos estratégicos en caminados a mejorar los métodos de control de entrada y mitigación de riesgos expuestos. Por ello, se logró establecer a través de los lineamientos estipulados por la ISO 27001:2015, las etapas para la mejora continua de los métodos y protección de la información, estableciendo a su vez mecanismos para la concientización y sensibilización del SGSI, fortaleciendo la cultura en seguridad a los trabajadores de la empresa Magdaniel Ltda.

RECOMENDACIONES

Tomando como marco referencial las conclusiones emitidas por los trabajadores, se plantea a continuación sugerencias donde a modo de reflexión final se redactaron de acuerdo a los datos registrados como resultados en el desarrollo del trabajo de investigación que contribuyan a la finalidad de la misma la cual es proporcionar a los directivos y empleados pautas para el dirección adecuado de la información dentro y fuera de la compañía.

Atendiendo al primer objetivo de investigación, concerniente a las políticas de seguridad, el cual debe ser aprobado en la alta gerencia donde debe de poner en conocimiento el grado de promover la seguridad en la información de la empresa por medio de la disponibilidad, confidencialidad e integridad, donde es importante el compromiso para establecer soportes que conlleven al mejoramiento continuo de las operaciones, logrando de tal manera la alineación entre los objetivos de la organización con las políticas de seguridad de la información .

El segundo objetivo, definir la seguridad física y del entorno se demuestra la capacidad de la empresa en referencia a sus activos, con el objetivo de responder dentro de la ejecución de inspecciones y métodos de gestión requeridos para interceptar las fallas en los diagnósticos realizados, ya que la mayoría requiere de un dispositivo técnico, los cuales están relacionados con los monitores, cámaras, software especializado para la identificación del personal, entre otros. Estos procesos son logrados por medio de ejecución de herramientas informáticas es de la mano con las capacitaciones constantes al personal de la empresa y contratación de capital humano idóneo para la ejecución y manipulación de los activos que representan a la organización.

En cuanto al tercer objetivo, identificar los activos de información es importante la realización de operaciones de seguridad, con la intención de forjar sentido de pertenencia y apropiación en temas de seguridad siendo consientes sobre las inseguridades que pueden afectar la disponibilidad de la información. Así mismo, el determinar las amenazas existentes relacionadas con los activos de la empresa conlleva a detallar las especificaciones técnicas, las cuales se recomienda documentarse y emitir informes para el conocimiento de toda la empresa y de esta manera, capacitar al personal en los temas relacionados con la seguridad de la información.

En relación a los lineamientos establecidos para el mejoramiento del sistema de gestión de la información basado en la ISO 27001:2015, se proponen estrategias relacionadas con las fases para una apropiada ejecución del sistema,, permitiendo establecer lineamientos basados en la mejora continua o ciclo PHVA, identificando paso a paso la situación real de la disposición de información por parte de la empresa y las personas en la cual tienen acceso. Así mismo, se manifiesta el método para la caracterización y categorización de los activos, donde es importante su valoración y tratamiento.

REFERENCIAS BIBLIOGRÁFICAS

27001, I. (2015). *Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información (Sgsi). Requisitos .* ICONTEC.

Alvarez, G., & Perez, P. (2004). *Seguridad infomartica ara las empresas y particulares.* Madrid, España: McGraw-hill.

Arias, F. (2016). *El proyecto de investigación: Introducción a la metodología científica.* Caracas, Venezuela: Episteme. 7ª edición.

Balestrini Acuña, M. (2016). *Como se elabora un proyecto de investigación.* Caracas, Venezuela: Consultoria asociados.

Benavides, A. & Blandón, C. (2017). *Modelo de sistema de gestión de la información bajo la norma NTC ISO/IEC 27001 para las instituciones públicas de educación básica de la comuna universidad de la ciudad de Pereira.* Tesis de Maestría: Universidad autónoma de Manizales. Manizales, Colombia.

Bernal, C. (2010). *Metodologia de la Investigación. Administración, economía, humanidades y ciencias sociales.* Bogotá, Colombia: Pearson. 3ª edición.

Berrio (2016). *Metodología para la evaluación del desempeño de controles en sistema de gestión de seguridad de la información sobre la norma ISO /IEC 27001*. Tesis de Maestría: Universidad nacional de Colombia. Medellín.

Bonilla, E. (2011). *Metodología de la investigación. Un enfoque práctico.* Bogotá: Gente Nueva Editorial.

Cadme, C. & Duque, D. (2012). *Auditoria de seguridad informática ISO 27001 para la empresa de alimentos "Italimentos Cia. Ltda."* Tesis. Universidad del Ecuador. Cuenca-Ecuador.

Camelo, L. (2010). *Seguridad de la Informacion en Colombia.* Experiencia personal: dificultades en la implementacion de un SGSI. Disponible en internet:(seguridaddelainformacionencolombia.blogsplot.com.co/2010/02/experiencia-personal-difilcultades-en-la-htm)-

Cárdenas, A. (2018). *ISO 27001 Gestión Integral de la Seguridad de la información*. Block Novasec.

Correa, M. y Cabezas, I. (2014). *Definición de políticas de seguridad informática de los servidores y sitios web del Sistema de Investigación de la Universidad Nacional.* SIUN. Bogotá, Colombia.

Devece, Guiral & Lapiedra, (2011). Introducción a la gestión de sistemas de información en la empresa. Editorial, publicacions de la Universitat Jaume I. UJI.

Díaz -Ricardo, Y; Pérez del Cerro, Y; & Proenza-Pupo, D. (2014). *Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguí*. *Ciencias Holguin*, 1-14.

Espinosa, García y Giraldo (2016). *Sistema de gestión de seguridad de la información para los tres procesos misionales de la corporación autónoma regional de Risaralda.* Tesis de Maestría: Universidad autónoma de Manizales. Manizales, Colombia.

García, A & Alegre, M. (2011). *Seguridad Informática.* Madrid, España. Paranifo. 1ª Edición.

Gómez V, A. (2013). *Análisis y gestión de riesgos. Seguridad en equipos informáticos.* Ediciones de la U. Bogotá, Colombia.

Gómez Vieites, Á. (2013) Análisis y gestión de riesgos. En Gómez Vieites, A. Seguridad en equipos informáticos. Bogotá: Ediciones de la U.

Gómez, L., & Álvarez, A. (2012). *Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre la seguridad en sistemas de información para pymes.* España: España .

Guamán (2015). *Diseño de un sistema de gestión de seguridad de la información para instituciones militares:* Tesis de maestría: Quito, Ecuador**.** Escuela Politécnica Nacional.

Gutarra, A. (2016). *Los riesgos de la red informática y las responsabilidades de los educadores.* Artículo de la Universidad Complutense. Madrid - España

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2014). *Metodología de la Investigación.* Mexico: McGraw-Hill. 6ª edición.

Hodegha, U, & Nayak, U. (2014). *El manual de InfoSec: una introducción a la seguridad de la información.* Nueva York: Edición Apress Media.

Hurtado, J. (2012). *Metodologia de la investigación: Guía para una comprension holística de la ciencia.* Bogota: Ciea-Sypal y Quiron. 4ª edición.

ISO 27001 (2013). Portal de la ISO. Que es un SGSI. http://www.iso27000.es/iso27000.html.

Kim, S & Solomon, M. (2011). *Fundamentos del Sistema de Seguridad de Información.* Canadá. Editorial Jones & Bartlett Learning.

Landeta, J. (2011). *El metodo Delphi: una metodología para facilitar la contribución de expertos en contextos profesionales.* Revista Pronostico tecnologico y cambio social. Madrid, España: Edición Ariel.

Laudon, K. y Laudon, J. (2012). *Sistemas de información gerencial.* México: Pearson educación.

Mendez Alvarez, C. E. (2013). *Metodologia. Diseño y desarrollo de investigación con enfasis en ciencias empresariales.* Mexico: Limusa. 4ª edición.

Mejía, M. & Lobo, J. (2015). *Diseño e implementación de una estrategia de seguridad de la información.* Ministerio de tecnologías de la información y las comunicaciones. Guía estratégica. Bogotá.

Ministerio de Ambiente y Desarrollo Sostenible (2014). *Políticas de seguridad de la información.* MinAmbiente. Bogotá, Colombia.

Moncoyo, A. & Marco, M. (2012). *Sistemas de información.* Departamento de lenguajes y sistemas informáticos. San Vicente, España: Universidad de Alicante.

Niño, V. (2014). *Metodologia de la Investigación.* Bogota: Ediciones de la U.

Ochoa, M. (2016). *Implementación de la norma ISO/IEC 27001 para la seguridad del Data Center del GAD Municipal del Cantón Cuenca*. Cuenca Ecuador. Escuela de Ingeniería Electrónica. Trabajo de grado.

Palella, S., & Martins, F. (2012). *Metodología de la investigación cuantitativa.* Caracas, Venezuela: Holistica. 3ª edición.

Peltier, T. (2014). *Information Security Fundamentals.* Segunda Edició. Taylor & Frances Group. Estados Unidos.

Rodríguez, S. (2018). *Ciberseguridad práctica: Servidores y estaciones de trabajo.*

Rivas (2017). *Diagnóstico y plan de acción para la implementación del marco de negocio para el gobierno y gestión de tecnologías de la información (cobit5.0).* Tesis de Maestría: Universidad técnica de Machala

Ruiz, L. (2018). *Sistema de seguridad de la informacion es la clave en la empresa*. Bogota-Colombia. Revista Vanguardia .

Sabino, C. (2013). *El proceso de investigación.* Caracas, Venezuela: Panamericana.

Suarez (2015). *Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la*

*infraestructura tecnológica de la organización***.** Tesis de Maestría: Universidad Nacional Abierta y a Distancia. Bogotá, Colombia.

Stewart, P. (2012). *Política hacia estados frágiles: un enfoque integrado de la seguridad y desarrollo.* Estados Unidos, Washington.

Tamayo y Tamayo, M. (2014). *El proceso de la investigación cientifica.* Mexico: Limusa S.A.

TICs, Ministerio. (2016). "Vive Digital Colombia". {En línea}. octubre de 2015} disponible en: http://www.ideca.gov.co/sites/default/files/files/Presentaciones/Presentaciones_20 13/Modelo%20de%20Seguridad_MINTIC_Oct%206_2013.pdf.

Velásquez, J. (2015). *Modelamiento de los procesos de auditoría en seguridad de la información asociados a los dominios,8,13, y 14 del anexo A de la norma ISO 27001 mediante una herramienta de flujo de trabajo.* Tesis de Maestría: Universidad Tecnológica de Pereira. Pereira, Risaralda.

Anexo A. Matriz de consistencia

Objetivo genera	Analizar el sistema de gestión de seguridad de la información, bajo la norma ISO7/IEC 27001:2015, en la empresa Magdaniel Ltda., en el Distrito Especial Turístico y Cultural de Riohacha.			
Variable	**Objetivos específicos**	**Dimensión**	**Indicadores**	**Ítems**
Sistema de Gestión de Seguridad de la Información, bajo la norma ISO7/IEC 27001:2015	Determinar las políticas de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.	Políticas de seguridad. Rojas (2014), MinAmbiente (2014), MinTic (2016).	Objetivos de seguridad	1, 2, 3, 4
			Roles y responsabilidades	5, 6
			Control de acceso	7, 8
	Definir la seguridad física y del entorno de la información bajo la norma ISO /IEC 27001:2015 en la empresa Magdaniel Ltda.	Seguridad física y del entorno ISO27001 (2013), Ochoa (2016), Peltier (2014)	Sistemas de protección	9, 10
			Áreas seguras	11, 12
			Valoración de riesgo	13, 14
			Análisis de riesgo	15, 16
	Identificar los activos de información, bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda.	Activos de la información ISO27001 (2013), Gómez & Álvarez (2012), Hodeghatta & Nayak (2014)	Propiedad de los activos	17, 18
			Inventario de activos	19, 20
	Proponer lineamientos para el sistema de gestión de seguridad de la información, bajo la norma ISO7/IEC 27001: 2015, en la empresa Magdaniel Ltda., en el distrito turístico y cultural de Riohacha.	Este objetivo no se operacionaliza. Será alcanzado con el desarrollo de los objetivos anteriores.		

Anexo B. Validación del contenido del instrumento

Expertos	Grado de formación	Formación: Link CvLac	Observaciones	Criterio
Experto 1	Magister Gerencia de las organizaciones y candidato a Doctor en Ciencias Gerenciales	https://n9.cl/rjys	Valido sin observaciones	Aprobado
Experto 2	Magister en telemática	https://n9.cl/kp4u	Valido con correcciones. Anexar un ítem más	Aprobado
Experto 3	Magister en Gestión de la I+D, Doctora en Ciencia y Tecnología	https://n9.cl/2hbg	Valido con correcciones. Anexar dos afirmaciones en relación al indicador de objetivos de seguridad	Aprobado
Experto 4	Doctorado en Ciencias Gerenciales	https://n9.cl/1sea	Valido con correcciones. Mejorar la redacción	Aprobado
Experto 5	Doctorado en Ciencias Gerenciales	https://n9.cl/fo4t	Valido con correcciones. Mejorar la redacción	Aprobado

Anexo C. Cuestionario definitivo

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVA
PROGRAMA DE MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS
UNIVERSIDAD DE LA GUAJIRA

El presente cuestionario pretende como objetivo general analizar el sistema de gestión de seguridad de la información, bajo la norma ISO/IEC 27001:2015, en la empresa Magdaniel Ltda., en el Distrito Turístico Especial y Cultural de Riohacha, donde las respuestas serán sometidas a un análisis para dar cumplimiento al objetivo planteado, por lo cual es necesario su sinceridad en la respuesta de cada uno de los ítems planteados. La información recolectada será de carácter confidencial y con fines investigativos.

La respuesta a cada una de las preguntas debe ser contestadas teniendo en cuenta los siguientes criterios: Totalmente de acuerdo (5) De acuerdo (4) Neutral (3) En desacuerdo (2) Totalmente en desacuerdo (1).

AFIRMACIONES	Totalmente de acuerdo	De acuerdo	Neutral	En desacuerdo	Totalmente en desacuerdo
	5	4	3	2	1
1. La empresa cumple con los objetivos de seguridad de la información					
2. Dentro de la empresa se dispone de garantías para la confidencialidad de la información					
3. La información de la entidad cuenta con garantías de integridad dentro del sistema de información					
4. En la entidad los trabajadores cuentan con disponibilidad de la información					
5. La empresa cumple con los requisitos para la asignación de responsabilidades en el aseguramiento del sistema de gestión de seguridad de la información.					
6. Los trabajadores son monitoreados en el desempeño de sus actividades					
7. La empresa cuenta con sistemas de contraseñas en sus equipos informáticos					
8. El sistema informático de la empresa cuenta con las características para evitar el ingreso de personas no autorizadas a la información.					
9. La empresa cuenta con sistemas de protección para evitar algún tipo de riesgo informático					
10. La información de la empresa se encuentra expuesta riesgos informáticos					
11. Se dispone de áreas seguras dentro de la empresa para el personal no autorizado					
12. La información manejada por la empresa Magdaniel se encuentra protegida contra daños e interferencia					
13. El sistema de información de la empresa se encuentra expuesta a la ocurrencia de eventos no deseados.					
14. Se cuenta con la identificación de los riesgos que pueden causar daño a los activos e impedimento de acceso a la información.					
15. La empresa realiza análisis para la identificación de las amenazas dentro del sistema de informativo.					
16. La empresa cuenta con herramientas basadas en la gestión de la seguridad en la información las cuales permiten la identificación de los riesgos.					
17. Se encuentran definidos los activos de la empresa dentro del procesamiento de la información					
18. El procesamiento de la información de la empresa es propiedad designada de la organización.					
19. La empresa realiza el proceso de inventario de sus activos					
20. Considera que los activos son parte importante de la empresa					

Anexo D. Cálculo de confiabilidad

Resumen de procesamiento de casos

		N	%
Casos	Válido	5	100,0
	Excluido	0	,0
	Total	5	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,960	,967	19